Enquête de la Commission LIBE

sur la surveillance électronique de masse des citoyens de l'Union européenne

Audience publique, Strasbourg, le 7 octobre 2013

Contribution de Peter Hustinx (CEPD)

- Je vous remercie de votre invitation. La «sphère de sécurité» (*US Safe Harbour*) et les autres instruments pour les transferts internationaux de données sont au programme de la session d'aujourd'hui et je souhaiterais profiter de cette occasion pour formuler quelques remarques générales sur les enjeux et sur les mesures qu'il faudrait prendre suite aux différentes révélations concernant la surveillance électronique de masse des citoyens de l'Union européenne (UE).

- Lorsque le premier épisode de l'histoire de l'Agence nationale de sécurité américaine (NSA) avait été publié en juin dernier, nous avions immédiatement exprimé nos préoccupations concernant les possibles graves implications pour la vie privée et autres droits fondamentaux des citoyens de l'UE. Nous avons demandé des explications détaillées et la clarification des faits, nous avons insisté pour que des mesures appropriées soient prises sur le champ et depuis nous n'en finissons pas de suivre les rebondissements de cette affaire.

- Je tiens à exprimer ma reconnaissance à la vice-présidente M^{me} Reding pour les mesures prises au nom de la Commission européenne, et

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: 32-2-283 19 00 - Fax: 32-2-283 19 50

j’apprécie également la fermeté des propos tenus par M^{me} Merkel et d’autres dirigeants européens.

- Comme vous le savez, le groupe de travail «Article 29» (GT29) travaille actuellement sur une évaluation des différents programmes de surveillance, de leurs éventuelles conséquences sur la protection des données des citoyens de l’UE et des possibles implications pour les transferts internationaux. Notre personnel s’emploie activement à cette analyse portant, par exemple, sur l’applicabilité de la législation de l’UE et les différents problèmes qui se posent dans ce contexte.

- Lors de sa dernière réunion plénière il y a seulement quelques jours, le GT29 a donné mandat à ses sous-groupes concernés de poursuivre leur analyse des différents programmes et d’en rendre compte lors de la réunion plénière de décembre. Le GT29 sera alors très probablement en mesure d’adopter une position sur tous les aspects importants du sujet.

- Certains faits ne sont pas encore suffisamment éclaircis – et pourraient bien ne jamais l’être, mais cela ne doit pas nous empêcher d’explorer tous les scénarios pertinents et d’analyser leurs conséquences. En outre, nous espérons bien tirer profit à un moment ou un autre des résultats et conclusions d’autres travaux en cours.

- Le CEPD est particulièrement soucieux des préjudices éventuellement causés aux institutions et organes de l’UE, et nous examinerons s’il s’avère nécessaire de renforcer les niveaux actuels de sécurité de l’information, en tenant certainement compte de la récente histoire de Belgacom. Dans ce contexte, nous intensifions actuellement nos contacts avec tous les services concernés.

- Les trois éléments les plus marquants, au stade actuel de nos connaissances, sont (i) l'ampleur de la surveillance déployée, (ii) le nombre d'acteurs privés, y compris les géants de l'Internet, qui ont apparemment été impliqués de manière active ou passive, et (iii) l'apparition de points faibles et de portes dérobées dans les systèmes de cryptage, avec pour résultats des effets pervers particulièrement importants et la confiance de la population largement ébranlée.

- À ce stade, il semble fort probable que nous soyons confrontés à des défis mettant en cause l'existence de nos droits et libertés fondamentaux. Nous devons donc être préparés à «*indiquer les limites à ne pas franchir*».

- D'importantes garanties en matière de protection de la vie privée doivent être négociées et adoptées, faute de quoi nous devrons envisager d'interrompre les transferts de données et de suspendre ou mettre fin aux accords existants pour l'échange de données.

- Dans le même temps, on doit pouvoir développer des réponses plus intelligentes, en transformant la crise en une opportunité et en tournant la situation à notre avantage.

- Il me semble qu'une première conclusion devrait être qu'il y a désormais encore plus de raisons de décider de l'adoption rapide d'un règlement général sur la protection des données qui nous permettra de cibler les acteurs privés de manière plus efficace que dans les cadres juridiques actuels.

- Cela implique des dispositions renforcées en termes de responsabilité et de responsabilisation et des modalités de supervision et d'application plus solides et plus cohérentes dans l'UE. Il sera ainsi essentiel d'élargir le

champ d'application de la législation de l'UE afin d'assurer des règles de jeu équitables pour tous les acteurs évoluant sur le marché européen.

- Le règlement devrait également introduire un mécanisme tel que celui initialement prévu à l'article 42 d'une version antérieure, pour parer à l'éventualité d'un conflit en matière de droit international où les juridictions ont des avis contradictoires de leurs intérêts publics respectifs. Le principe de base devrait être que tous les échanges de données soient conformes à la législation de l'UE, sauf dispositions contraires stipulées par un accord international ou sauf exception accordée par une autorité de contrôle ou judiciaire.

- Un autre sujet mérite toute notre attention: un protocole additionnel à la Convention sur la cybercriminalité – tel que celui en cours de discussion dans le contexte du Conseil de l'Europe – risque d'ouvrir la voie à des accès injustifiés de la part des services de renseignement, aux données stockées dans d'autres juridictions. Ce problème a été soulevé dans l'avis de la Commission LIBE pour la commission ITRE (Industrie, Recherche et Énergie) sur la stratégie pour l'informatique en nuage. Nous devrions faire tout notre possible pour nous assurer que ce protocole additionnel ne sera pas adopté.

- L'histoire avec la NSA a aussi d'autres implications que je peux seulement évoquer très brièvement à présent. Si nous devons *«indiquer les limites à ne pas franchir»,* il faudrait le faire en affirmant notre culture européenne en matière de protection des données, qui n'exerce aucune discrimination fondée sur la nationalité. Nous ne pouvons donc pas accepter une distinction entre personnes américaines et non américaines, qui laisse tous les citoyens de l'UE sans aucune protection juridique appropriée.

- Un autre problème est la *collecte* de données apparemment à grande échelle, soumise seulement à des restrictions concernant leur *utilisation*. Cela est totalement incompatible avec la priorité que nous accordons aux principes de nécessité et de proportionnalité dès lors que des droits fondamentaux ne sont pas respectés.

- Pour dire les choses très clairement, je pense que nous devons prendre position sur le sujet, et ce «*maintenant ou jamais*».

- À cet égard, il ne devrait pas être difficile d'établir un solide programme de discussions – et au besoin de négociations – transatlantiques pour l'avenir. Je reviendrai sur ce point à la fin de mes observations.

- Permettez-moi d'évoquer à présent la «sphère de sécurité» qui constitue l'un des thèmes spécifiques de cette audience. Je voudrais développer mes observations autour de trois axes: premièrement, le concept de «caractère adéquat»; deuxièmement, la «sphère de sécurité régulière»; et enfin, l'exception de la «sûreté de l'État» et des intérêts similaires.

- La notion de niveau de protection «adéquat» était prévue à l'article 25 de la directive pour assurer que les échanges de données avec des pays tiers bénéficient d'une protection suffisante, variable en fonction des circonstances du cas d'espèce, mais pas nécessairement équivalente au niveau de protection existant dans l'UE. Il s'agit d'une approche pragmatique qui reflète la diversité des cultures juridiques dans le monde.

- La notion d'«adéquation» a été développée dans un avis du groupe de travail «Article 29» (WP 12) adopté en 1998, qui a servi de base à toutes les décisions d'adéquation de la Commission, y compris celle sur la

«sphère de sécurité». Un niveau de protection adéquat, tel que celui auquel il est fait référence, nécessite de respecter un ensemble de principes relatifs au «contenu» et des exigences «de procédure/ d'application» afin d'assurer efficacement la conformité aux principes, de soutenir et d'aider les personnes concernées, et de garantir une réparation appropriée. En d'autres termes, une approche «objective» ou fonctionnelle».

- Parmi les principes relatifs au contenu mentionnés dans l'avis figurent la limitation de la finalité, la qualité et proportionnalité des données, la transparence, la sécurité des données, les droits d'accès et de rectification, et les restrictions aux transferts ultérieurs. Toutefois, l'avis mentionnait également que des exceptions pouvaient s'appliquer, lesquelles *"devraient être conformes à l'article 13 de la directive"* (voir page 6). Cet article 13 autorise des exceptions, dans la mesure nécessaire, pour la sûreté de l'État et la sécurité publique. Bien que cette disposition ne soit pas applicable dans un pays tiers, elle est invoquée par analogie.

- Dans le contexte des dispositions contractuelles visant à assurer le niveau de protection adéquat, l'avis évoque également le problème de «primauté du droit» (voir pages 21-22). L'une des conclusions est que «*les pays où les autorités nationales se dotent d'un pouvoir en matière d'accès à l'information qui va au-delà de celui autorisé par les normes internationalement reconnues en matière de protection des droits de l'homme ne seront pas des destinations sûres pour les transferts de données sur la base de clauses contractuelles»* (voir page 23). Mais la même approche serait bien évidemment applicable aux constatations concernant l'adéquation.

- La «sphère de sécurité» est sujette à controverse depuis le début. Le GT29 a adopté une série d'avis très critiques au cours des négociations entre la Commission et le ministère américain du commerce. Mais une fois que les négociations ont été clôturées et que la décision de la Commission sur la «sphère de sécurité» a été adoptée, le GT29 s'est largement investi pour la mettre en œuvre et améliorer son fonctionnement.

- Permettez-moi de dire clairement que, s'agissant de la «sphère de sécurité», les autorités chargées de la protection des données dans l'UE mettent l'accent sur les travaux et efforts à faire au niveau national. Les institutions et organes de l'UE transfèrent occasionnellement des données à caractère personnel vers des pays tiers, mais cela n'implique généralement pas la «sphère de sécurité». Toutefois, d'un point de vue stratégique, l'évaluation est bien différente. Nous avons donc été étroitement impliqués à différents stades du processus.

- On peut dire à juste titre que la «sphère de sécurité» a connu un démarrage lent et qu'elle est montée progressivement en puissance. Nous pensons que des améliorations conséquentes ont été apportées et que la plupart des problèmes ont désormais été réglés. À cet égard, il convient de mentionner le rôle plus actif du ministère américain du commerce dans la procédure d'autocertification et le rôle de la Commission fédérale du Commerce (FTC - Federal Trade Commission) en matière d'application. La «sphère de sécurité» a donc un certain mérite.

- Mais l'absence d'un tour d'horizon complet de la pratique et de l'expérience de la «sphère de sécurité» et de données statistiques suffisamment fiables demeure problématique. C'est la raison pour laquelle un groupe de contact sur la protection de la vie privée a été constitué avec des représentants des deux parties, lequel se consacre à

combler cette lacune depuis quelques années. À ce stade, le GT29 attend avec impatience le rapport d'évaluation dont l'arrivée imminente a été annoncée par la Commission européenne.

.

- Selon la partie introductive des principes de la «sphère de sécurité» (voir annexe I de la décision de la Commission du 26 juillet 2000), l'adhésion à ces principes peut être limitée par: *«les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois ... »*. Il y a également une disposition similaire qui traite de la primauté des lois. Toutefois il conviendrait de garder présent à l'esprit que nous traitons dans ce contexte d'exceptions aux droits fondamentaux, que la Cour de justice européenne et la Cour européenne des droits de l'homme interprètent toujours de manière restrictive.

- En outre, le texte auquel il est fait référence est soigneusement formulé – avec les termes *«dans la mesure nécessaire»* – tandis que dans la situation actuelle, nous semblons être confrontés à un non-respect systématique des principes de la «sphère de sécurité» dans tous les cas où les entreprises approchées ont peut-être fait l'objet d'un quelconque programme de surveillance de masse.

- Les deux parties risquent bien de ne pas s'entendre sur la question de l'applicabilité de cette exception. Dans tous les cas, il conviendrait d'y répondre par la négative si nous considérons que les programmes de surveillance concernés étaient réellement excessifs. Mais là aussi, il est probable que les deux parties ne partageront pas cette conclusion.

- Cela pourrait donner l'occasion d'invoquer l'article 4 de la décision de la Commission, lequel indique que cette 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 (...) est dépassé par les exigences du droit américain.» Tout élément de preuve pertinent pourrait par exemple être fourni par un rapport d'évaluation de la Commission tel que celui attendu d'ici la fin de l'année.

- D'autres éventuelles mesures devraient alors être prises par la Commission, conjointement avec les représentants des États membres du Comité de l'article 31. Dans ce cas, l'accent sera davantage mis sur *«l'approche à adopter pour faire face à une surveillance excessive»* ou *«le désaccord sur ce sujet»* que sur l'efficacité de la «sphère de sécurité» en tant qu'instrument visant à garantir un niveau de protection adéquat. Mais le rapport de la Commission pourrait prendre en compte les deux aspects et nourrir ainsi le débat et les négociations avec la partie américaine. Dans ce contexte, permettez-moi d'ajouter qu'on ne devrait pas se débarrasser de la «sphère de sécurité» en tant que telle sans avoir étudié les possibilités de l'améliorer.

- Un plan d'amélioration de la «sphère de sécurité» *«à la lumière de l'expérience acquise»* pourrait être combiné avec la prise en compte d'autres problématiques, soit dans le cadre de la coopération en matière d'application de la loi ou des échanges commerciaux, ou dans la perspective à long terme d'un nouvel accord international avec des principes de surveillance licite.

- Dans ce contexte, nous ne devrions pas exclure que la solution vienne en partie du côté américain. Elle pourrait prendre la forme de recommandations du Conseil de surveillance de la vie privée et des libertés civiles des États-Unis (US Privacy and Civil Liberties Oversight Board) ou du groupe d'experts interne mis en place par l'administration

américaine sur le renforcement de la transparence, ou d'autres garanties importantes.

- Dans tous les cas, il serait judicieux de garder ouvertes toutes les options et dans le même temps d'explorer toutes les possibilités pertinentes pour un engagement constructif.