Nos 6759[4]
6762[4]

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant approbation du „Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information", signé à Luxembourg le 20 juin 2012

PROJET DE LOI

portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(30.7.2015)

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée „la loi modifiée du 2 août 2002"), la Commission nationale pour la protection des données (ci-après désignée „la Commission nationale") a notamment pour mission d'*„être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi"*.

Par courrier du 5 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6759 portant approbation du „Memorandum of Understanding between the Government of the Grand Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information", signé à Luxembourg le 20 juin 2012.

Par courrier du 6 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6762 portant approbation de l'Accord entre le Gouvernement de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012.

Les deux projets de loi sous avis, amendés le 10 avril 2015 par le gouvernement, portent sur l'approbation d'accords prévoyant des échanges, en matière policière et judiciaire, de données à caractère personnel du Luxembourg en direction des Etats-Unis d'Amérique et vice versa.

*

1. FINALITES

En vertu du principe de finalité, les données à caractère personnel ne peuvent être traitées qu'en vue d'une ou de plusieurs finalités légitimes, ce qui implique qu'il doit toujours y avoir une raison concrète pour laquelle les données à caractère personnel seront traitées, et que cette raison doit être établie précisément avant le début du traitement. Ce principe est un des principes de base de la protection des données.

Considérations d'ordre général

Les deux accords ont comme objectif de combattre le terrorisme. Mais alors que le *Memorandum of Understanding between the Government of the Grand Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information* (ci-après le „Mémorandum") se limite à la lutte contre le terrorisme, l'*Accord entre le Gouvernement de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave* (ci-après l'„accord crime grave") englobe la lutte contre la criminalité de manière générale, même si un accent particulier semble être mis sur le terrorisme (préambule, article 11).

L'accord crime grave prévoit une utilisation à la fois préventive et répressive des données, le Mémorandum semble, à la lecture du préambule, avoir un caractère essentiellement préventif. L'utilisation des données à des fins répressives n'y est pas exclue, mais soumise à des restrictions (article V point 2.).

Les finalités des deux accords se chevauchent donc en grande partie.

La CNPD déplore que l'exposé des motifs ne donne pas davantage d'informations sur les raisons pour lesquelles il est recouru à deux accords séparés, ainsi que sur les liens exacts entre les deux accords.

Les infractions visées

Pour ce qui est du Mémorandum, il vise les infractions terroristes. La CNPD se demande si le mot „terrorisme" a la même signification aux Etats-Unis d'Amérique qu'au Luxembourg? Ni le Mémorandum lui-même, ni le projet de loi d'approbation ne contient de définition ni une quelconque référence à des infractions précises en droit luxembourgeois ou en droit américain ou à des textes supranationaux auxquels il faudra se référer en cas de difficulté d'interprétation.

Pour ce qui est de l'accord crime grave, celui-ci s'applique à toutes les infractions qualifiées de crimes graves par l'accord. L'expression „crime grave" désigne, en vertu de l'article 1er de l'accord, *„un agissement constitutif d'une infraction passible d'un emprisonnement maximum de plus d'un an, ou d'une sanction plus lourde"*. Il s'agirait donc le cas échéant d'*infractions* graves et pas forcément de *crimes* graves selon la terminologie du droit pénal luxembourgeois.

L'accord ne précise pas si cette condition de peine doit être remplie dans le chef de la législation de l'Etat requérant, de l'Etat requis ou des deux.

Rappelons que la Cour de justice de l'Union européenne a déclaré invalide la *directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE* en épinglant notamment le fait que la notion de l'„infraction grave" permettant un accès par les autorités répressives aux données n'y était pas délimitée de manière assez précise, alors que seulement les infractions suffisamment graves justifient une ingérence aux droits fondamentaux telle que celle résultant de la directive[1]. Le Luxembourg (dont la législation prévoit que toute infraction pénale, qui emporte une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, est à considérer comme infraction grave au sens de cette directive précitée) est justement

---

1 Considérant 60 de l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130deb6f9lfca9baf400aaa56cdd0274c2f3b.e34KaxiLc3eQc40LaxqMbN4ObxaMe0?text=&docid=150642&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=224005

en train de remplacer ce seuil d'un an par un catalogue précis des infractions visées (projet de loi n° 6763) pour tenir compte dudit arrêt.

Force est de constater qu'en l'espèce, on a de nouveau recours à un seuil de peine général pour déterminer les infractions ayant une gravité suffisante pour justifier certains traitements de données très délicats, au lieu d'analyser de manière précise quelles sont les infractions nécessitant un recours aux traitements en question.

On peut d'ailleurs signaler que des accords similaires signés par la France[2] et la Belgique[3] comportent en annexe un catalogue des infractions à considérer comme crimes graves au sens de l'accord.

Pour ce qui est de l'article 11 de l'accord crime grave, il s'applique, selon l'intitulé de l'article, aux „infractions criminelles et terroristes graves". Faut-il comprendre par-là les infractions *criminelles* graves *et* les infractions *terroristes* graves? Apparemment oui, puisque le paragraphe 1. lettre c. vise de manière expresse les infractions criminelles graves en plus des infractions terroristes visées à la lettre a. du paragraphe premier. Contrairement à ce qui est affirmé dans le commentaire des articles, le champ d'application de l'article 11 semble donc englober toutes les infractions auxquelles s'appliquent les autres dispositions de l'accord et ne pas se limiter aux infractions terroristes. Par ailleurs, l'article 11 ne prévoit aucune différence de régime entre les infractions terroristes et les autres infractions graves.

Il y a lieu de noter qu'un accord similaire conclu par l'Allemagne contient un article semblable à l'article 11. Cependant, il n'y est question que d'infractions terroristes (et de l'entraînement en vue de la commission de ces infractions terroristes) et non d'infractions graves de manière générale.[4] Par ailleurs, une procédure de notifications entre Etats signataires y est prévue pour déterminer les infractions concernées par l'article en question.[5] La CNPD se demande pourquoi le gouvernement luxembourgeois n'a pas insisté sur la mise en place de garanties similaires.

L'utilisation des données pour d'autres finalités

L'article 13 paragraphe 1 de l'accord crime grave dispose que chaque Partie peut traiter les données obtenues en vertu de l'accord *„pour toute autre finalité, mais uniquement avec le consentement préalable de la Partie ayant transmis les données."*

Une telle utilisation pour d'autres finalités se heurterait au principe de finalité énoncé ci-dessus.

Elle nécessite certes le consentement de la Partie ayant transmis les données, mais n'exige pas celui des personnes concernées et se ferait, le cas échéant, même à l'insu de celles-ci.

D'ailleurs, le commentaire des articles ne donne aucun exemple d'une telle utilisation pour une autre finalité.

Dans ces conditions, et étant donné que l'article 13 précité prévoit que l'utilisation à d'autres fins ne peut se faire qu'avec avec le consentement préalable de la Partie ayant transmis les données, c'est-à-dire ne peut pas se faire contre le gré de la Partie requise, il se pose la question si on ne pourrait pas

---

2 Accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des Etats-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de lutter contre la criminalité grave et le terrorisme

http://www.senat.fr/leg/pjl14-018.pdf

3 Accord entre le Royaume de Belgique et les Etats-Unis d'Amérique sur le renforcement de la coopération dans la prévention et la lutte contre la criminalité grave, établi à Bruxelles le 20 septembre 2011

http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=14-10-15&numac=2014015140

4 *Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität*, Article 10 paragraphe (1)

http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&start=//*%255B@attr_id='bgbl209s1010.pdf'%255D#_bgbl_%2F%2F*%5b%40attr_id3D%27bgbl209s1010.pdf%27%5D_1431526476000

5 Article 10 paragraphe (3):

„(3) Mit der Notifikation nach Artikel 24 Satz 1 können die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten. Diese Erklärung kann jederzeit durch eine Notifikation gegenüber der anderen Vertragspartei geändert werden."

déjà exclure, au niveau de la loi d'approbation, une telle utilisation pour ce qui est des transferts du Luxembourg vers les Etats-Unis d'Amérique.

Si une telle utilisation à des finalités autres ne peut pas être exclue à ce stade, elle devrait au moins être entourée de conditions très strictes, comme celles proposées par la *Commission de la protection de la vie privée* belge[6]:

„41. Le fait de pouvoir utiliser ces données „pour toute autre finalité, moyennant l'accord préalable de l'autre Etat" (article 14, § 1er d)) n'est pas, en l'état actuel du libellé, de nature à rassurer la Commission. Ce traitement ultérieur pour toute autre finalité devrait être assorti de garanties, telles qu'au minimum:

- *cette faculté ne s'applique qu'au cas par cas,*
- *pour une autre finalité spécifiée et motivée au moment de la demande,*
- *moyennant l'accord préalable, spécifique et au cas par cas de l'Etat (un accord de principe général ne serait pas admissible), et*
- *avec une journalisation non seulement des transferts internationaux de données, mais aussi des transferts au sein même de l'Etat (entre autorités nationales habilitées), de sorte qu'un contrôle effectif, notamment par la Commission, soit rendu possible (voir infra point 45),*
- *l'accord préalable de l'Etat et la décision de transmission doivent pouvoir faire l'objet d'un contrôle juridictionnel,*
- *si les cinq conditions ci-dessus ne sont pas rencontrées dans le corps même du texte de l'Accord PCSC, la Commission émet un avis défavorable sur cette transmission „pour toute autre finalité" et recommande la suppression pure et simple d'une telle possibilité dans l'Accord PCSC."*

Enfin, on peut se demander quelles sont les hypothèses dans lesquelles une communication des données à des personnes privées (avec l'accord de la Partie requise), telle qu'évoquée par l'article 13 paragraphe 2 de l'accord crime grave et l'article V paragraphe 2 lettre d du Mémorandum serait possible et si une telle communication respecterait le principe de finalité.

*

2. LES CATEGORIES DE DONNEES

Le Mémorandum évoque d'une part la „terrorism screening information" et d'autre part la „background information".

Par terrorism screening information, il faut comprendre les données d'identification telles que définies à l'article II point 2. du Mémorandum.

La définition de la *„background information"* du Mémorandum est très vague. Peut-il s'agir de données à caractère sensible telle que des informations sur les opinions politiques ou les convictions religieuses des personnes concernées? Le Mémorandum définit d'ailleurs cette notion sans, par la suite, expliquer de manière spécifique quelles seront précisément les communications de données ou autres traitements effectués concernant les données en question. On peut donc se demander pourquoi on définit la „background information" sans y attacher un régime particulier.

De même, les „données complémentaires" des articles 5 et 8 de l'accord crime grave ne sont pas précisées davantage. Ici encore, il se pose notamment la question de savoir s'il peut s'agir de données sensibles comme les données sur les opinions politiques ou les convictions religieuses des personnes concernées.

*

6 Avis n° 27/2010 du 24 novembre 2010, *Objet: Projet d'accord bilatéral entre la Belgique et les Etats-Unis sur le renforcement de la coopération dans la prévention et la lutte contre les crimes graves (draft agreement on enhancing cooperation in Preventing and Combating Serious Crime – „Accord PCSC") (CO-A-2010-025),* point 41
http://www.privacycommission.be/sites/privacycommission/files/documents/avis_27_2010_0.pdf

3. L'ORIGINE DES DONNEES

Plusieurs questions relatives à l'origine des données et la manière dont sont transmises les données (accès direct ou indirect à des bases de données nationales, communication sur demande etc.) se posent.

Les deux accords à approuver permettent-ils aux autorités américaines d'accéder indirectement via des bases de données luxembourgeoises à un certain nombre de systèmes d'information européens, comme les banques de données SIS II, EUROPOL ou VIS qui sont alimentées par des données nationales provenant des autorités répressives respectives des Etats membres de l'Union européenne?

Il se pose aussi la question de savoir si les échanges de données en direction des Etats-Unis d'Amérique peuvent porter sur des personnes sur lesquelles il n'existe – au moment de la demande effectuée par des autorités américaines – pas d'informations policières ou judiciaires au Luxembourg. Il y a lieu de relever qu'en droit interne luxembourgeois, les autorités policières et judiciaires peuvent accéder, sous certaines conditions, à des informations concernant n'importe quel habitant du pays, informations contenues dans une série de banques de données d'autorités publiques. Lesdits accès sont effectués en vertu l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police respectivement l'article 48-24 du Code d'instruction criminelle. Est-ce que, en application des deux accords à approuver, les autorités américaines peuvent, de manière indirecte, voire directe, avoir accès aux mêmes bases de données d'autorités publiques luxembourgeoises même pour des personnes jusqu'alors inconnues des autorités policières et judiciaires luxembourgeoises? En effet, les amendements gouvernementaux évoquent de manière expresse des *„traitements de données à caractère personnel visés par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'inspection générale de la police"*.

Enfin, lors de la mise en œuvre des accords sous avis, on aura recours à la base de données créée par le règlement grand-ducal modifiée du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale („règlement Ingepol").

La CNPD voudrait rappeler[7] dans ce contexte que le règlement Ingepol qui date de 1992 ne répond pas à toutes les exigences juridiques de protection des données découlant de la loi modifiée du 2 août 2002, ni de la *décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale* et qu'il devrait être remplacé par un nouveau règlement grand-ducal en exécution de l'article 17 paragraphe (1) lettre (a) des articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Dans ses rapports annuels, l'autorité de contrôle spécifique „Article 17" a d'ailleurs régulièrement critiqué la prorogation annuelle du règlement Ingepol depuis l'adoption de la loi modifiée du 2 août 2002, ainsi que l'absence d'adoption d'un nouveau règlement grand-ducal.

*

4. LA TRANSMISSION DES DONNEES

L'initiative de la transmission

Le Mémorandum ne donne aucune précision relative à l'initiative de la transmission. Il ne permet donc pas de savoir si les données sont transmises par le biais d'un accès direct accordé à l'autre Partie, sur demande de la part de la partie qui veut obtenir des données ou de manière spontanée par la Partie donnant les informations.

Il est seulement précisé dans le projet de loi d'approbation que, pour une partie des données, l'accès se fera après autorisation du Procureur général d'Etat. La même disposition se retrouve dans le projet de loi d'approbation de l'accord crime grave.

Les amendements gouvernementaux (aux deux textes sous avis) donnent davantage de précisions pour ce qui est des transmissions soumises à l'accord du Procureur d'Etat. Cependant cet accord n'est

---

7 La CNPD a déjà épinglé ce problème dans son avis relatif au projet de loi n° 6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière, délibération n° 385/2013 du 25 juillet 2013, http://www.cnpd.public.lu/fr/decisions-avis/2013/securite-routiere/385_2013_Deliberation_Ministre-du-Developpement-durable-et-des-infrastrctures_avis_PL_6566_securite_routiere.pdf

pas requis pour les *„traitements de données à caractère personnel visés par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'inspection générale de la police"*. Cette exclusion est problématique tant au regard du grand nombre de catégories de données concernées que des personnes concernées – en fait potentiellement toute la population du Luxembourg.

L'accord crime grave prévoit que la consultation des données dactyloscopiques et des profils ADN se fait par accès direct accordé à la Partie qui reçoit les informations, par le biais du point de contact (articles 4 et 7), des précisions supplémentaires devant être données par des ententes ou des accords de mise en oeuvre (articles 6 point 2. et 9 point 2.). Un tel accès direct est en principe problématique, car l'Etat détenant les données en perd, en quelque sorte, la maîtrise.

Il est dès lors important de veiller à ce que cet accès direct se limite à l'information s'il y a une correspondance entre un profil dactyloscopique ou génétique américain et un profil correspondant luxembourgeois sans communication d'autres informations par le biais de cet accès direct (stricte limitation au système „hit, no hit").

Pour ce qui est de la communication des données complémentaires prévue par les articles 5 et 8, il faudra apparemment complètement se référer à des ententes ou des accords de mise en oeuvre. Or, ces textes font défaut et il aurait été utile de pouvoir les apprécier ensemble avec les textes de base.

Enfin, l'article 11 prévoit, du moins partiellement, une communication spontanée par l'Etat qui détient les informations.

Il se pose la question de savoir quand une telle communication a lieu et sur base de quel motif. Seulement chaque fois qu'une personne suspectée d'actes terroristes a un quelconque lien avec l'autre Partie signataire? Malheureusement l'accord ne donne pas de réponse à cette question.

Dans ces circonstances, et vu la quantité considérable des données le cas échéant transmises (article 11 paragraphe 2.), il est d'autant plus important de délimiter de manière plus précise les infractions auxquelles s'applique l'article 11 (cf. partie „finalités" du présent avis).

Conservation des traces des transmissions et accès

Pour pouvoir sanctionner des abus et des accès non autorisés, il est primordial que les transmissions et accès puissent être retracés.

En vertu de l'article V paragraphe (8) du Mémorandum, chaque Partie doit déterminer les personnes ayant accès aux données de l'autre Partie. Il n'y est cependant pas précisé si on devra pouvoir retracer chaque accès individuel aux données qui est effectué.

L'article 15 de l'accord crime grave prévoit un système de conservation des traces. Il prévoit notamment que des informations sur les données transmises et la date de la transmission seront conservées. Il serait primordial qu'une information – serait-elle minime – sur le motif de la transmission soit également conservée, comme c'est le cas en droit interne luxembourgeois pour les accès des officiers de police judiciaire ou les magistrats aux banques de données d'administrations publiques en vertu l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police respectivement l'article 48-24 du Code d'instruction criminelle.

Pour ce qui est des personnes ou institutions recevant les données après leur transmission, une conservation des traces est prévue concernant *„le destinataire des données au cas où ces dernières sont transmises à d'autres entités"*.

Cette disposition laisse présumer que les traces des destinataires primaires recevant des données à travers le point de contact c'est-à-dire les institutions policières ou judiciaires ne seraient pas conservées contrairement aux traces des autres destinataires.

Cependant, les destinataires primaires, c'est-à-dire les institutions policières ou judiciaires recevant les données en premier devraient également pouvoir être retracées. Il se pose aussi la question de savoir si le système devra seulement permettre de retracer les institutions recevant les informations ou également l'agent individuel qui a accès aux données.

*

5. LA SECURITE DES TRAITEMENTS

L'article V paragraphe 5 du Mémorandum ne pose que le principe de base du respect de la sécurité des données et renvoie pour l'essentiel aux droits nationaux applicables.

Est ce que les règles des Etats-Unis d'Amérique sont satisfaisantes, sachant que les Etats-Unis d'Amérique ne constituent pas un pays ayant un niveau adéquat de protection des données au sens de la législation européenne et luxembourgeoise?

Mais même du côté luxembourgeois, il n'est pas sûr que le droit applicable soit satisfaisant. Le projet de loi d'approbation ne prévoit pas de dispositions particulières relatives à la sécurité des données. Ce seraient donc les règles de droit commun qui s'appliqueraient, c'est-à-dire celles des articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui s'appliquent. Or, ces règles, qui s'appliquent à tous types de traitements, laissent au responsable du traitement une marge de manoeuvre importante – peut-être trop importante au regard des traitements effectués en vertu du Mémorandum. D'ailleurs, la Cour de justice de l'Union européenne a déclaré invalide la directive sur la rétention des données de télécommunications en partie parce qu'elle ne prévoyait pas assez de dispositions précises en matière de sécurité adaptées aux caractéristiques particulières des traitements effectués et renvoyait en partie aux règles générales applicables en matière de protection des données[8].

Du moins pour les traitements de données opérés par la Police Grand-Ducale, un règlement grand-ducal pris en exécution de l'article 17 de la loi modifiée du 2 août 2002 aurait dû prévoir ces mesures. Or, comme déjà expliqué ci-avant, ce règlement n'a jamais été pris (cf. point 3 dernier paragraphe, page 6 du présent avis).

En ce qui concerne l'accord crime grave, l'article 16 pose certes quelques principes de base mais renvoie encore aux Etats signataires pour préciser les détails.

*

6. LES DROITS DES PERSONNES CONCERNEES

Les accords ne règlent pas les droits des personnes concernées. Par exemple, il n'y a pas de dispositions relatives au droit d'accès ou au droit de rectification.

De même, les accords ne prévoient pas de voies de recours pour les justiciables.

Certes, l'article V paragraphe 11 du Mémorandum par exemple prévoit l'obligation pour les parties de prévoir des possibilités pour les individus d'introduire des „complaint", mais ne précise pas s'il s'agit d'un recours devant une instance judiciaire, une instance administrative (indépendante du gouvernement et de l'autorité qui traite les données?) ou simplement d'une possibilité offerte d'introduire une réclamation auprès de l'autorité qui traite les données.

Aucun des deux accords ne prévoit le contrôle du respect de la protection des données par une autorité de supervision indépendante.

Sur toutes ces questions, ce sera en fin de compte le droit national des Parties signataires qui déterminera seul les règles du jeu avec toutes les incertitudes que cela comporte.

A ces incertitudes d'ordre juridique s'ajoutent les difficultés pratiques pour les personnes concernées de s'adresser à des institutions situées de l'autre côté de l'Atlantique.

*

---

8 Considérants 66 à 68 de l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130deb6f91fca9baf400aaa56cdd0274c2f3b.e34KaxiLc3eQc40LaxqMbN40bxaMe0?text=&docid=150642&pageIndex=0&doclang=FR&mode=req&dir=%dir=&occ=first&part=1&cid=224005

7. CONCLUSION

Tant le Memorandum que l'accord crime grave présentent beaucoup d'imprécisions sur un bon nombre de questions ayant trait à la protection des données. La CNPD s'interroge dès lors sur la conformité des traitements de données, visés par les deux accords, à la législation européenne et nationale sur la protection des données.

Le fait que beaucoup de questions seront régies principalement, voire exclusivement par le droit interne des Etats signataires, laisse persister des doutes quant à l'existence de garanties suffisantes en matière de protection des données et de la vie privée des citoyens.

La CNPD regrette par ailleurs qu'elle n'ait pas été consultée lors de la phase de négociation, respectivement avant la signature des accords, alors que les projets de loi sous examen ont pour objet d'approuver les deux accords signés qui ne peuvent plus être modifiés à moins de les renégocier avec les Etats-Unis d'Amérique.

La CNPD espère donc qu'elle sera consultée préalablement à la conclusion d'ententes ou accords conclus en vertu des deux accords[9] et à la mise en oeuvre pratique et technique des deux accords.

Ainsi décidé à Esch-sur-Alzette en date du 30 juillet 2015.

La Commission nationale pour la protection des données

Tine A. LARSON	Thierry LALLEMANG	Georges WANTZ
Présidente	*Membre effectif*	*Membre effectif*

9 par exemple ceux prévus par les articles 6 et 9 de l'accord crime grave