



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session extraordinaire 2013-2014

TS/LB/yh/pk

P.V. J 26
P.V. ERMCE 31

Commission juridique

et

**Commission de l'Enseignement supérieur, de la Recherche,
des Médias, des Communications et de l'Espace**

Procès-verbal de la réunion du 16 juillet 2014

Ordre du jour :

1. Approbation des projets de procès-verbal de la réunion du 25 juin 2014 et de la réunion jointe du 2 juillet 2014

2. Examen des documents européens suivants:

COM(2013) 846 COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN ET AU CONSEIL Rétablir la confiance dans les flux de données entre l'Union européenne et les Etats-Unis d'Amérique

Le dossier précité ne relève pas du contrôle du principe de subsidiarité.

COM(2013) 847 COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN ET AU CONSEIL relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire

Le dossier précité ne relève pas du contrôle du principe de subsidiarité.

3. Echange de vues au sujet des deux arrêts de la Cour de Justice de l'Union européenne suivants:

C-293/12 - Digital Rights Ireland et Seitlinger e.a.

Arrêt de la Cour (grande chambre) du 8 avril 2014. Digital Rights Ireland Ltd (C-293/12) contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung (C-594/12) et autres. Demandes de décision préjudicielle: High Court - Irlande, Verfassungsgerichtshof - Autriche. Communications électroniques - Directive 2006/24/CE - Services de communications électroniques accessibles au public ou de réseaux publics de communications - Conservation de données générées ou traitées dans le cadre

de la fourniture de tels services - Validité - Articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne. Affaires jointes C-293/12 et C-594/12

C-131/12 - Google Spain et Google

Arrêt de la Cour (grande chambre) du 13 mai 2014. Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González. Demande de décision préjudicielle: Audiencia Nacional - Espagne. Données à caractère personnel - Protection des personnes physiques à l'égard du traitement de ces données - Directive 95/46/CE - Articles 2, 4, 12 et 14 - Champ d'application matériel et territorial - Moteurs de recherche sur Internet - Traitement des données contenues dans des sites web - Recherche, indexation et stockage de ces données - Responsabilité de l'exploitant du moteur de recherche - Établissement sur le territoire d'un État membre - Portée des obligations de cet exploitant et des droits de la personne concernée - Charte des droits fondamentaux de l'Union européenne - Articles 7 et 8. Affaire C-131/12

4. Divers

*

Présents : M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Franz Fayot, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth, membres de la Commission juridique

M. Claude Adam, Mme Diane Adehm, M. André Bauler, Mme Simone Beissel, M. Eugène Berger, Mme Cécile Hemmen remplaçant Mme Tess Burton, Mme Claudia Dall'Agnol remplaçant M. Yves Cruchten, Mme Martine Hansen, Mme Octavie Modert, M. Roger Negri, M. Marcel Oberweis, M. Roy Reding, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

M. Justin Turpel, député (*observateur*)

M. Xavier Bettel, Premier Ministre, Ministre d'Etat

M. Félix Braz, Ministre de la Justice

M. Gérard Lommel, du Ministère d'Etat, Service des Médias et des Communications, Président de la Commission nationale pour la protection des données

Mme Michèle Bram, du Ministère d'Etat, Direction "Médias, audiovisuel et société de l'information"

Mme Marie-Anne Ketter, du Ministère de la Justice

M. Robert Biever, Procureur général d'Etat

M. Laurent Besch, Mme Tania Sonnetti, de l'Administration parlementaire

Excusés : M. Alex Bodry, M. Léon Gloden, Mme Josée Lorsché, membres de la Commission juridique

Mme Taina Bofferding, Mme Tess Burton, M. Yves Cruchten, M. Serge Wilmes, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission juridique
Mme Simone Beissel, Président de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

1. Approbation des projets de procès-verbal de la réunion du 25 juin 2014 et de la réunion jointe du 2 juillet 2014

Les projets de procès-verbal de la réunion du 25 juin 2014 et de la réunion jointe du 2 juillet 2014 sont approuvés.

2. Examen des documents européens suivants:

COM(2013) 846 COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN ET AU CONSEIL Rétablir la confiance dans les flux de données entre l'Union européenne et les Etats-Unis d'Amérique

Le dossier précité ne relève pas du contrôle du principe de subsidiarité.

COM(2013) 847 COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN ET AU CONSEIL relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire

Le dossier précité ne relève pas du contrôle du principe de subsidiarité.

L'expert gouvernemental procède à une brève présentation des deux documents européens COM(2013) 846 et COM(2013) 847, pour le détail desquels il est renvoyé aux documents envoyés par courrier électronique aux membres des deux commissions en date du 8 juillet 2014.

L'orateur précise d'emblée que les transferts de données à caractère personnel constituent un volet important et nécessaire dans le cadre des échanges commerciaux entre l'Union européenne et les Etats-Unis d'Amérique. Or, suite aux révélations publiques sur les programmes de collecte de renseignements à grande échelle mis en œuvre par les services et agences de renseignement américains, et eu égard notamment au maniement peu respectueux du volet relatif à la protection des données à caractère personnel, la confiance dans ledit partenariat transatlantique a été ébranlée.

La Commission européenne vise par les communications sous examen à rétablir la confiance dans les transferts de données entre l'Union européenne et les Etats-Unis et ce notamment en renforçant les règles en matière de protection des données.

1) Document COM(2013) 846

Le document COM(2013) 846, visant le rétablissement de la confiance dans les flux de données entre l'Union européenne et les Etats-Unis, présente les enjeux et les risques faisant suite aux révélations sur les programmes américains de collecte de renseignements, ainsi que les mesures à mettre en œuvre le plus rapidement possible afin d'y répondre adéquatement et ce en vue de rétablir la confiance ébranlée dans ce partenariat.

1) Document COM(2013) 847

Le document COM(2013) 847 comporte une analyse du fonctionnement de la sphère de sécurité qui régit les transferts de données à des fins commerciales entre l'Union européenne et les Etats-Unis du point de vue des citoyens de l'Union européenne et des entreprises établies sur son territoire (accord «*Safe Harbor*»). Dans ce document une série de problèmes que les Etats-Unis doivent résoudre pour améliorer le régime de protection des données mis en place en 2000 est exposé. Ce dernier permet la libre circulation de données à caractère personnel à des fins commerciales entre l'Union européenne et les entreprises américaines qui adhèrent aux principes de la sphère de sécurité. En effet, l'accord «*Safe Harbor*», qui crée une base juridique pour les transferts de données à caractère personnel depuis l'Union européenne vers des entreprises aux Etats-Unis, oblige ces dernières à se conformer au principe européen de protection de la vie privée lorsqu'elles traitent des données européennes, même en dehors de l'Union européenne. A noter que si l'adhésion est volontaire, l'entreprise s'engage, une fois souscrit audit accord, à respecter les principes qui sont contractuels.

Il y a notamment lieu de se référer à la page 20 du document sous examen illustrant les conclusions et recommandations formulées par la Commission européenne, eu égard aux questions qui se posent relatives à la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux Etats-Unis.

Les recommandations devront servir de base à la discussion portant sur ces questions relatives à la protection des données à caractère personnel entre les Etats-Unis et la Commission européenne, représentant les Etats membres de l'Union européenne. Il est prévu que lesdites discussions se terminent d'ici à l'automne 2014.

Il est également affirmé que les normes de protection des données ne feront pas partie des points abordés au sens strict dans le cadre des négociations en cours en vue d'un partenariat transatlantique de commerce et d'investissement. En effet, dans ce cadre il est souligné qu'il ne sera pas transigé sur les niveaux de protection existants au niveau européen pour parvenir à un accord, le haut niveau de protection garanti au sein de l'Union européenne n'étant pas négociable. Il est néanmoins relevé qu'il s'avère cependant difficile d'en faire abstraction complète au cours des négociations dudit accord commercial.

[A titre de rappel : Cet accord commercial devra permettre d'« éliminer les obstacles au commerce (tarifs douaniers, réglementations superflues, restrictions aux investissements, etc.) dans un large éventail de secteurs économiques, de manière à faciliter l'achat et la vente de biens et services entre l'Union européenne et les Etats-Unis, qui souhaitent

également que leurs entreprises respectives puissent investir plus facilement dans l'autre économie. »^{1]}

Explications par M. le Président de la Commission nationale pour la protection des données (ci-après la « CNPD »)

M. le Président de la Commission nationale pour la protection des données soulève que la CNPD est actuellement poursuivie devant le Tribunal administratif luxembourgeois dans une affaire l'opposant à un activiste du groupe de défense des droits à la protection des données « *Europe versus facebook* ».

En effet, à la suite des révélations d'Edward Snowden, la CNPD avait reçu deux demandes de vérification de la licéité des traitements mis en œuvre par les sociétés Skype et Microsoft, ayant leur siège européen au Luxembourg. Suite à des investigations menées auprès de Skype et Microsoft, la CNPD n'avait pas constaté de violations en matière de protection des données de la part des deux sociétés susmentionnées. L'un des deux requérants (à savoir un étudiant autrichien, M. Max Schrems, déjà en procès avec Facebook qu'il accuse d'enfreindre les règles de protection des données) ne s'est pas contenté de cette décision et a par conséquent décidé de poursuivre la CNPD devant le Tribunal administratif.²

3. Echange de vues au sujet des deux arrêts de la Cour de Justice de l'Union européenne suivants:

C-293/12 - Digital Rights Ireland et Seitlinger e.a.

Arrêt de la Cour (grande chambre) du 8 avril 2014. Digital Rights Ireland Ltd (C-293/12) contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung (C-594/12) et autres. Demandes de décision préjudicielle: High Court - Irlande, Verfassungsgerichtshof - Autriche. Communications électroniques - Directive 2006/24/CE - Services de communications électroniques accessibles au public ou de réseaux publics de communications - Conservation de données générées ou traitées dans le cadre de la fourniture de tels services - Validité - Articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne. Affaires jointes C-293/12 et C-594/12

C-131/12 - Google Spain et Google

Arrêt de la Cour (grande chambre) du 13 mai 2014. Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González. Demande de décision préjudicielle: Audiencia Nacional - Espagne. Données à caractère personnel - Protection des personnes physiques à l'égard du traitement de ces données - Directive 95/46/CE - Articles 2, 4, 12 et 14 - Champ d'application matériel et territorial - Moteurs de recherche sur Internet - Traitement des données contenues dans des sites web - Recherche, indexation et stockage de ces données - Responsabilité de l'exploitant du moteur de recherche - Établissement sur le territoire d'un État membre - Portée des obligations de cet exploitant et des droits de la personne concernée - Charte des droits fondamentaux de l'Union européenne - Articles 7 et 8. Affaire C-131/12

¹ « *In focus: Transatlantic Trade and Investment Partnership (TTIP)* » - « *Questions fréquentes* », in <http://ec.europa.eu>, consulté en juillet 2014 (http://ec.europa.eu/trade/policy/in-focus/ttip/questions-and-answers/index_fr.htm).

² « *La charge de Schrems contre le Luxembourg* », *Le Quotidien*, 17 juin 2014.

A titre liminaire, Mme la Présidente de la Commission juridique rappelle qu'au cours de la réunion jointe des deux commissions du 2 juillet 2014, le Ministre des Communications et des Médias, M. Xavier Bettel et le Ministre de la Justice, M. Félix Braz, ont fait connaître la position du Gouvernement, suite aux deux arrêts *C-293/12 - Digital Rights Ireland et Seitlinger e.a.* et *C-131/12 - Google Spain et Google* de la Cour de Justice de l'Union européenne. Cette présentation de la situation actuelle a été suivie d'un échange de vues qui est poursuivi lors de la présente réunion.

Madame la Présidente rappelle que trois solutions sont envisageables :

- au niveau européen, l'élaboration d'une nouvelle proposition de directive par la Commission européenne. (A cet égard, il est précisé que ces travaux n'avancent guère au niveau du Conseil des Ministres JAI) ;
- au niveau national, soit l'adaptation ponctuelle du cadre légal (les mesures nationales de transposition de la directive devront être modifiées si elles contiennent des dispositions proches de celles de la directive désormais invalidée),
- soit la suppression pure et simple du chapitre relatif à la conservation des données à caractère personnel figurant dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

A. C-293/12 - Digital Rights Ireland et Seitlinger e.a. (ci-après « l'arrêt »)

A titre de rappel, le 8 avril 2014, la Cour de Justice de l'Union européenne, saisie de plusieurs recours par le « *High Court* » (Irlande) et le « *Verfassungsgerichtshof* » (Autriche) visant à examiner la validité à l'égard de la directive 2006/24/CE du 15 mars 2006 sur la conservation des données, l'avait déclarée invalide, entre autres en raison du fait que « *l'ingérence vaste et particulièrement grave de cette directive dans les droits fondamentaux en cause n'est pas suffisamment encadrée afin de garantir que cette ingérence soit effectivement limitée au strict nécessaire* ». En effet, cette directive a pour objectif principal d'harmoniser les dispositions des Etats membres sur la conservation de certaines données générées ou traitées par les fournisseurs de services de communications électroniques.

Cette directive vise à garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite des infractions graves, notamment les infractions liées à la criminalité organisée et au terrorisme, en prévoyant l'obligation pour les fournisseurs précités de conserver un certain nombre de données de leurs clients pour une durée de 6 à 24 mois.

Il convient de renvoyer à la loi du 18 juillet 2014 par laquelle le Luxembourg a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 ainsi que le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination de certains actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 18 janvier 2003 (ci-après « *la Convention de Budapest* »).

Le système instauré par la Convention de Budapest prévoit une procédure en deux étapes, à savoir (I) la conservation des données pendant une certaine période et (II) la faculté de saisir ces données suivant les procédures de droit.

Quant à la conservation rapide de données informatiques stockées, le nouvel article 48-25 du Code d'instruction criminelle dispose que :

« Lorsqu'il y a des raisons de penser que des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, le procureur d'Etat ou le juge d'instruction saisi peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, de ces données ».

Quant à la saisie des données informatiques, cette dernière peut être ordonnée directement ou à la suite d'une demande de conservation rapide de données.³

Il échet de noter que d'un point de vue de la hiérarchie des normes juridiques, les conventions internationales se situent au-dessus de la loi nationale. Ainsi, la question qui s'ensuit est de savoir si les dispositions de la Convention de Budapest concernant la conservation de données sont conformes aux exigences de la jurisprudence se dégageant de l'arrêt C-293/12 – Digital Rights Ireland et Seitlinger e.a.

Explications de M. le Procureur général d'Etat

L'orateur s'interroge quant à l'effet de la décision de la Cour de Justice de l'Union européenne, invalidant la directive en tant que telle, et les incidences consécutives sur notre législation.

Il est constant que la loi modifiée du 30 mai 2005 transposant en droit luxembourgeois la directive européenne 2006/24/CE du 15 mars 2006 (ci-après « la directive »), a une existence propre et distincte par rapport à la directive invalidée par la Cour de Justice de l'Union européenne, de sorte qu'elle continue à s'appliquer. Il s'avère cependant nécessaire de vérifier si cette loi répond aux exigences posées par la Cour de Justice de l'Union européenne.

L'orateur met l'accent sur la nécessité d'une réglementation harmonisée au niveau européen, tout en constatant qu'une telle réglementation n'est guère envisageable dans un prochain temps. Or, une coopération policière et judiciaire s'avère difficile dans le cas de figure d'une disparité des règles de fond des différents Etats membres. Il s'ensuit qu'une harmonisation du cadre juridique européen en matière de protection des données s'impose.

M. le Procureur général d'Etat estime que la Convention de Budapest est dorénavant sans objet. En effet, en cas d'interprétation stricte de l'arrêt, ladite Convention ne trouve pas application. Ainsi, il ne sera plus possible d'obtenir accès à des données susceptibles de constituer un élément de preuve notamment pour un acte de délinquance de nature raciste et xénophobe commis par le biais de systèmes informatiques. Il s'ensuit que la constatation d'une infraction s'avère difficile. A noter que la Convention de Budapest a été élaborée à une période avant l'arrêt rendu par la Cour de Justice de l'Union européenne. Il se pose dès lors la question de savoir si l'invalidation de la directive prévaut sur les dispositions contenues dans la Convention de Budapest.

Par ailleurs, l'orateur donne à considérer que l'arrêt de la Cour de Justice de l'Union européenne pourrait également avoir un impact sur d'autres instruments européens et nationaux concernant la rétention des données et l'accès à ces données par les autorités (notamment le Centre des technologies de l'information de l'Etat (CTIE), les Recommandations du GAFI n°11 ou encore la troisième directive anti-blanchiment du 26 octobre 2005). Il ne plaide pas pour une suppression pure et simple de la rétention des

³ Pour de plus amples informations veuillez notamment consulter le site internet www.droit.lu, le portail du droit luxembourgeois.

données, mais se prononce en faveur d'une sélectivité des instruments autorisant une rétention.

Une autre interrogation qui s'impose est l'appréciation, au moment où on opère la rétention des données de la pertinence des données aux fins de poursuite des infractions. Une sélection des données à retenir dès le départ n'est guère réalisable en pratique.

Dans ce même ordre d'idées, si l'orateur se prononce en faveur de l'établissement d'un catalogue d'infractions, plutôt que de fixer un seuil de peine d'emprisonnement, il donne cependant à considérer que la solution de l'établissement d'une liste des infractions graves ne s'avère guère satisfaisante en pratique, et ce notamment au vu du fait que l'établissement d'une telle liste conduit automatiquement à une exclusion des infractions ne tombant pas dans le champ d'application de cette liste (comme par exemple le délit de harcèlement). En outre, une telle liste nécessitera constamment des mises à jour.

L'orateur donne à considérer que la transmission ou l'utilisation de données à caractère personnel a donné lieu à 3518 ordonnances nationales et 170 entraides judiciaires pour les années 2012, 2013 et 2014 en cours.

Explications par M. le Premier Ministre, Ministre d'Etat

M. le Premier Ministre, quant à la question relative au principe de la double incrimination dans le cadre du mandat européen⁴, informe les membres des deux commissions que ce principe n'est pas absolu. En effet, les infractions pouvant donner lieu à la remise sans contrôle préalable de la double incrimination du fait sont nombreuses⁵, et ce sous condition toutefois qu'elles soient punies dans l'Etat membre d'émission par une peine d'au moins trois ans.⁶

L'orateur se prononce aussi en faveur de l'établissement d'un catalogue d'infractions pour lesquelles l'article 67-1 du Code d'instruction criminelle (premier alinéa) permet l'accès aux données personnelles plutôt que d'opter pour la détermination d'un seuil de peine d'emprisonnement.

Explications par M. le Ministre de la Justice

M. le Ministre de la Justice plaide également pour l'établissement d'un catalogue d'infractions nécessitant des adaptations régulières au lieu de déterminer un seuil de peine d'emprisonnement.

L'orateur estime que le problème essentiel du dossier sous examen consiste en ce qu'il comporte deux volets, à savoir une dimension nationale et une dimension européenne. Toute modification éventuelle de la loi nationale concernée sera conditionnée par les initiatives éventuellement à prendre et les travaux menés au sein de l'UE. Par conséquent, M. le Ministre de la Justice se prononce en faveur d'une adaptation ponctuelle de la législation nationale, alors que l'élaboration d'un nouveau cadre légal avant tout progrès au niveau européen risque de conduire à des contradictions.

⁴ (En vertu duquel la remise est subordonnée à la condition que le fait pour lequel est demandée la remise constitue une infraction en application du droit de l'Etat membre d'exécution.)

⁵ (Le terrorisme, la traite des êtres humains, la corruption, la participation à une organisation criminelle, le faux monnayage, l'homicide, le racisme et la xénophobie, le viol, le trafic de véhicules volés, la fraude, y compris la fraude aux intérêts financiers de l'Union.)

⁶ « *Mandat d'arrêt européen* », in <http://europa.eu>, consulté en juillet 2014 (http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/1331_67_fr.htm).

L'orateur souligne que le Luxembourg plaide au niveau européen clairement pour l'élaboration d'un nouveau cadre légal européen.

Dans ce contexte, l'orateur donne à considérer qu'il est important pour le Luxembourg de fixer et d'exposer sa position à ce sujet, notamment au égard au fait que le volet de la conservation des données à caractère personnel sera un thème de prédilection lors de la Présidence de l'Union européenne par le Luxembourg (2^e semestre de 2015).

Au niveau européen, l'orateur préconise de privilégier l'adoption d'une nouvelle directive en vue de remplacer la directive invalidée.

Quant à la question de l'incidence de l'arrêt sur la collecte de données personnelles par des opérateurs, M. le Ministre de la Justice donne à considérer que ce volet n'est pas concerné par l'arrêt. En effet, la collecte de données personnelles par un opérateur se fait dans le cadre de l'affectation d'une relation contractuelle soumise à une réglementation stricte.

Explications par M. le Président de la Commission nationale pour la protection des données

L'orateur se prononce en faveur d'une définition plus précise et restrictive de la notion de « *criminalité grave* ». Dans ce cadre il apparaît préférable aux yeux de la CNPD d'établir une liste d'infractions. En effet, une énumération limitative permettrait de réserver l'accès aux données pour les besoins d'enquête et de poursuites judiciaires visant des infractions qui se situent clairement dans le contexte du terrorisme et de la criminalité organisée ou de poursuites d'infractions dont le degré de gravité permet de les y assimiler.

A noter qu'en l'état actuel, l'article 67-1, alinéa 1^{er} du Code d'instruction criminelle autorise l'accès aux données pour des faits susceptibles d'emporter une peine criminelle ou correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. La CNPD estime que ce taux est trop bas pour correspondre à l'objectif fixé de prévention et poursuite de la criminalité grave et de la lutte contre le terrorisme et la criminalité internationale organisée.

En outre, l'orateur signale qu'il existe déjà une sorte de filtre au Luxembourg. Il n'est en effet pas possible pour la police d'accéder directement à ces données auprès des opérateurs téléphoniques ou de réseaux internet. Une ordonnance du juge d'instruction est nécessaire pour accéder à ces données. L'orateur souligne que ceci constitue déjà une protection importante, qui fait cependant défaut dans d'autres pays de l'Union européenne.⁷

M. le Président de la CNPD se prononce en faveur d'une adaptation ponctuelle du cadre légal au niveau national, tout en soulignant cependant que le choix d'adapter ponctuellement le cadre légal ou de supprimer tout simplement le chapitre relatif à la conservation des données à caractère personnel dans la loi modifiée du 2 août 2002, est une décision purement politique.

Il insiste également sur le fait qu'une harmonisation du cadre juridique européen en matière de protection des données s'impose. (A l'état actuel l'Angleterre semble se prononcer en faveur d'une adaptation de la législation nationale, tandis que d'autres pays comme l'Autriche ont annoncé préconiser la suppression de la rétention des données.)

*

⁷ Pour de plus amples informations veuillez notamment consulter l'avis de la CNPD du 26 avril 2010 (Délibération n°85/2010), ainsi que l'avis de la CNPD du 13 mai 2014 (Délibération n°214/2014).

Echange de vues

Des membres du groupe politique CSV partagent l'avis de la CNPD et plaident pour une adaptation ponctuelle de la législation luxembourgeoise et non pour une suppression pure et simple du chapitre relatif à la conservation des données à caractère personnel dans la loi modifiée du 2 août 2002. En outre, ils se prononcent pour l'établissement d'un catalogue d'infractions.

Un membre du groupe politique LSAP souligne qu'un catalogue d'infractions restrictif n'a de sens que s'il est exhaustif.

En même temps, il se prononce pour un encadrement plus strict de la conservation des données.

En outre, il estime que l'ordonnance du juge d'instruction requise au Luxembourg pour accéder à ces données constitue déjà une protection importante. Par ailleurs, il attache une importance primordiale au respect d'une stricte nécessité et du critère de proportionnalité.

Un membre de la sensibilité politique déi Lénk se prononce contre une collecte massive et indifférenciée de données indépendamment de tout soupçon. Dans ce contexte il donne à considérer que l'exigence de l'existence d'un soupçon concret ne semble guère compatible avec l'établissement d'un catalogue d'infractions.

Par ailleurs, la sensibilité politique déi Lénk favorise aussi une adaptation ponctuelle de la législation nationale. Toutefois, l'orateur donne à considérer qu'il s'avère nécessaire de prévoir une solution transitoire dans l'attente d'une adaptation de la législation nationale.

Dans ce cadre, il souhaite recevoir du gouvernement de plus amples informations quant aux adaptations législatives nécessaires à entreprendre.

B. C-131/12 - Google Spain et Google

En l'occurrence, une personne de nationalité espagnole avait constaté, en renseignant son nom dans le formulaire de requête du moteur de recherche Google, que ses données personnelles étaient disponibles sur le site d'un quotidien qui faisait état d'une vente aux enchères immobilière liée à une saisie pratiquée en recouvrement de ses dettes de sécurité sociale.

Dans un premier temps, la personne concernée s'est adressée aux sociétés Google Spain et Google Inc. pour leur demander de supprimer ses données, mais ce sans succès.

Par conséquent, elle s'est ensuite adressée à l'agence espagnole de protection des données (l'«*AEPD*»), qui a ordonné aux sociétés Google Spain et Google Inc. le retrait des données en supprimant les liens litigieux. Ces dernières ont formé un recours devant la juridiction supérieure espagnole (l'«*Audiencia Nacional*»). Celle-ci a saisi la Cour de Justice de l'Union Européenne d'une série de questions préjudicielles, notamment relatives à la question des obligations qui incombent aux exploitants de moteurs de recherche concernant la protection des données à caractère personnel des personnes souhaitant invoquer un droit à l'oubli.

Explications par M. le Président de la Commission nationale pour la protection des données

A titre liminaire, l'orateur tient à soulever que la décision de la Cour de Justice de l'Union européenne constitue un pas important pour le renforcement de la protection des données personnelles des citoyens européens. Par ailleurs, il estime que l'arrêt ne sera probablement pas sans incidence sur la législation nationale.

L'orateur relève qu'une des questions préjudicielles posées à la Cour de Justice de l'Union européenne a porté sur la reconnaissance d'un droit à l'oubli numérique des informations ayant fait l'objet de publications sur des sites web tiers et pour lesquelles les moteurs de recherche ne font que référencer le contenu desdits sites internet.

Dans son arrêt, la Cour de Justice de l'Union européenne reconnaît à la personne concernée un «*droit à l'oubli*» pour autant que plusieurs critères soient remplis, à savoir notamment qu'elle puisse démontrer que le fait de rechercher son nom sur un moteur de recherche conduit à des informations pouvant lui porter préjudice.

En outre, s'agissant du champ d'application territorial de la directive, l'orateur constate que la Cour retient que Google Inc., une société américaine, qui effectue la majeure partie des traitements de données personnelles est soumise à la législation européenne en matière de protection des données personnelles, et ce au vu du fait que sa filiale espagnole Google Spain est établie sur le territoire de l'Union européenne. Il s'agit donc d'un «*établissement*» au sens de la directive. En effet, la Cour de Justice de l'Union européenne considère que le traitement des données est effectué dans le cadre des activités de la société Google Spain, ayant en charge les activités de commercialisation de publicité ciblée aux habitants de l'Espagne.

Ainsi, la Cour de Justice de l'Union européenne a soutenu une interprétation très large du critère de rattachement, à savoir que si le traitement de données personnelles est nécessaire à l'activité de la société désignée comme étant responsable (aux Etats-Unis en l'occurrence) et qu'un établissement de cette même société en Europe participe à cette activité, on pourra considérer que le traitement de données personnelles est opéré dans le cadre des activités de l'établissement européen et ce sans qu'il soit nécessaire qu'il existe un rapport spécifique avec le traitement de données personnelles lui-même.

Pour l'orateur il s'agit d'une motivation très artificielle.

En outre, il est relevé que pour se mettre en conformité avec l'arrêt, la société Google a mis en place un formulaire destiné aux clients dans l'Union européenne qui veulent demander la suppression de liens vers des pages contenant des données personnelles, formulaire qui peut être téléchargé sur le site internet suivant : https://support.google.com/legal/contact/lr_eudpa?product=websearch.

A noter à cet égard qu'une telle demande de suppression doit encore être justifiée. Plus précisément, le «*droit à l'oubli*» est soumis à plusieurs conditions. En effet, «*la Cour relève que, s'il est constaté, suite à une demande de la personne concernée, que l'inclusion de ces liens dans la liste est, au stade actuel, incompatible avec la directive, les informations et liens figurant dans cette liste doivent être effacés. La Cour observe à cet égard que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque, eu égard à l'ensemble des circonstances caractérisant le cas d'espèce, ces données apparaissent inadéquates, pas ou plus*

pertinentes ou excessives au regard des finalités pour lesquelles elles ont été traitées et du temps qui s'est écoulé. La Cour ajoute que, dans le cadre de l'appréciation d'une telle demande introduite par la personne concernée à l'encontre du traitement réalisé par l'exploitant d'un moteur de recherche, il convient notamment d'examiner si cette personne a un droit à ce que les informations en question relatives à sa personne ne soient plus, au stade actuel, liées à son nom par une liste de résultats qui est affichée à la suite d'une recherche effectuée à partir de son nom. Si tel est le cas, les liens vers des pages web contenant ces informations doivent être supprimées de cette liste de résultats, à moins qu'il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations. »⁸

A relever que d'un point de vue juridique la personne concernée dispose de deux bases légales pour demander la suppression, respectivement pour faire valoir son « droit à l'oubli », à savoir (I) l'article 12, sous b) (effacement pour donnée illicite), et (II) l'article 14, premier alinéa, sous a) (droit d'objection), de la directive 95/46 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.

A cet égard, l'orateur tient encore à préciser que dans les deux premiers mois suivant l'arrêt sous examen quelque 70.000 demandes de suppression de 270.000 liens ont été enregistrées.

Par ailleurs, la CNPD est actuellement en concertation avec les opérateurs, en vue de les inciter à uniformiser leurs formulaires.

L'orateur soulève qu'il existe un risque que les sociétés proposant un moteur de recherche, tel que Google, Microsoft ou encore Bing, se déclarent incapables au vu du volume des demandes leur adressées) pour l'évaluation des demandes, pour s'en adresser aux Commissions nationales de protection des données et leur demander de les vérifier.

La CNPD publiera (au courant du mois de septembre) sa position quant aux modalités pratiques des demandes de suppression. En tout état de cause les citoyens luxembourgeois désireux de faire valoir ce « droit à l'oubli », ont toujours la faculté de s'adresser à la CNPD si une demande de suppression adressée à la société exploitant le moteur de recherche est restée infructueuse.

D'après l'orateur, si l'arrêt n'est pas susceptible de différentes interprétations, il y a cependant un potentiel de confusion chez le grand public au niveau du champ d'application dudit arrêt. Il souligne que sont seulement visés les moteurs de recherche et non les réseaux sociaux.

Finalement, l'orateur constate que l'arrêt ne fait qu'une application correcte des dispositions de la directive de 95/46 du 24 octobre 1995 qui aurait dû être appliquée dans ce sens dès le début.

Quant à la question de savoir si une personne dispose d'un droit d'exiger la suppression de liens dans les pages de résultats d'un moteur de recherche et ce alors même qu'il s'agirait d'informations publiées légalement par des tiers, l'orateur souligne que la Cour a répondu en principe par l'affirmative, sauf en cas de « raisons particulières, telles que le rôle joué par

⁸ « L'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers », communiqué de presse n°70/14, Cour de Justice de l'Union européenne, in <http://curia.europa.eu>, 13 mai 2014, consulté en juillet 2014. (<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf>)

ladite personne dans la vie publique» (point 99 de l'arrêt). L'orateur note que le terme « *information* » vise également les photos en tant que telles.

M. le Président de la CNPD estime qu'une publication illicite, pour autant que le caractère illicite soit suffisamment prouvé, ouvre droit à une demande d'indemnisation à intenter contre le site internet diffusant les informations.

Un expert gouvernemental informe qu'une réforme globale des règles adoptées par l'UE en 1995 en matière de protection des données a été élaborée par la Commission européenne en janvier 2012. Il note à cet égard que si le « *droit à l'oubli* » a effectivement déjà été envisagé dans la proposition de texte initiale, il est toutefois considéré qu'il serait mieux rendu compte d'un tel principe dans un article séparé. L'orateur relève que le groupe de travail, travaillant actuellement sur une nouvelle proposition de texte estime qu'il conviendrait d'examiner une éventuelle généralisation de l'application du « *droit à l'oubli* ».

Par ailleurs, l'expert gouvernemental souligne qu'il résulte de l'arrêt que le « *droit à l'oubli* » n'est pas un droit absolu, mais devra toujours être mis en balance avec d'autres droits fondamentaux, notamment la liberté d'expression et la liberté des médias. En effet, la Cour de Justice de l'Union européenne estime à cet égard que « *dans la mesure où la suppression de liens de la liste de résultats pourrait, en fonction de l'information en cause, avoir des répercussions sur l'intérêt légitime des internautes potentiellement intéressés à avoir accès à l'information en question, la Cour constate qu'il y a lieu de rechercher un juste équilibre notamment entre cet intérêt et les droits fondamentaux de la personne concernée, en particulier le droit au respect de la vie privée et le droit à la protection de données à caractère personnel. La Cour relève à cet égard que, si, certes, les droits de la personne concernée prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à recevoir cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.* »⁹

4. Divers

La prochaine réunion de la Commission juridique aura lieu le 24 septembre 2014.

Le secrétaire-administrateur,
Tania Sonnetti

La Présidente de la Commission juridique,
Viviane Loschetter

Le Président de la Commission de
l'Enseignement supérieur, de la Recherche,
des Médias, des Communications et de
l'Espace,
Simone Beissel

⁹ « *L'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers* », communiqué de presse n°70/14, Cour de Justice de l'Union européenne, in <http://curia.europa.eu>, 13 mai 2014, consulté en juillet 2014. (<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf>)

