Commission consultative des Droits de l'Homme
du Grand-Duché de Luxembourg

Avis

sur

le projet de loi 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Avis 5/2015

Conformément à l'article 2(1) de la loi du 21 novembre 2008 portant création d'une Commission consultative des droits de l'Homme au Grand-Duché de Luxembourg, la Commission consultative des droits de l'Homme (CCDH) a été saisie par le Gouvernement pour émettre un avis sur le projet de loi 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

I) Considérations générales

Par son arrêt du 8 avril 2014[1], la Cour de justice de l'Union européenne (CJUE) a invalidé la directive 2006/24/CE relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, en s'appuyant sur les dispositions de la Charte des droits fondamentaux de l'Union européenne.

Il s'agit d'une décision clé, qui ne s'oppose pas seulement à la conservation générale et indifférenciée des données dans le cadre de la fourniture de services de communications électroniques, mais qui a aussi un impact sur de nombreuses autres mesures de conservation des données dans l'Union européenne[2].

Au Luxembourg, la directive 2006/24/CE a été transposée par la loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle[3] et cette loi du 30 mai 2005 a encore été modifiée par la loi du 28 juillet 2011.[4]
Avant l'adoption de cette loi de 2010, la CCDH a adressé ses observations au législateur dans son avis 02/2010[5].
Dans son arrêt dit « Digital Rights », la CJUE a jugé que la directive 2006/24 comporte « *une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* » (point 65). Elle a en outre posé plusieurs

[1]CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12
[2]Pour plus d'informations, voir : Prof. Dr. Franziska Boehm and Prof. Dr. Mark D. Cole, Data Retention after the Judgement of the Court of Justice of the European Union (30.6.2014), disponible sur http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/Data/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
[3]Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle, Mémorial A, n°122, 29 juillet 2010
[4]Projet de loi portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle
[5]CCDH avis 02/2010 sur le projet de loi 6113

exigences relatives aux mesures de sécurité nécessaires pour assurer la protection des données conservées.
Le présent projet de loi a pour objectif d'adapter la législation luxembourgeoise à ces exigences.

Alors que la directive européenne a été invalidée par la CJUE, les législations nationales restent en place et continuent à être appliquées. Voilà pourquoi la CCDH salue l'initiative du Gouvernement luxembourgeois de réagir comme un des premiers pays à cet arrêt de la CJUE en modifiant la législation actuelle, sans attendre les réactions au niveau de l'Union européenne.
Afin d'offrir une protection plus élevée aux citoyens, il n'en demeure pas moins qu'une position unifiée au niveau européen reste indispensable. A ce titre, la CCDH rappelle au Gouvernement l'engagement qu'il a pris de mettre la question sur l'agenda européen lors de la présidence luxembourgeoise du Conseil de l'Union européenne[6] à défaut d'initiative de la part de la Commission européenne.[7]

Cependant, la CCDH regrette que le projet de loi se limite à des modifications ponctuelles et n'aborde pas du tout la question principale du maintien ou de l'abandon du principe même de la rétention des données, qui a pourtant été le sujet de nombreux débats en Europe.

1. Nécessité et utilité de la rétention des données

La conservation des données « *concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves* » .(point 58)
Elle place ainsi toute la population sous une sorte de soupçon généralisé et constitue une ingérence grave dans l'exercice du droit au respect de la vie privée et de la correspondance de toute personne. Or, une telle ingérence ne peut être justifiée que si elle est nécessaire, appropriée et proportionnée.

La Cour est arrivée à la conclusion que la directive poursuit le but légitime de la prévention des infractions et de la lutte contre la criminalité, mais que « *le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité »* (point 69).
La question de la nécessité, voire de l'utilité des mesures générales de conservation des données, n'a pas vraiment été analysée en profondeur dans l'arrêt « Digital Rights ». La CJUE note simplement que « *la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive* » (point 49).

[6] 2e semestre 2015
[7] http://www.europaforum.public.lu/fr/actualites/2015/02/gouv-chd-retention-donnees-cjue/index.html

Or, comme le souligne la professeure Marie Laure Basilien Gainche « *si l'on peut saluer le fait que le juge de Luxembourg n'ait pas considéré l'outil indispensable, on peut toutefois déplorer qu'il n'interroge pas un instant la prétendue utilité - pourtant sujette à caution - de la conservation des données électroniques pour lutter contre la criminalité organisée et le terrorisme* »[8]
Ce sujet a pourtant été vivement discuté par de nombreux experts en matière de protection des données, et ceci aussi bien avant[9] qu'après[10] l'adoption de la directive 2006/24/CE.

Un point qui est souvent relevé est le manque de preuves limpides pour démontrer la nécessité de la conservation systématique et obligatoire des données électroniques. Ainsi, le rapport d'évaluation concernant la directive 2006/24/CE publié en 2011 par la Commission européenne[11], qui est arrivé à la conclusion que « *la conservation de données est très utile aux systèmes de justice pénale et aux services répressifs de l'UE* », a été fortement critiqué[12] par le Contrôleur européen de la protection des données, qui a estimé que « *la Commission se base principalement sur des déclarations des États membres sur leur perception de la conservation des données comme étant un outil nécessaire aux fins de la répression. Ces déclarations, cependant, indiquent plutôt que les États membres concernés sont heureux d'avoir des règles de l'UE sur la conservation des données* »[13], mais que « *les informations quantitatives et qualitatives fournies par les États membres ne sont pas suffisantes pour confirmer la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données* »[14].

---

[8]Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 12 mai 2015. URL : http://revdh.revues.org/746

[9]Groupe de travail «ARTICLE 29» sur la protection des données, Avis 4/2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE(COM(2005)438 final du 21.09.2005), disponible sur http://www.cnpd.public.lu/fr/publications/groupe-art29/wp113_fr.pdf
Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final], JO C 298 du 29.11.2005

[10]Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)(2011/C 279/01) ;
Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", European Journal of Law and Technology, Vol. 1, Issue 3, 2010 ; Voir aussi la lettre datée du 22 juin 2010 d'un groupe important d'organisations de la société civile aux commissaires Malmström, Reding et Kroes, http://www.vorratsdatenspeicherung.de/content/view/363/158/lang,en

[11]Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE) (COM(2011) 225 final)

[12]Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE) (2011/C 279/01)

[13]Point 41 du texte p. 5

[14]Point 44 du texte p 6

Dans le même ordre d'idées, il y a lieu de soulever l'exemple de l'Allemagne, qui est un des pays où la loi nationale transposant la directive 2006/24/CE a été déclarée inconstitutionnelle[15].
Suite à cette décision de la Cour constitutionnelle, le ministre allemand de la Justice a décidé d'abandonner la conservation des données et a publié un rapport, réalisé par le Max-Planck Institut[16], sur les conséquences de la suppression de cette conservation des données. Ce rapport est arrivé à la conclusion que l'absence d'une législation prévoyant la rétention des données n'a pas eu comme résultat une chute du nombre d'enquêtes criminelles résolues.

2. Mesures alternatives

Dans le cadre de cette discussion sur la nécessité de la conservation des données, il faut aussi considérer d'autres mesures utiles à prendre en compte à des fins d'enquête qui pourraient s'avérer comme des alternatives, car moins intrusives dans la vie privée.
Le principal moyen alternatif qui est souvent invoqué est la conservation rapide des données (gel immédiat ou gel rapide). Cette méthode prévoit de *« conserver temporairement ou de «geler» certaines données de trafic des télécommunications et de localisation portant uniquement sur des personnes déterminées soupçonnées d'activités criminelles, qui peuvent par la suite être mises à la disposition des autorités répressives avec une autorisation judiciaire* ».[17]
Cette conservation rapide des données informatiques a été introduite en droit luxembourgeois par la loi du 18 juillet 2014[18], par laquelle le Luxembourg a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité, et par son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.
La conservation rapide des données « *ne garantit pas la possibilité de remonter en amont de l'injonction, pas plus qu'elle ne permet de recueillir des preuves sur les mouvements des victimes ou des témoins d'une infraction, par exemple* »[19] et elle n'est utile que dans des situations où un suspect a été identifié. Cette méthode ne permet donc pas d'obtenir autant d'informations que le système général de la conservation des données, mais c'est exactement à cause de sa nature plus ciblée qu'elle est souvent

[15] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, jugement du 2 mars 2010, disponible sur http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html
[16] Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung, http://vds.brauchts.net/MPI_VDS_Studie.pdf
[17] Définition donnée dans l'avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE) (2011/C 279/01), point 54
[18] Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, Mémorial A n°133, 25 juillet 2014
[19] Rapport d'évaluation concernant la directive sur la conservation des données, p.6

jugée moins attentatoire aux droits fondamentaux.[20] Avant d'exclure cette méthode, parce qu'elle ne constitue pas une alternative exactement équivalente, il serait opportun de voir si elle pourrait produire des résultats comparables.
La CCDH estime qu'il faudrait évaluer si la conservation des données est non seulement utile pour les enquêtes criminelles, mais effectivement un outil absolument indispensable pour la lutte contre le terrorisme et la criminalité organisée et si des résultats comparables pourraient être obtenus avec des alternatives moins intrusives dans la vie privée de la population totale. Ces questions mériteraient indubitablement une discussion approfondie au Luxembourg, à l'instar d'autres pays européens comme l'Allemagne.

En attendant les développements futurs au niveau national aussi bien qu'au niveau européen, il est essentiel de limiter le champ d'application de la conservation des données au strict minimum et d'instaurer des contrôles suffisants permettant de protéger efficacement les données à caractère personnel contre les risques d'abus et les utilisations illicites.

II) Analyse du projet de loi par la CCDH

1. Liste limitative d'infractions graves

Dans son article 1er, le projet de loi sous avis propose de remplacer à l'article 67-1 du Code d'instruction criminelle le seuil de peine des infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs (infractions prévoyant une peine privative de liberté dont le maximum est égal ou supérieur à un an) par une liste précise d'infractions .
La CCDH avait déjà recommandé dans son avis 02/2010[21] sur le projet de loi 6113 d'opter pour une liste d'infractions bien concise au lieu de la définition d'un seuil minimal de peine prévue.
La Commission nationale pour la protection des données (CNPD) avait aussi opté en faveur d'une liste d'infractions.[22]

Alors qu'en 2010, le législateur n'avait pas retenu cette recommandation, les auteurs du présent projet de loi ont choisi d'intégrer une liste d'infractions dans l'article 67-1 du Code d'instruction criminelle.

[20]Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données
[21]CCDH avis 02/2010 sur le projet de loi 6113
[22]Avis de la Commission nationale pour la protection des données sur le projet de loi et sur le projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics, 26 avril 2010, http://www.cnpd.public.lu/fr/decisions-avis/2010/retention-donnes/avis_CNPD_projet_loi_6113.pdf

Or, il s'agit en l'espèce d'une liste assez extensive qui comprend 33 infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs.
Cette liste contient entre autres des infractions comme le trafic illicite de biens culturels, les infractions contre l'environnement, l'incendie volontaire, le harcèlement et les atteintes à la vie privée, les homicides et coups et blessures volontaires.

Il convient de rappeler que dans son arrêt « Digital Rights », la CJUE a souligné que la conservation des données, telle que prévue par la directive 2006/24/CE, comporte une ingérence dans les droits fondamentaux des citoyens européens *« sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* » (point 65). Et elle a noté qu'il faut prévoir des limitations à l'utilisation de ces données conservées « *concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence* » (point 60).

Dans son avis en 2010, la CCDH avait déjà proposé de se limiter aux infractions suivantes :
- Les actes de terrorisme prévus par les articles 135-1 à 135-16 du Code pénal,
- L'association de malfaiteurs et le crime organisé, tels que prévus par les articles 322 et suivants du Code pénal, ainsi que la circonstance aggravante de l'association de malfaiteurs prévue spécifiquement en matière de trafic de stupéfiants par la loi modifiée du 19 février 1973, concernant la lutte contre la toxicomanie.

Comme le projet de loi ainsi que les textes précédents (projet de loi 6113 et la directive 2006/24/CE) se placent dans un contexte de lutte contre le terrorisme et la criminalité organisée, la CCDH est d'avis que les infractions qui se trouvent sur la liste sous avis ne sont pas toutes « *suffisamment graves pour justifier une telle ingérence* ». Par conséquent, il vaudrait mieux limiter l'accès aux données conservées pour les infractions qui se situent clairement dans ce contexte et raccourcir cette liste pour ne garder que le strict nécessaire.

2. <u>La sécurité et la protection des données</u>

Dans l'arrêt précité, la CJUE émet plusieurs exigences pour les règles visant la sécurité des données conservées par les fournisseurs de services de communication électroniques, sachant que ces règles doivent permettre « *d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que tout accès et toute utilisation illicites de ces données* » (point 66).

a) Effacement des données à l'expiration du délai de rétention

La CCDH est satisfaite de constater que les auteurs du texte tiennent compte des exigences exprimées au point 67 de l'arrêt en proposant au point 2) de l'article 2 du projet de loi de modifier l'article 5 (1) (b) de la loi du 30 mai 2005 afin de préciser que

les données retenues doivent être effacées irrémédiablement et sans délai à l'expiration du délai de rétention. Il ne sera donc plus possible de sauvegarder ces données sous une forme anonymisée après la fin de la durée de rétention.

b) Conservation des données sur le territoire de l'Union européenne

Le point 4) de l'article 2 du projet de loi prévoit de modifier l'article 5-1 de la loi modifiée du 30 mai 2005 en créant l'obligation de conserver les données concernées par les articles 5 et 9 sur le territoire de l'Union européenne. Il s'agit d'une exigence exprimée au point 68 de l'arrêt de la CJUE, qui l'estime nécessaire afin de garantir le contrôle par une autorité indépendante. Ce contrôle constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel.

Or, les coûts de stockage des données pour les fournisseurs, surtout ceux d'une taille moyenne et petite, n'étant pas négligeables, il a souvent été proposé de réfléchir à accorder des compensations financières étatiques aux fournisseurs.[23] Dans ce contexte, il est important d'assurer un contrôle effectif du respect des obligations imposées aux fournisseurs.
La CCDH regrette de constater que la question de la sécurité des données n'est abordée que par renvoi à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à un règlement grand-ducal qui n'a d'ailleurs pas été soumis à l'avis de la CCDH.
Elle estime que les mesures de sécurité principales devraient être inscrites dans le présent projet de loi.

c) Augmentation des sanctions en cas de la violation des obligations

Les points 3) et 7) de l'article 2 du projet de loi proposent de modifier les articles 5(6) et 9(6) de la loi du 30 mai 2005 en vue d'augmenter les peines d'emprisonnement prévues. Celles-ci seront augmentées de « huit jours à un an » à « six mois à deux ans ».
Le commentaire précise que le but de cette modification est « *d'augmenter le caractère dissuasif de cette peine et de souligner ainsi l'importance accordée à la protection de ces données* ».
Il ne s'agit en l'espèce pas d'une revendication formelle de la CJUE, mais d'une initiative du Gouvernement.

Dans son avis en 2010, la CCDH a déjà insisté sur l'importance de sanctions (y compris de sanctions administratives et pénales) efficaces, proportionnées et dissuasives.

---

[23] Cecilia Malmström, « Taking on the Data Retention Directive », SPEECH/10/723, European Commission conference, Brussels, 3 December 2010 ; SURVEILLE, Comparative law paper on data retention regulation in a sample of EU Member States, 30.04.2013
Voir aussi la lettre datée du 22 juin 2010 d'un groupe important d'organisations de la société civile aux commissaires Malmström, Reding et Kroes,

Elle est satisfaite de constater que la loi de 2011 a introduit des sanctions administratives (avertissement et amende administrative) dans l'article 3 (3) de la loi de 2005, permettant ainsi à la CNPD de réagir en cas de manquement à l'obligation de notification des violations de données de la part du fournisseur.

Pourtant, elle estime qu'il ne suffit pas d'alourdir les sanctions afin de garantir la sécurité et la protection des données, comme le réclame la CJUE. Il est essentiel de garantir leur mise en œuvre effective en cas de violation de la loi.
D'ailleurs, afin de garantir un contrôle efficace de la protection des données, il importe d'accorder les moyens nécessaires à la CNPD, qui est responsable d'assurer le respect des dispositions de la loi modifiée du 30 mai 2005.

La CCDH entend formuler les recommandations suivantes :

1. Une évaluation de la nécessité absolue de la conservation des données doit être faite et des méthodes alternatives doivent être considérées.
2. La liste des infractions doit se limiter au strict nécessaire et inclure seulement des infractions qui se situent dans le contexte de la lutte contre le terrorisme et la criminalité organisée.
3. Des sanctions efficaces, proportionnées et dissuasives doivent effectivement être mises en œuvre.
4. La CNPD doit obtenir les moyens nécessaires pour effectuer un contrôle régulier du respect de la loi.