

Avis du Conseil de l'Ordre

Sur le projet de loi n°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

Le Conseil de l'Ordre a été invité à exprimer son avis sur un projet de loi ayant pour objet l'adaptation du dispositif légal national relatif à la conservation des données de communications électroniques à des fins de poursuite pénale.

Le Conseil de l'Ordre a pris connaissance de l'avis de la Chambre de Commerce du 13 février 2015, de l'avis de la Commission Nationale pour la Protection des Données du 19 juin 2015, de l'avis du Conseil d'Etat du 10 juillet 2015 et de l'avis de la Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg du 22 juillet 2015.

Le projet de loi fait suite à l'arrêt *Digital Rights*¹ rendu par la Cour de Justice de l'Union Européenne (CJUE) qui a jugé invalide la Directive 2006/24/CE sur 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.

Fruit du contexte post 11 septembre 2001, cette directive imposait notamment aux fournisseurs de services de communication électroniques de conserver, pour une durée allant de six à vingt-quatre mois, des données de trafic permettant d'identifier l'émetteur et le destinataire d'une communication, sa durée et localisation pour la recherche et la constatation d'infractions pénales graves. En revanche, elle n'autorise pas la conservation du contenu de la communication et des informations consultées. Or, « ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. »²

C'est donc dans son respect des droits fondamentaux, du droit au respect de la vie privée (article 7 de la Charte des Droits Fondamentaux de l'Union Européenne (la Charte)) et de celui de la protection des données à caractère personnel (article 8) que la validité de la Directive 2006/24/CE était mise en cause par la CJUE. Fondant son raisonnement sur la Charte des Droits Fondamentaux de l'Union Européenne la Cour a notamment jugé disproportionnée l'obligation de conservation des données qui s'applique de manière générale sans exiger un lien, fût-il indirect, entre la personne

¹ CJUE (gr. Ch.) 8 avril 2014, aff. Jtes C-293/12 et C-594/12, *Digital Rights Ireland Ltd & Kärntern Landesregierung, Seitlinger, Tschohl et a.*

² *ibid* point 27

dont les données sont conservées et un risque d'infraction³ (point sur lequel nous reviendrons dans le présent avis).

La CJUE fait également grief à la Directive 2006/24/CE de ne prévoir aucun critère permettant de délimiter l'accès des autorités nationales aux données⁴, ni aucune distinction entre les catégories de données, les personnes concernées ou quelque autre critère objectif quant à la durée de conservation⁵.

Le présent avis traitera dans un premier temps de la protection des personnes soumises selon les lois nationales au secret professionnel (I), puis émettra un avis sur le principe de collecte *a priori* et de conservation généralisées des données sans que la personne concernée ait participé directement ou indirectement à une infraction (II). Enfin le Conseil de l'Ordre analysera les autres dispositions prévues par le Projet de loi (III).

I. La protection du secret professionnel

Il est à noter que dans son arrêt *Digital Rights*, la CJUE fait expressément référence au secret professionnel pour lequel la Directive 2006/24/CE *aurait dû prévoir une exception*⁶. Le projet de loi ne répond pas à cette question fondamentale de préservation du secret professionnel en ne prévoyant aucune exception à la collecte et la rétention des données pour les personnes soumises à celui-ci.

Or, le secret professionnel de l'avocat repose sur de nombreuses normes impératives, qu'il s'agisse de prescriptions légales pénalement sanctionnées ou de règles déontologiques. Il est protégé par la Cour Européenne des Droits de l'Homme qui le définit comme « la base de la relation de confiance qui existe entre l'avocat et son client⁷ » et érigé comme norme communautaire par la CJUE⁹. Le secret professionnel de l'avocat est d'ordre public et ceci dans l'intérêt du client. Il est général, absolu et illimité dans le temps¹⁰ et il participe à l'Etat de droit. Il couvre toutes les confidences que l'avocat a pu recevoir à raison de son état ou de sa profession. Sont ainsi couverts par le secret les informations reçues du client, celles reçues de tiers dans le cadre du dossier concernant ce client, mais également, et il convient de le rappeler pour la présente, le nom du client ainsi que l'agenda de l'avocat¹¹.

Le projet de loi vise la rétention des données relatives au trafic et à la localisation. Ces données désignent les informations liées à l'utilisation des réseaux et permettent d'identifier les interlocuteurs, leur localisation et la durée de leur communication. Si comme rappelé précédemment la conservation du contenu des communications électroniques et des informations consultées n'est pas visée ni par la loi de transposition de la Directive invalidée, ni par le présent Projet de loi commenté, il n'en demeure pas moins que les données relatives au trafic et à localisation collectées

³ *ibid* point 58

⁴ *ibid* point 60

⁵ *ibid* point 63

⁶ *ibid* point 58: « En outre, elle (la Directive 2006/24/CE) ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »

⁷ CEDH Cour EDH, 5e Sect. 24 juillet 2008, André et autres c. France, Req. n° 18603/03, point 41

⁸ Article 7.1.2 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

⁹ CJCE, 18 mai 1982, A.M. & S. c/ Commission des Communautés européennes, Aff. 155/79, Rec, p. 1575.

¹⁰ Article 7.1.1 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

¹¹ Article 7.1.3. du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

permettent d'identifier les interlocuteurs de l'avocat. Les déplacements précis, noms des personnes en correspondance avec l'avocat, donc de ses clients, lieux et dates de rencontre de l'avocat avec ses contacts sont autant d'éléments protégés par le secret professionnel de l'avocat.

Si le secret professionnel peut connaître des exceptions, celles-ci ne peuvent pas, à l'image de celles prévues pour les écoutes téléphoniques ou perquisitions¹², porter atteinte au secret de manière disproportionnée par rapport au but poursuivi et doivent s'accompagner de garanties procédurales particulières.

En ce sens le Conseil de l'Ordre se range derrière les avis du Conseil d'Etat du 10 juillet 2015 et de la Commission Nationale pour la Protection des Données (CNPD) du 19 juin 2015 et recommande l'insertion à l'article 67-1 du Code d'instruction criminelle d'une exception analogue à celle existant en matière d'écoutes téléphoniques qui dispose que « *les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes de tenter de commettre ou d'avoir commis ou tenté de commettre l'infraction comme auteurs ou complices, ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le chef du service de renseignements.* » (Article 88-4 du Code d'instruction criminelle).

Le Conseil de l'Ordre seconde la proposition du Conseil d'Etat d'insérer entre l'actuel paragraphe 3 de l'article 67-1 du Code d'instruction criminelle et le paragraphe 4 projeté, qui deviendrait alors le paragraphe 5, un paragraphe 4 s'inspirant du paragraphe 4 de l'article 88-1 du Code d'instruction criminelle, libellé comme suit:

« (4) Les mesures visées à l'alinéa (1) ne peuvent être ordonnées à l'égard d'une personne liée par le secret professionnel au sens de l'article 458 du Code pénal, à moins qu'elle ne soit elle-même suspecte d'avoir commis l'infraction. »

Toujours afin d'assurer la protection du secret professionnel, le Conseil de l'Ordre est d'avis que la modification suivante devrait être apportée au paragraphe 2 de l'article 67-1 du Code d'instruction criminelle, comme suit :

« (2) Chaque opérateur de télécommunications et chaque fournisseur d'un service de télécommunications communique les informations qui ont été demandées dans les meilleurs délais. Toutefois, les informations qui relèvent du secret professionnel, au sens de l'article 458 du Code pénal, et notamment celles relatives au destinataire des appels, ne peuvent être communiquées, sauf si le dépositaire d'un tel secret est lui-même suspecté d'avoir commis l'infraction. »

Enfin, le Conseil de l'Ordre est également favorable à la proposition de la CNPD d'insérer une exception analogue pour les personnes soumises au secret professionnel à l'article 10 paragraphe (2) du projet de loi n°6675 portant organisation du Service de Renseignement de l'Etat¹³. Cet article autorise le Service de Renseignement de

¹² CEDH, 16 décembre 1992, Niemietz c. Allemagne.

¹³ *Projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat, la loi du 31 mai 2005 relative aux dispositions spécifiques de*

l'Etat à procéder au repérage de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de télécommunications. Le Conseil de l'Ordre estime que le secret professionnel doit être protégé dans cette législation.

II. La problématique de la conservation a priori indifférenciée et massive de données personnelles

La CJUE, dans son arrêt *Digital Rights* reconnaît l'ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte que constitue la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci. Si la Cour juge l'ingérence justifiée en ce qu'elle répond à un objectif d'intérêt général, elle la considère cependant non proportionnée notamment par ses reproches aux points 58 et 59.

La Cour reproche dans un premier temps à la Directive 2006/24 d'être dirigée contre l'ensemble des utilisateurs des services de communication sans qu'un lien direct ou indirect avec la commission d'une infraction ne soit exigé.

Le point 58 de l'arrêt Digital Rights affirme en ce sens que: « la directive 2006/24 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 ».

Dans un deuxième temps la CJUE fait grief à la Directive 2006/24 de ne faire aucun lien entre les données conservées et une menace pour la sécurité publique et de ne prévoir aucune limite temporelle, géographique ou humaine à cette collecte.

Le point 59 de l'arrêt Digital Rights affirme en ce sens que : « D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves ».

protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, le Code d'Instruction criminelle, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, et la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Ledit projet de loi a été déposé à la Chambre des Députés comme projet de loi n° 6675 en date du 2 avril 2014.

Le Conseil de l'Ordre regrette que si le projet de loi prévoit notamment des mesures limitant l'accès à ces données et relatives à la durée et à la localisation de la conservation, il ne répond pas formellement à ces critiques relatives à la conservation a priori, généralisée et indiscriminée des données relatives au trafic et à la localisation. Par conséquent, il n'est pas exclu que le Projet continue à se voir critiquer en justice pour ne pas avoir pris en considération l'entière des critiques de la CJUE.

Les Professeurs de droit Dr. Franziska Boehm de l'Université de Münster et Dr. Mark D. Cole de l'Université de Luxembourg concluent, dans leur rapport *Conservation des données après l'arrêt de la Cour de Justice de l'Union Européenne*¹⁴, que la conservation généralisée des données de personnes non suspectes pour une utilisation future à des fins répressives est contraire aux articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne dès lors qu'il n'est pas possible d'établir un lien entre les données conservées et une menace à la Sécurité Publique¹⁵. La lutte contre le terrorisme et la criminalité organisée sont des combats louables en cette période de tension et de menaces internationales. Cependant, elle ne peut justifier des atteintes inutiles, inadéquates et inappropriées aux droits fondamentaux des citoyens européens. D'autres auteurs, dont Bernard Glandz¹⁶ et Christofi, voient dans les développements de l'arrêt *Digital Rights* le rejet de toute collecte massive de données et la nécessité de remettre en cause le travail législatif¹⁷ dans son entièreté.

Le Conseil de l'Ordre rejoint donc l'avis de la Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg en ce qu'il est regrettable que les rédacteurs du Projet de loi n'abordent pas les justifications du maintien de la conservation généralisée des données et ne répondent pas aux critiques de la CJUE visées aux points 57 et 58 de l'arrêt *Digital Rights*.

Il convient de s'interroger sur l'adéquation d'une telle mesure avec la recherche et la poursuite des infractions. La Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg fait état de l'exemple allemand dont le Tribunal constitutionnel fédéral a déclaré inconstitutionnelle la loi nationale transposant la Directive 2006/24/CE. Suite à cette décision, 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, 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.

Le Conseil de l'Ordre rejoint également l'avis de la Commission consultative des Droits de l'Homme qui préconise une analyse approfondie des mesures alternatives à cette obligation de conservation généralisée comme la collecte rapide (dite gelée) des données qui concerne seulement les personnes soupçonnées d'avoir directement ou

¹⁴ Dr. Franziska Boehm, Dr. Mark D. Cole, *Data Retention after the Judgment of the Court of Justice of the European Union*, Münster/Luxembourg, 30 juin 2014.

¹⁵ "The study has demonstrated the impact of the Data Retention Directive Judgment on data protection and privacy in the Law Enforcement sector and on other data retention measures. Essential is that blanket retention of data of unsuspecting persons for the later use for Law Enforcement is not in line with Article 7 and 8 of the Charter of Fundamental Rights of the European Union since it is not possible to establish a link between the data retained and a threat to public security".

¹⁶ Christophe Bernard-Glandz, *Les arrêts Digital Rights Ireland et Google Spain, ou le printemps européen de la protection des données*, C.D.E. 2014/3, pp 685-717

¹⁷ A. Christofi, «Arrêt Digital Rights Ireland», *Revue du droit de l'Union européenne*, 2014, pp.399-406.

III. Autres Dispositions

13 OCT. 2015

Paul J. Farrow

6