# Avis de la Commission nationale pour la protection des données quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour 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 communication

Délibération n° 214/2014 du 13 mai 2014

Conformément à l'article 32 paragraphe (3) lettre (e) et (f) 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 du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission de présenter au gouvernement toutes suggestions susceptibles d'améliorer le cadre légal et d'aviser *« 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 lettre du 9 avril 2014, Monsieur le Ministre de la Justice a saisi la Commission nationale d'une demande d'examen de la conformité de la législation luxembourgeoise avec les exigences posées par la Cour de Justice de l'Union Européenne dans son arrêt du 8 avril dernier par lequel elle a invalidé la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données modifiant la directive 2002/58/CE.

Il y a lieu de rappeler en introduction que l'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans notre législation par la loi du 30 mai 2005 sur base de l'article 15 § 1$^{er}$ de la directive 2002/58/CE du 12 juillet 2002 qui permettait aux Etats membres d'introduire une telle mesure lorsqu'une telle limitation des principes prévus aux articles 5, 6, 8 et 9 constitue une mesure nécessaire appropriée et proportionnée au sein d'une société démocratique pour sauvegarder la sûreté de l'Etat, la défense et la sécurité publique. Il s'agit là d'une référence explicitée au 2$^{ième}$ paragraphe de l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme de 1950 et donc indirectement d'une réserve des droits fondamentaux prévus par la Charte, en particulier ceux visés par les articles 7 (vie privée) et 8 (données personnelles).

Après avoir ramené à 6 mois le délai de conservation initialement fixé à 12 mois (loi du 27 juillet 2007), le législateur a transposé la directive 2006/24/CE en modifiant la loi du 30 mai 2005 par les dispositions de la loi du 24 juillet 2010 assorties par ailleurs d'un règlement grand-ducal du même jour qui en a réglé les modalités d'application (déterminant les catégories de données visées).

Les modalités d'accès aux données font l'objet des dispositions des articles 67-1 (loi du 29 juillet 2010) et des articles 88-1 à 88-5 (loi du 30 mai 2005) du Code d'instruction criminelle.

La Commission nationale avait exprimé son appréciation et ses recommandations dans un avis relatif au projet de loi 6113 (N° 85/2010) le 26 avril 2010.

L'analyse de l'arrêt du 8 avril 2014 fait apparaître avec force l'attachement de la haute juridiction aux principes consacrés par la Charte des droits fondamentaux de l'Union européenne, en particulier ses articles 7 et 8 qui prennent leur racine dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [CEDH signée à Rome le 4 novembre 1950].

Le paragraphe 2 de l'article en question ci-dessus prévoit qu'il « ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, entre autres, à la sécurité nationale, à la sûreté publique, à la défense l'ordre et à la prévention des infractions pénales, ou à la protection des droits et libertés d'autrui ».

Les juridictions nationales autrichiennes et irlandaises ont posé dans leurs décisions respectives la question préjudicielle de la validité de la directive 2006/24 à la lumière des articles 7 (« respect de la vie privée »), 8 (« protection des données à caractère personnel ») et 11 (« liberté d'expression ») de la Charte des droits fondamentaux de l'Union européenne.

La Cour retient en premier lieu la vaste ampleur et le caractère intrusif de l'ingérence dans l'exercice de ces droits fondamentaux que comporte l'obligation faite aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver les données de trafic et de localisation des utilisateurs par la directive incriminée.

Nous n'estimons pas nécessaire d'évoquer plus amplement les motifs afférents retenus (couverture générale de toutes personnes et tous moyens de communication, sensibilité des données, sentiment de la population de surveillance massive et indépendante de toute suspicion, ...) mais nous nous attachons dans la suite à examiner les conséquences que la Cour en a tiré.

Nous passerons dès lors en revue une à une les conditions de compatibilité exigées selon l'arrêt de la Cour pour une conformité avec le régime des droits fondamentaux de la Charte.

La CJUE a invalidé la directive mais non le principe même d'une rétention de données rendue obligatoire par des législations nationales. L'accent est mis dans ce cas sur un encadrement suffisamment restrictif de façon à limiter l'ingérence au minimum nécessaire et des conditions et modalités aptes à prévenir des abus.

Un écueil dans l'interprétation du sens de l'arrêt consisterait à notre avis à ne pas distinguer la validité de l'instrument juridique communautaire de celle d'une disposition nationale mettant en œuvre une « Vorratsdatenspeicherung ».

Certes notre législation nationale, comme celle des plus de 20 Etats membres disposant d'un régime de conservation de données de communications obligatoire pendant une durée limitée en vue de garantir l'accès aux autorités chargées des missions afférentes dans la prévention d'atteintes à la sécurité publique, sûreté de l'Etat et la répression de la criminalité grave, ne saurait être reconnue respectueuse des valeurs fondamentales de la Charte, si elle(s) ne prévoient pas les restrictions, précautions et garanties reconnues nécessaires dans les motifs de l'arrêt, mais il nous semble que les conditions dégagées dans l'examen de la validité de la directive ne s'appliquent pas toutes et cumulativement à une législation nationale donnée de la même façon que la Cour les a estimé nécessaires pour qu'une directive imposant la rétention des données dans toute l'Union soit reconnue valide (cf. 30[1]).

C'est la seule lecture qui permette à notre avis de ne pas voir une contradiction dans les développements relevant que la rétention des données s'applique à toutes personnes et tous moyens de communication sans différenciation suivant la probabilité d'un lien avec des infractions graves avec ceux mettant en évidence que la rétention obligatoire des données peut être considérée comme apte à réaliser l'objectif poursuivi (9, 50) reconnu comme intérêt général suffisamment fondamental pour justifier la mesure (44, 51), à condition que celle-ci soit précisément encadrée et s'opère dans les limites du strict nécessaire (46, 52), et avec toutes les garanties qui l'entourent (54). La directive est invalidée compte tenu de la portée de l'ingérence dans les droits fondamentaux des personnes et l'absence de proportionnalité et de règles claires et suffisantes imposant des limites et mesures de sauvegarde.

Il convient donc de noter que la CJUE « a interdit d'obliger dans les conditions de la directive 2006/24 sans pour autant obliger l'Union à interdire aux Etats membres d'obliger à la rétention des données ».

Voyons donc une à une les conditions de validité qui devront être remplies par les lois nationales. Pour cela, il y a lieu de distinguer les conditions et garanties exigées pour encadrer l'obligation de conservation (A) d'une part, de celle nécessaire au niveau de l'accès aux données par les autorités d'autre part (B).

## A. Obligation de rétention des données

1) La constatation de la Cour que la directive ne fait aucune différenciation en fonction de l'objectif de lutte contre les infractions graves dans la définition de son champ d'application (qui couvre toutes personnes et tous moyens de communication (57)) sans requérir par ailleurs aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (59) ne doit à notre avis être seulement comprise comme une critique de l'étendue excessive de la directive.

Si ces aspects devraient être considérés comme critères d'exclusion dans le contexte d'un régime légal national, le modèle de la rétention de données conservatoire devrait être considéré en soi comme répudié par la Cour et seul un schéma du type « quick freeze » serait conforme à son arrêt, ce qui n'est, dans l'interprétation communément admise, pas le cas.

[1] les numéros référencés entre parenthèses renvoient aux différents points de l'arrêt de la Cour commenté

Quant aux avantages et inconvénients respectifs de ces deux modèles alternatifs envisageables pour permettre aux autorités judiciaires et de sécurité publique d'avoir recours aux données générées dans le cadre des communications électroniques, nous aimerions donner à considérer que les données faisant l'objet de l'obligation de conservation actuellement en place au Luxembourg (catégories reprises au règlement grand-ducal du 24 juillet 2010) sont générées et traitées de toute façon dans les systèmes des fournisseurs de services et opérateurs de réseaux. Le Code d'instruction criminelle en permet l'accès aux autorités judiciaires sous réserve du respect des conditions afférentes.

Les données de trafic peuvent en effet être conservées sous certaines conditions pendant une durée maximale de 6 mois par les fournisseurs de service pour leur servir aux besoins de la facturation, de l'établissement des décomptes de paiement d'interconnexion entre réseaux, des poursuites engagées en cas de non-paiement, des litiges et contestations non encore vidés, et des besoins techniques et de gestion du trafic (article 5 § 3 à 5 de la loi modifiée du 30 mai 2005).

Ce ne serait donc que pour des données que les opérateurs seraient amenés à effacer le cas échéant plus rapidement que la période de 6 mois d'obligation de conservation généralisée prévue aux articles 5 § 1 et 9 § 1 de ladite loi du 30 mai 2005 se révélerait plus attentatoire aux droits des personnes concernées qu'un système de quick freeze qui n'affecterait de façon ciblée que les données ponctuellement jugées nécessaires par le juge. Il appartiendrait dans cette hypothèse au gouvernement d'arbitrer entre ces deux systèmes en tenant encore compte d'autres facteurs non analysés ici.

Alors que la durée de conservation obligatoire en vue de la mise à disposition des données des autorités judiciaires n'est pas plus longue que celle pendant laquelle les opérateurs peuvent les conserver pour les besoins de la facturation, les risques engendrés par le régime légal luxembourgeois nous semblent proportionnés aux objectifs d'intérêt public poursuivis.

Par ailleurs la législation luxembourgeoise entoure l'obligation de conservation et l'accès aux données d'un certain nombre de restrictions et garanties qu'il nous semble plus important d'examiner une à une au niveau de leur conformité aux exigences de l'arrêt de la CJUE et de l'opportunité d'y apporter encore des améliorations.

2) <u>Durée de conservation imposée par la loi</u>

La Cour fédérale constitutionnelle allemande, dans son arrêt du 2 mars 2010, avait considéré qu'une durée de conservation non excessive au regard de la gravité de l'ingérence d'une rétention de données de communication devrait être inférieure à un an et qu'une durée de 6 mois pourrait être justifiée dans le respect du principe de proportionnalité.

Sur ce point la CJUE s'exprime moins clairement que la plus haute juridiction allemande parce qu'elle avait à statuer par rapport aux dispositions de la directive communautaire et non d'une législation nationale individuelle. Elle critique la fourchette prévue par le législateur communautaire (6 mois à 2 ans) et relève l'absence de critères objectifs et notamment d'une quelconque différenciation entre les catégories de données (63) ou selon les moyens de communications utilisés.

La Commission nationale estime en revanche qu'en appliquant une durée unitaire de 6 mois à l'ensemble des données faisant l'objet de l'obligation de conservation et des moyens de communication concernés, le législateur a efficacement minimisé les risques d'atteinte au respect de la vie privée et des données personnelles.

3) Défaut d'exceptions pour les personnes dont les communications sont soumises au secret professionnel

La loi luxembourgeoise ne prévoit pas d'exceptions en faveur de personnes dont le secret des communications bénéficierait d'une protection renforcée.

Il est à signaler toutefois que l'article 88-2 du Code d'instruction criminelle dispose à son paragraphe (5) que « les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectées d'avoir elles-mêmes commis l'infraction, ou d'y avoir participé, ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction. »

L'article 88-4 contient un paragraphe (3) d'une teneur similaire applicable aux cas de surveillance des communications et correspondances à opérer pour le Service de renseignement de l'Etat.

Certes il s'agit dans un de ces cas d'une surveillance concernant également le contenu des communications et correspondances et non seulement des données de trafic (et de localisation) mais l'ajout d'une disposition analogue à l'article 67-1 serait sans doute de nature à répondre à l'exigence reflétée dans l'arrêt de la CJUE examiné d'exempter les données relatives aux communications de ces personnes.

La Commission nationale s'interroge en outre sur le point de savoir s'il ne faudrait pas étendre l'effet de cette exception aux communications des journalistes lorsque cela est nécessaire pour éviter une atteinte à la protection des sources dont ils bénéficient de par la loi dans l'exercice de leur activité professionnelle.

Nous sommes conscients que les mesures préconisées ci-dessus ne reviennent pas rigoureusement à exempter ces personnes de la conservation légalement obligatoire de leurs données de communication mais se limiteraient à en exclure l'accès et l'utilisation.

La Commission nationale estime pourtant que cette voie - bien plus facilement praticable - reviendrait à réduire de façon équivalente les conséquences pour la vie privée résultant de l'ingérence dans le secret de leurs communications électroniques des personnes visées par la CJUE au regard de la protection spéciale dont ils bénéficient dans les activités considérées.

4) Obligation de destruction à l'expiration de la durée de conservation légale

L'arrêt mentionne l'exigence que la législation impose la destruction irrémédiable des données à caractère personnel à la fin de la période de conservation obligatoire.

L'article 5, paragraphe 1$^{er}$ (b) de la loi modifiée du 30 mai 2005 prévoit effectivement « qu'après la période de conservation, le fournisseur de services ou l'opérateur est obligé

d'effacer les données relatives au trafic concernant les abonnés et utilisateurs, ou les rendre anonymes ».

On peut donc à notre avis conclure que la législation luxembourgeoise est conforme sur ce point. Certes on pourrait s'interroger sur le point de savoir si la préservation des données permise en cas d'anonymisation ne constitue pas une entorse à l'exigence en question. Tout est ici une question d'interprétation du terme « anonymisation » (pour davantage de développements sur la distinction entre pseudonymisation, données dépersonnalisées et données anonymes, cf. WP 05/2014 du Groupe de l'Art. 29, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

Des données rendues irréversiblement anonymes sont en effet à considérer comme en dehors du champ d'application de la protection des données selon la directive 95/46/CE (cf. aussi considérant 26 : données conservées sous une forme ne permettant plus l'identification de la personne concernée).

Au cas où le gouvernement voudrait néanmoins se prémunir de tout malentendu sur ce point, il conviendrait de proposer la suppression du bout de phrase « ou les rendre anonymes » dans les articles 5 et 9 de la loi modifiée du 30 mai 2005.

5) Obligation de conserver les données sur le territoire de l'Union européenne

La législation luxembourgeoise ne prévoit aucune limitation de la sorte. Le responsable du traitement pourrait donc théoriquement avoir recours à des moyens de traitements ou à des sous-traitants situés sur le territoire de pays-tiers reconnus offrir un niveau de protection adéquate ou les transmettre en dehors de l'UE dans les autres circonstances prévues à l'article 26 de la directive faisant échec au principe général d'interdiction de transfert de données personnelles de l'article 25. L'arrêt motive cette exigence (plus rigoureuse que celle prévue aux articles 25 et 26 de la directive 95/46/CE) par la nécessité de voir soumettre le traitement et la conservation de ces vastes quantités de données sensibles par une autorité de contrôle indépendante mettant en œuvre le droit européen de protection des libertés et droits fondamentaux. Il conviendrait donc de rajouter une limitation afférente aux articles 5-1 et 9-2 de la loi modifiée du 30 mai 2005 visée ci-haut.

6) Mesures techniques et d'organisation destinées à assurer la confidentialité et la sécurité des données conservées

L'article 5-1 de la loi du 30 mai 2005 renvoie aux articles 22 à 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 quant aux mesures de sécurité.

La CJUE pose des exigences plus strictes dans son arrêt du 8 avril.

La Commission nationale avait déjà dans son avis du 26 avril 2010 plaidé pour l'inscription dans la loi de l'obligation pour les fournisseurs de service et opérateurs de réseaux de prendre des mesures de protection spécifiques pour les données faisant l'objet de la rétention obligatoire et avait mentionné les mesures envisageables suivantes :

- le stockage distinct sur des serveurs physiquement séparés et déconnectés de l'Internet,
- un chiffrement basé sur une encryptage asymétrique avec une sauvegarde séparée des clés d'encryptage,
- le principe des quatre yeux relatif à l'accès aux données lié à des procédés avancés concernant l'authentification relative à l'accès aux clés d'encryptage,
- la journalisation révisable des accès aux données et leur destruction,
- l'application de mécanismes de correction automatique de fautes respectivement d'erreurs et de méthodes de plausibilités.

7) Sanction des abus

La loi luxembourgeoise prévoit des sanctions pénales en cas d'accès non autorisé aux données retenues par les fournisseurs de service et opérateurs de réseaux. La CNPD avait suggéré dans son avis de 2010 sur le projet de loi 6113 d'inscrire en outre expressément dans le Code d'instruction criminelle la nullité de la preuve obtenue moyennant un accès illicite ou un abus des données en question.

### B. Conditions d'accès aux données par les autorités

C'est à ce niveau que se situe à notre avis la nécessité la plus importante de modification de la législation luxembourgeoise pour la rendre conforme avec les exigences dégagées par la Cour en application des principes de proportionnalité et pour réduire l'ingérence dans l'exercice des droits individuels au strict minimum nécessaire.

1) Le seuil définissant les incriminations des faits pour lesquels l'article 67-1 du Code d'instruction criminelle (premier alinéa) permet l'accès aux données nous est déjà apparu en 2010 comme sensiblement 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 (cf. point B.1. de l'avis de la CNPD du 26 avril 2010 sur le projet de loi 6113).

Elle préconise aussi de privilégier la voie de détermination d'un catalogue d'infractions plutôt que d'un seuil de peine d'emprisonnement prévu.

2) En revanche la législation luxembourgeoise prévoit d'ores et déjà un accès subordonné à une autorisation préalable du juge d'instruction (art. 67-1) et n'a pas à être modifiée et apparaît exemplaire en Europe à cet égard.

## Conclusion

Les autorités de protection des données européennes ont unanimement salué l'arrêt de la Cour de Justice de l'Union européenne, ce qui n'est pas étonnant puisque le G29 au sein duquel elles se coordonnent avait exprimé clairement l'appréciation dans son rapport sur les

mises en œuvre nationales de la directive 2006/24[2] que la directive invalidée ne répondait pas à l'ensemble des exigences du droit européen de la protection des données. Une étude détaillée des textes de transposition nationale et de leur application pratique a mis en lumière une grande diversité de situations nationales, au niveau des durées de conservation prescrites, des services et données concrètes soumis à l'obligation de conservation, des autorités bénéficiant de l'accès à ces données et des conditions, modalités, de ces accès et du contrôle de la justification de ces accès et finalement des garanties établies en vue de la sécurité et confidentialité des données conservées ainsi que de la prévention et de la sanction d'éventuels abus.

Dans leurs réactions, nos collègues ne s'expriment guère quant à l'expectative de l'élaboration d'une réédition de la directive comportant des dispositions intégralement conformes aux exigences de l'arrêt par la Commission européenne. Il nous semble pourtant qu'une harmonisation serait souhaitable dans ce domaine, moins pour imposer une conservation obligatoire des données, mais pour que les conditions de celles-ci prévues dans les législations nationales soient conformes aux standards dégagés par la Cour et conformément à la Charte des droits fondamentaux de l'Union européenne.

La plupart des autorités nationales de protection des données sont engagées, pour ce qui les concerne, dans un travail d'analyse de la conformité de leur législation nationale, ou accompagnent un passage en revue initié par leurs autorités gouvernementales, en vue d'établir les modifications nécessaires à apporter aux règles nationales en place.

Aussi nous félicitons-nous d'avoir été consultés par le gouvernement et recommandons-nous vivement l'élaboration d'un projet de loi visant à amender les dispositions actuellement en vigueur sur les points évoqués ci-dessus, parmi lesquels la redéfinition de la condition correspondant à l'objectif de lutte contre la criminalité grave et organisée et le terrorisme par un critère plus approprié de qualification et d'incrimination des faits qui font l'objet de l'enquête, nous semble la plus importante.

Ainsi décidé à Esch-sur-Alzette en date du 13 mai 2014.

La Commission nationale pour la protection des données

| | | |
|---|---|---|
| Gérard Lommel<br>Président | Pierre Weimerskirch<br>Membre effectif | Thierry Lallemang<br>Membre effectif |

[2] WP 172/2010 Rapport sur le respect au niveau national par les fournisseurs de services de télécommunication et de services Internet des obligations découlant de la législation nationale sur la conservation des données de trafic http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf