Avis de la Commission nationale pour la protection des données concernant le projet de loi n°6113 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 et 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

Délibération n°85/2010 du 26 avril 2010

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission 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 courrier du 9 février 2010, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6113 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 (ci-après : le projet de loi) et au sujet du 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 (ci-après le projet de règlement grand-ducal).

Suivant l'exposé des motifs, le projet de loi et le projet de règlement grand-ducal se placent dans le contexte de la lutte contre le terrorisme et la criminalité grave. Ces textes traitent plus précisément de la rétention des données relatives au trafic et de données de localisation en matière de télécommunications en vue d'assurer leur disponibilité à des fins de recherche, de détection et de poursuite d'infractions graves.

La disponibilité des données de localisation et de trafic aux autorités judiciaires va au-delà de la conservation de données que les opérateurs effectuent en tout état de cause pour leurs propres besoins opérationnels, techniques et administratifs.

Elle concerne les données personnelles de tous les citoyens utilisant des moyens de télécommunication électroniques. Elle porte dès lors atteinte à la sphère privée de l'ensemble de la population qui se trouve en quelque sorte placée sous une suspicion généralisée (« *verdachtsunabhängiger Generalverdacht* »). Certes, la rétention ne porte pas directement sur le contenu des communications, mais uniquement sur les données de trafic et de localisation. Cependant, l'accès à ces données permet de connaître toutes sortes d'informations sur la vie privée et de

reconstituer une grande partie des contacts sociaux de tout un chacun. Par ailleurs, il permet de retracer les déplacements de chaque individu utilisant un téléphone mobile. L'accès à ces données révèle des informations concernant non seulement la personne directement ciblée, par exemple un auteur présumé d'une infraction, mais concernant également toutes les personnes ayant communiqué avec elle par téléphone, courriel etc.

A ce sujet, on peut citer la Cour constitutionnelle allemande:

« *(a) Die sechs Monate andauernde Möglichkeit des Zugriffs auf sämtliche durch eine Inanspruchnahme von Telekommunikationsdiensten entstandenen Verkehrsdaten bedeutet eine erhebliche Gefährdung des in Art. 10 Abs. 1 GG verankerten Persönlichkeitsschutzes. Dass ein umfassender Datenbestand ohne konkreten Anlass bevorratet wird, prägt auch das Gewicht der dadurch ermöglichten Verkehrsdatenabrufe. Von der Datenbevorratung ist annähernd jeder Bürger bei jeder Nutzung von Telekommunikationsanlagen betroffen, so dass eine Vielzahl von sensiblen Informationen über praktisch jedermann für staatliche Zugriffe verfügbar ist. Damit besteht für alle am Telekommunikationsverkehr Beteiligten das Risiko, dass im Rahmen konkreter behördlicher Ermittlungen über einen längeren Zeitraum hinweg Verkehrsdaten abgerufen werden. Dieses Risiko konkretisiert sich im einzelnen Abruf, weist jedoch angesichts der flächendeckenden Erfassung des Telekommunikationsverhaltens der Bevölkerung weit über den Einzelfall hinaus und droht, die Unbefangenheit des Kommunikationsaustauschs und das Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen insgesamt zu erschüttern (vgl. zu einzelnen Datenabrufen BVerfGE 107, 299 <320>).*

(b) In dem Verkehrsdatenabruf selbst liegt ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen zu erlangen, gegebenenfalls sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299 <318 ff.>).

Weiter werden in vielen Fällen die durch den Verkehrsdatenabruf erlangten Erkenntnisse die Grundlage für weitere Ermittlungsmaßnahmen bilden, die ohne diese Erkenntnisse nicht durchgeführt worden wären. Solche Ermittlungsmaßnahmen, beispielsweise Wohnungsdurchsuchungen oder Überwachungen der Telekommunikation, können ihrerseits den Betroffenen erheblich belasten, ohne dass es darauf ankommt, ob sie den gegen ihn bestehenden Verdacht einer strafbaren Handlung erhärten oder widerlegen. Auch die darin liegenden Nachteile können im Anschluss an die Ermittlungsmaßnahme nicht mehr behoben werden.»[1]

La rétention des données et l'accès à ces données par les autorités chargées de la recherche, de la détection et de la poursuite d'infractions graves constituent une ingérence profonde dans la jouissance des droits fondamentaux prévus par la Constitution et par la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales.

[1] BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. 155-157

En effet, l'article 28 de la Constitution dispose que « *le secret des lettres est inviolable. - La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste. La loi réglera la garantie à donner au secret des télégrammes.* »

L'article 11 paragraphe (2) de la Constitution dispose que « *l'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi.* »

Enfin, l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales dispose ce qui suit :

« *Droit au respect de la vie privée et familiale*

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. 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 à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Il résulte des trois dispositions susmentionnées qu'une exception aux droits y énoncés n'est possible qu'en vertu d'une loi. Il appartient en outre au législateur de faire la balance entre, d'un côté, un droit fondamental et, de l'autre côté, l'intérêt supérieur qui justifie cette exception.

Toute exception à un droit fondamental ne peut avoir lieu que dans le respect du principe de proportionnalité. La Cour constitutionnelle allemande a énuméré les devoirs du législateur pour ce qui est de la mise en œuvre de ce principe de proportionnalité en matière de rétention des données :

« *Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.*»[2]

La rétention des données de télécommunications et les possibilités qu'ouvre l'accès à ces données représentent une atteinte sans précédent au droit au respect de la vie privée. Aux yeux de la Commission nationale, une mesure attentatoire au respect de la vie privée ne se justifie que dans le contexte particulier de la lutte contre la criminalité grave et plus particulièrement le terrorisme et la criminalité organisée et que sous des conditions très strictes, en particulier celle d'un contrôle juridictionnel préalable.

[2] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, 2e „Leitsatz"

I. Le projet de loi n° 6113 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

Le projet de loi n° 6113 a pour objet la transposition en droit luxembourgeois de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 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, et modifiant la directive 2002/58/CE.

La directive 2002/58/CE prévoyait déjà la faculté pour les Etats membres de mettre en place une conservation obligatoire relative aux communications électroniques pour les besoins de la recherche, de la détection et de la poursuite d'infractions sans en harmoniser le régime. Au Luxembourg, le législateur a fait usage de cette faculté dans la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (ci-après désignée « la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques») transposant la prédite directive.

La directive 2006/24/CE a pour but le rapprochement des législations nationales en matière de rétention des données de trafic et de localisation. Elle ne comporte toutefois pas de disposition visant à règlementer l'accès à ces données par les autorités judiciaires. La Cour de justice des Communautés européennes précise en effet ce qui suit:

« *À cet égard, il importe de constater que les dispositions de cette directive sont essentiellement limitées aux activités des fournisseurs de services et ne réglementent pas l'accès aux données ni l'exploitation de celles-ci par les autorités policières ou judiciaires des États membres.*

Plus précisément, les dispositions de la directive 2006/24 tendent au rapprochement des législations nationales concernant l'obligation de conservation de données (article 3), les catégories de données à conserver (article 5), la durée de conservation des données (article 6), la protection et la sécurité des données (article 7) ainsi que les conditions de stockage de celles-ci (article 8).

En revanche, les mesures prévues par la directive 2006/24 n'impliquent pas, par elles-mêmes, une intervention répressive des autorités des États membres. Ainsi qu'il ressort notamment de l'article 3 de cette directive, il est prévu que les fournisseurs de services doivent conserver les seules données qui sont générées ou traitées lors de la fourniture des services de communication concernés. Ces données sont uniquement celles qui sont étroitement liées à l'exercice de l'activité commerciale de ces fournisseurs.

La directive 2006/24 réglemente ainsi des opérations qui sont indépendantes de la mise en œuvre de toute éventuelle action de coopération policière et judiciaire en matière pénale. Elle n'harmonise ni la question de l'accès aux données par les autorités nationales compétentes en matière répressive ni celle relative à l'utilisation et à l'échange de ces données entre ces autorités. Ces questions, qui relèvent, en principe, du domaine couvert par le titre VI du traité UE, ont été exclues des

dispositions de cette directive, ainsi qu'il est indiqué notamment au vingt-cinquième considérant et à l'article 4 de celle-ci. »[3]

Comme la règlementation des conditions et modalités d'accès ordonnés par les autorités judiciaires sont de la compétence des Etats membres, les dispositions y relatives du projet de loi ne découlent pas de la directive 2006/24/CE. Le projet de loi sous examen ne fait que reprendre les dispositions actuelles des articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 et adapter celles de l'article 67-1 du Code d'instruction criminelle. Elles sont analysées sous le point B. du présent avis.

A. L'obligation de conservation des données en vertu de la directive 2006/24/CE

1. La finalité de la conservation

La rétention des données a pour but, selon les termes de la directive 2006/24/CE « *de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* »

Pour garantir que l'utilisation des données de télécommunication conservées ne dépasse pas la finalité voulue par la directive, une importance particulière revient à la définition des « infractions graves » et à la limitation des accès. Ces questions seront abordées dans la partie B. du présent avis.

2. Les catégories de données concernées

Le projet de loi ne détermine pas les catégories de données faisant l'objet de la rétention, mais prévoit que celles-ci sont fixées par voie de règlement grand-ducal.

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques prévoyait déjà la détermination des données faisant l'objet de l'obligation de rétention par un règlement grand-ducal. Or, un tel règlement n'a jamais été adopté ce qui a donné lieu à une situation d'incertitude dans le domaine des droits fondamentaux.

Les catégories de données sont désormais fixées dans le projet de règlement annexé au projet de loi. Ces catégories de données y retenues correspondent a celles fixées par la directive 2006/24/CE.

[3] Cour de justice des communautés européennes (grande chambre), 10 février 2009, affaire C-301/06, points 80 - 83

3. La durée de conservation

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques prévoyait initialement une durée de conservation de 12 mois. Cette durée a été ramenée de 12 mois à 6 mois par la loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

La Commission nationale approuve que la durée de conservation des données reste limitée à 6 mois, comme c'est le cas en Allemagne, aux Pays-Bas et dans d'autres pays de l'Union européenne.

4. La question de la sous-traitance

L'obligation de conservation pèse sur les fournisseurs de services de communications électroniques accessibles au public et les opérateurs d'un réseau public de communication.

Le projet de loi prévoit que les « *fournisseurs de services ou opérateurs peuvent déléguer l'exécution de ces obligations à une ou plusieurs entités tierces, publiques ou privées, qui agissent au nom et pour le compte des fournisseurs de services ou opérateurs*». Or, une telle sous-traitance n'est pas prévue par la directive 2006/24/CE. Vu le caractère confidentiel et la quantité des données concernées, la Commission nationale est réservée en ce qui concerne cette possibilité de sous-traitance. Elle s'interroge sur l'opportunité de prévoir la faculté d'externalisation du stockage des données confidentielles concernant des millions de communications.

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques contient des dispositions spécifiques en matière de sécurité et de confidentialité pesant sur les fournisseurs de service, dispositions qui devront encore être renforcées dans le cadre de la transposition du second paquet de directives en matière de télécommunications. Les sous-traitants seront-ils toujours en mesure de répondre à ces exigences qui pèsent sur leurs clients, notamment lorsqu'ils presteront leurs services sous forme de « cloud computing » ? Dans l'hypothèse où le législateur maintient le possible recours à un sous-traitant, la Commission nationale estime pour le moins nécessaire de prévoir un encadrement législatif spécifique et rigoureux.

La disposition du projet de loi sous avis relatif à la faculté de la sous-traitance permettrait la mise en place d'un stockage centralisé de données provenant de l'ensemble des opérateurs auprès d'un organisme unique à l'image du « Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) » existant au Pays-Bas.

Un tel système peut avoir certains avantages, comme par exemple celui de garantir des standards de sécurité uniformes ou celui d'une meilleure préservation du secret de l'instruction parce que les accès aux données par les autorités policières et judiciaires se feront à l'insu des opérateurs.

Néanmoins, la Commission nationale n'est pas favorable à l'établissement d'un tel système. Elle est d'avis, en effet, qu'un stockage centralisé augmenterait les risques d'abus et de détournements de finalités et le sentiment des citoyens d'être exposés à une surveillance imperceptible de la part des autorités.

Il semble d'ailleurs qu'aux Pays-Bas, l'accès aux données de télécommunications par les autorités policières et judiciaires soit beaucoup plus fréquent que dans d'autres pays, probablement parce que les données sont stockées par un organisme public proche de ces autorités.

5. La question de la sécurité des données

Le projet de loi ne contient pas de dispositions relatives aux mesures spécifiques de sécurité à appliquer aux données conservées en application de l'obligation de rétention. Néanmoins, l'article 4 (1) du projet de règlement grand-ducal prévoit que « *les données conservées sont soumises aux exigences prévues aux articles 22 (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.* »

La Commission nationale estime cependant que la question de la sécurité devrait être traitée au niveau de la loi, ne serait-ce que pour garder un parallélisme avec la question de la sous-traitance également prévue au niveau de la loi.

Elle relève que le récent arrêt de la Cour constitutionnelle allemande a jugé inconstitutionnelle la législation allemande régissant la rétention des données notamment en raison des garanties de sécurité jugées insuffisantes.[4] Ledit arrêt a estimé que l'hypothèse de la conservation des données de communication électronique nécessite des exigences particulières au niveau de la sécurité dans le texte même de la loi et qu'il ne suffit pas d'y renvoyer aux dispositions de la législation générale.[5]

Il paraît dès lors souhaitable de voir compléter le projet de loi par des dispositions relatives aux obligations spécifiques de sécurité en tenant compte de la nature des données et du risque d'atteinte à la vie privée du citoyen.

Le récent arrêt de la Cour constitutionnelle allemande cite comme mesures de sécurité envisageables[6] :

- 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.

En ce qui concerne le principe de séparation des systèmes, le Groupe de travail «ARTICLE 29» sur la protection des données a également estimé dans son avis

[4] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010
[5] « Absatz » 274
Le §9 BDSG y mentionné et son « Anlage » correspondent aux articles 22 paragraphe (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
[6] « Absätze » 223 et 275

3/2006 que, « *concrètement, les systèmes de stockage de données à des fins d'ordre public devraient logiquement être séparés des systèmes utilisés à des fins commerciales.*»[7]

Finalement, la Commission nationale suggère à l'endroit de l'article 4 paragraphe (1) du projet de règlement grand-ducal de ne pas limiter la référence au seul premier paragraphe de l'article 22 de la loi modifiée du 2 août 2002, mais de l'étendre aux deux autres paragraphes du même article dont les dispositions sont également concernées par le projet de loi.

B. L'accès aux données par les autorités judiciaires

Si on peut considérer que la seule conservation des données de trafic et de localisation n'est attentatoire à la vie privée qu'en cas de défaillance des mesures de sécurité, il en est autrement de l'accès à ces données. En effet, c'est à partir du moment où quelqu'un accède aux données concernant un individu qu'il peut retracer où cet individu s'est trouvé à quel moment, à qui il a téléphoné et de qui il a été appelé ou à qui il a envoyé des SMS ou courriels et de qui il en a reçu, quels sites Internet il a consulté etc.

Il est dès lors nécessaire de voir encadré strictement l'accès des autorités policières et judiciaires en vue de limiter au maximum les atteintes à la vie privée des citoyens.

Il s'agit d'une part de limiter les cas d'ouverture en définissant de manière suffisamment restrictive les infractions dont la recherche, la détection et la poursuite pourra donner lieu à un accès aux données (point 1.) et d'autre part, de prévoir des dispositions réglementant la procédure d'accès qui doivent comporter des garanties appropriées visant à exclure toute utilisation allant au-delà de la finalité qui se trouve à la base de la directive et du projet de loi (point 2.).

1. La limitation des infractions pouvant donner lieu à un accès aux données

La rétention des données de communications électroniques telle que prévue par la directive 2006/24/CE vise à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves. La directive laisse aux Etats membres le soin de déterminer ces infractions graves.

Pour ce faire, deux options se présentent :

- l'établissement d'une énumération d'incriminations auxquelles les faits recherchés doivent correspondre ou
- la définition d'un seuil minimal de peine prévue.

[7] Groupe de travail «ARTICLE 29» sur la protection des données
Avis 3/2006 sur la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE
654/06/FR, WP 119
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_fr.pdf

L'établissement par le législateur d'une liste d'infractions apparaît préférable aux yeux de la Commission nationale.

Une énumération limitative permettrait de réserver l'accès aux données aux enquêtes et aux actes de poursuite relatifs à des infractions qui se situent clairement dans le contexte du terrorisme et de la criminalité organisée ou à la poursuite d'infractions dont le degré de gravité permet de les y assimiler. En ce qui concerne la définition des infractions graves, la Cour constitutionnelle allemande s'est exprimée comme suit:

« *Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen.* »[8]

Si néanmoins le législateur retient la voie de la définition d'un seuil de peine - notamment parce que l'exercice de l'élaboration d'un catalogue apparaît excessivement complexe -, le seuil choisi devrait être suffisamment élevé de façon à garantir que l'accès aux données ne soit possible uniquement pour des infractions dont la gravité ne fait aucun doute.

La Commission nationale considère que le seuil de peine envisagé, à savoir celui d'une peine dont le maximum est égal ou supérieur à un an d'emprisonnement, n'est pas assez élevé vu le nombre certainement très important d'infractions concernées. Un seuil de peine de deux ans d'emprisonnement au moins nous semble mieux correspondre aux motifs de la directive. Tel est d'ailleurs le seuil prévu par l'article 88-1 du Code d'instruction criminelle en matière d'écoutes téléphoniques. L'accès aux données faisant l'objet de la rétention et les écoutes téléphoniques affectent en effet le même droit fondamental à savoir celui du secret des communications.

Il est à noter que certains pays ont choisi un seuil de peine de cinq ans.

2. L'exigence d'une autorisation judiciaire préalable

Dans son avis du 25 mars 2005, le groupe de l'article 29 estime que les Etats-membres devraient mettre en place dans leurs lois de transposition des garanties spécifiques notamment sur les points suivants[9] :

- la limitation des accès en fonction de la définition de l'infraction grave,
- la limitation des accès aux seuls services répressifs compétents et dans les seuls cas des infractions graves définies,

[8] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, Absatz 228

[9] Groupe de travail «ARTICLE 29» sur la protection des données
Avis 3/2006 sur la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE
654/06/FR, WP 119

- l'exclusion d'une exploration à grande échelle des données conservées (sans éléments suffisants en relation avec une telle infraction).

La Commission nationale considère que tel serait le cas si chaque accès aux données était soumis à autorisation judiciaire préalable.

Or, le projet de loi laisse inchangé les articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques qui permettent l'accès par la police dans l'hypothèse du crime flagrant et du délit flagrant, sans ordonnance d'un juge d'instruction.

La vérification par le juge constituerait une bonne garantie contre d'éventuels abus. La nécessité d'une ordonnance d'un juge d'instruction permettrait d'empêcher le recours aux données de communications conservées pour des recherches systématiques de type „Rasterfahndung". Une telle exigence serait par ailleurs de nature à éviter le sentiment diffus de la population d'être surveillé à son insu, les données de connexion et de localisation de tout un chacun étant librement disponibles pour la police.

La Cour constitutionnelle allemande se prononce à ce sujet comme suit:

« *Für die Gewährleistung effektiven Rechtsschutzes ist eine Abfrage oder Übermittlung dieser Daten grundsätzlich unter Richtervorbehalt zu stellen.*

Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist (vgl. BVerfGE 120, 274 <331>). Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein. Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren ».[10]

La Commission nationale donne également à considérer que si l'accès aux données dans le cadre de l'enquête de flagrant crime ou de flagrant délit est possible sans autorisation du juge en vertu des articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005, cela entraînerait une contradiction avec le régime de l'article 67-1 du Code d'instruction criminelle aux termes duquel le repérage des communications n'est possible que s'il est ordonné par le juge d'instruction.

La question de l'application des dispositions relatives au repérage des communications dans le cadre d'une enquête pour crime flagrant ou délit flagrant a été examinée par la Cour d'appel :

« *Cette localisation de la provenance de l'appel téléphonique* [...] *constitue un repérage de données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, au sens de l'article 67-1*

[10] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, „Absätze" 247 et 248

du Code d'instruction criminelle. La compétence pour ordonner un tel repérage appartient en principe au seul juge d'instruction, et ce depuis la loi du 21 novembre 2002 ayant introduit au Code d'instruction criminelle ledit article 67-1. Alors qu'auparavant de telles investigations étaient opérées sur base des articles 65 et 66 du Code d'instruction criminelle, et pouvaient donc également être opérées dans le cadre des crimes et délits flagrants par les officiers de police judiciaire agissant sur base des articles 31 et 33 du Code d'instruction criminelle, le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction. Le fait que l'article 67-1 continue à figurer sous la section III « Des transports, perquisitions et saisies » du chapitre Ier du titre III du Livre premier du Code d'instruction criminelle a uniquement pour objet de distinguer le repérage des moyens de surveillance spéciale des télécommunications (articles 88-1 à 88-4 du Code d'instruction criminelle), mais n'autorise pas les officiers de police judiciaire, agissant en vertu des pouvoirs qui leur sont spécialement conférés au titre des crimes et des délits flagrants, à opérer un tel repérage au titre des articles 33 et 31 du Code d'instruction criminelle (perquisition et saisie). L'article 33 du Code d'instruction criminelle est le pendant de l'article 66 du même code, il n'inclut pas les pouvoirs que le juge d'instruction tient de l'article 67-1 dudit code. »[11]

Par ailleurs, contrairement à ce qui est indiqué dans le commentaire des articles du projet de loi sous examen, le repérage prévu par le prédit article 67-1 du Code d'instruction criminelle vise non seulement le recours à des données concernant des communications qui auront lieu après que le juge d'instruction a ordonné leur repérage mais aussi le recours à des données concernant des communications qui ont eu lieu avant que le juge d'instruction n'ait ordonné leur repérage.

En effet, l'article en question dispose notamment qu'il s'applique « *au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés* ». Cela ressort d'ailleurs aussi des travaux parlementaires relatifs à la loi du 21 novembre 2002 qui précisent ce qui suit : « *Il ressort dès lors clairement du libellé de cette disposition que la période sur laquelle porte le repérage peut viser aussi bien les communications passées que les communications futures*» [12]. Dès lors, dans les deux cas, le repérage est impossible en enquête de flagrance.

La Commission nationale retient donc que la jurisprudence considère que l'accès par la police pendant l'enquête de flagrance ne peut jamais avoir lieu sans ordonnance du juge d'instruction.

Enfin, on peut relever que « *l'enquête de flagrance a pour fondement l'urgence qu'il y a à recueillir les preuves encore existantes, indispensables à la manifestation de la vérité, d'une infraction dont la commission est récente.*» [13] Or, à la différence de ce qui est le cas par exemple pour les preuves recherchées dans le cadre d'une perquisition au cours d'une enquête de flagrance, il n'existe pas de risque de dépérissement des preuves pour ce qui est des données faisant l'objet de la rétention, puisque leur conservation est assurée pendant le délai de six mois.

La loi ne saurait cependant se borner à déterminer qui a accès aux données et sous quelles conditions. La Commission nationale estime que la protection des droits du citoyen requiert également des sanctions effectives en cas de violation de la loi.

[11] Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V
[12] Projet de loi n° 4889[00], commentaire de l'article, p. 4
[13] JurisClasseur, Procédure pénale, fascicule 20, n° 2

Cette nécessité est déjà mentionnée au niveau de la directive 2006/24/CE:

« *Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives.*» (article 13)

La Commission nationale estime qu'il ne suffit pas que l'accès aux données et leur utilisation illicites soient assortis de sanctions pénales, mais la loi devrait également prévoir dans ces hypothèses la nullité de la preuve en matière de procédure pénale.

Enfin, la Commission nationale constate que l'article 5 paragraphe (2) de la loi modifiée du 30 mai 2005 mélange d'un côté la rétention des données pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales (renvoi au paragraphe (1) et au Code d'instruction criminelle) et de l'autre côté l'utilisation de certaines données de trafic dans le cadre de litiges d'ordre civil ou commercial (renvoi au paragraphes (3) et (4) et mention, dans le deuxième tiret, de « *litiges notamment en matière d'interconnexion ou de facturation* »).

La rédaction de cet article pourrait laisser croire que les données faisant l'objet de la rétention imposée par la directive 2006/24/CE peuvent servir de preuves dans des litiges civils ou commerciaux.

La Commission nationale estime que la conservation des données en vertu de la directive 2006/24/CE, d'une part, et la conservation des données de connexion qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion, d'autre part, devraient faire l'objet de paragraphes distincts.

II. 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

Le projet de règlement grand-ducal détermine les catégories de données faisant l'objet de la rétention. La Commission nationale n'a pas d'observations particulières à formuler à ce sujet étant donné que ce texte reprend, pour l'essentiel, les dispositions de la directive 2006/24/CE.

En ce qui concerne les mesures de sécurité, il est renvoyé aux observations formulées sous le point A. 5. selon lesquelles la Commission nationale souhaiterait que les mesures de sécurité soient traitées au niveau de la loi.

Elle relève encore que l'article 6 prévoit l'établissement de statistiques sur les accès aux données conservées en application de la directive 2006/24/CE. De telles statistiques, qui sont publiées déjà dans d'autres pays (en matière d'accès aux données de connexion et de localisation ainsi que dans le domaine des écoutes

téléphoniques et interceptions de correspondances), sont susceptibles de contribuer à une plus grande transparence, à la prévention des abus et au contrôle démocratique dans ce domaine.

Ainsi décidé à Luxembourg en date du 26 avril 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Pierre Weimerskirch	Thierry Lallemang
Président	Membre effectif	Membre effectif