

A-2274/10-11



CHFEP

Chambre des fonctionnaires
et employés publics

11-A, avenue de la Porte-Neuve | L-2227 Luxembourg | Tél.: 47 22 24 | Fax: 47 23 74 | E-mail: chfep@chfep.lu

A V I S

sur

le 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**

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

Par dépêche du 11 février 2010, Monsieur le Ministre des Communications et des Médias a demandé, "*dans les meilleurs délais*" bien évidemment, l'avis de la Chambre des fonctionnaires et employés publics sur le projet de loi et le projet de règlement grand-ducal spécifiés à l'intitulé.

1. Introduction

Les communications électroniques génèrent d'innombrables données relatives au trafic qui sont enregistrées et exploitées par les opérateurs et fournisseurs d'accès ou de services de communications électroniques.

Ces données relevant de la téléphonie fixe ou mobile, de courriels, d'SMS et de l'utilisation d'Internet sont constituées:

- de la source de la communication;
- de la destination d'une communication;
- de la date, de l'heure et de la durée de la communication;
- du type de communication;
- de la machine utilisée pour communiquer, et
- de la location des équipements de communication,

à l'exception du contenu des communications et des pages web visitées.

Il est ainsi possible de retracer quel usager a téléphoné ou envoyé un "SMS" ou un "*e-mail*", quand, à qui, pendant combien de temps et de quel endroit.

Il s'ensuit que, sur base des données du trafic, il est possible de se faire une idée plus ou moins précise de certains aspects de la vie privée de l'utilisateur.

La directive 2002/58/CE, dénommée "*directive vie privée et communications électroniques*" (transposée en droit luxembourgeois par la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques), rappelle comme principe de base que les États membres de l'Union européenne doivent garantir, par leur législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications électroniques. En particulier, ils doivent interdire, à toute personne autre que l'utilisateur, d'écouter, d'intercepter ou de stocker les communications sans le consentement des utilisateurs concernés.

Les données précitées peuvent cependant être utilisées par les opérateurs et fournisseurs de services de communications électroniques pour leur facturation. Elles peuvent également servir à des fins commerciales, toutefois, dans ce cas, uniquement après autorisation des consommateurs concernés.

Outre ces objectifs de facturation ou commerciaux, des raisons d'ordre public (sécurité nationale, prévention, recherche, détection et poursuite d'infractions pénales, utilisation non autorisée du système de communications électroniques, communications à destination du numéro d'appel d'urgence 112) peuvent également être invoquées pour justifier le traitement ultérieur des données relatives au trafic.

L'Union européenne impose ainsi aux États membres d'obliger les opérateurs et fournisseurs d'accès et de services de communications électroniques à conserver les données sur le trafic, pendant une durée limitée déterminée, et de les mettre, en cas de besoin, à la disposition des autorités nationales compétentes.

Il ne peut toutefois, conformément à l'article 8 de la Convention européenne des Droits de l'Homme, être recouru à ces données que dans les cas où il s'agit d'une "*mesure nécessaire, appropriée et proportionnée dans une société démocratique*".

Après le délai de conservation défini, les données doivent être détruites ou rendues anonymes, à l'exception toutefois des données consultées qui sont préservées.

Le projet de loi et le projet de règlement grand-ducal sous avis entendent transposer en droit national les nouvelles dispositions de la directive 2006/24/CE (modifiant la directive 2002/58/CE précitée) 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.

2. Modifications apportées par la directive 2006/24/CE

La directive sous rubrique, censée renforcer la lutte contre le terrorisme et la grande criminalité, vise à harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques en matière de conservation des données. L'objectif est de garantir la disponibilité de ces données afin de pouvoir rechercher, détecter et poursuivre les infractions graves.

La directive définit notamment:

- les catégories de données à conserver;
- la durée de conservation;
- les conditions à observer pour le stockage des données conservées, et
- les principes à respecter en matière de sécurité des données.

La renégociation au niveau européen de la question de la conservation des données des communications électroniques a fait l'objet de discussions fort controversées. Ainsi, la Cour constitutionnelle allemande a déclaré une loi afférente comme anticonstitutionnelle puisqu'elle était jugée peu transparente, sans suffisamment de garde-fous quant à l'utilisation ultérieure des données, violant la vie privée des citoyens non suspects, et disproportionnée par rapport à son objectif, notamment la lutte contre la criminalité grave et le terrorisme.

3. La transposition de la directive 2006/24/CE en droit luxembourgeois

Le projet de loi sous avis a pour objet de préciser ce qu'il y a lieu d'entendre par des "*infractions graves*" pour lesquelles un stockage des données des communications électroniques est obligatoire, et de déterminer quelles données sont à retenir par les opérateurs et fournisseurs de service.

En outre, la durée obligatoire de conservation des données est ramenée de 12 à 6 mois.

Nul ne conteste que le stockage de données relatives au trafic des communications fait partie intégrante de la lutte contre la criminalité grave. Nul ne conteste non plus qu'il s'agit en l'occurrence d'un sujet très délicat qui touche à la vie privée des citoyens et au secret professionnel de certaines professions telles que les médecins, les avocats, etc.

Il en est de même du secret des sources des journalistes; faut-il rappeler dans ce contexte l'affaire de la confiscation de données qui, il y a quelques années, a été ordonnée par un ministre opposé à un quotidien et son rédacteur en chef, afin d'établir les sources de supposées indiscrétions, somme toute insignifiantes, et qui ne relevaient certainement pas de la "*criminalité grave*"?

Même si une partie des citoyens semble minimiser le droit à la protection de la vie privée par rapport à l'aspiration à la sécurité (du genre: "*Je n'ai rien à cacher, donc je ne vois aucun inconvénient à être contrôlé et surveillé*"), il faut toutefois reconnaître que les différentes données personnelles collectées dans de nombreuses bases de données, de même que l'explosion du nombre de caméras de surveillance, menacent le respect de la vie privée de tous ceux qui demandent l'application de leur droit afférent.

Par ailleurs, nombreux sont ceux qui estiment que la conservation généralisée d'informations n'apporte pas de solution aux problèmes de sécurité et n'offre aucune garantie contre le terrorisme et la grande criminalité.

Il est en effet fréquent que les opérateurs ne disposent pas des moyens techniques requis pour pouvoir identifier l'utilisateur de services de télécommunications. Ainsi, on ne peut par exemple pas déterminer si l'utilisateur final a lui-même consulté un site web, ni quel site Internet est concerné, du fait que souvent plusieurs utilisateurs se cachent derrière une seule adresse IP. En outre, les données sur le trafic Internet sont inutilisables en tant que pièce à conviction en raison du fait qu'elles peuvent très facilement être falsifiées ou manipulées par des individus ayant des connaissances informatiques avancées.

Comme par ailleurs les usagers de cartes prépayées de la téléphonie mobile ne sont pas obligés de déclarer leur identité, les communications au départ ou à l'arrivée à partir des appareils visés ne sauront être attribuées à un usager déterminé.

Les délinquants de la grande criminalité ne se heurteront donc certainement pas aux dispositions légales qui nous préoccupent; la généralisation de la conservation des données touchera plutôt les simples citoyens qui sont, a priori, tous considérés comme suspects ou potentiellement dangereux.

Comme le stockage des données en question empiète sur la vie quotidienne de tout un chacun et menace les valeurs et les libertés fondamentales érigées en principes confirmés par le traité de Lisbonne, notamment par la charte européenne des droits fondamentaux, il s'agira tout d'abord de protéger le droit des citoyens à la confidentialité lorsqu'ils utilisent des services de communications électroniques, condition que, selon la Chambre des fonctionnaires et employés publics, le projet de loi sous avis ne remplit pas pour les deux raisons qui suivent.

a) description de la finalité

Selon la directive 2006/24/CE, le terme "*infraction grave*" devrait être clairement défini et encadré; tout autre traitement devrait être exclu ou strictement limité, sur la base de garanties spécifiques.

Le projet de loi entend répondre à cette obligation en considérant comme graves les infractions dont le maximum de la peine est égal ou supérieur à un an d'emprisonnement.

Étant donné que par cette définition la très grande majorité des infractions rentrent dans le champ d'application de la loi sous examen, la Chambre estime qu'il n'y a pas de rapport raisonnable entre le but recherché (la répression des infractions relevant de la grande criminalité et du terrorisme) et les moyens mis en œuvre pour y arriver.

b) limitation de l'accès

Les données stockées par les fournisseurs de services de communications électroniques devraient être mises à la disposition des **seuls** services répressifs expressément désignés, en l'occurrence les autorités judiciaires, lorsqu'une telle mise à disposition est nécessaire, appropriée et proportionnée pour la recherche, la détection, la poursuite et/ou la prévention des infractions dans le cadre strict d'une instruction judiciaire ordonnée par un juge d'instruction sur base de soupçons concrets.

La disposition introduite dans le projet de loi sous avis, permettant aux fournisseurs et opérateurs de services de communications électroniques de déléguer l'exécution de l'obligation de stockage des données à une ou plusieurs entités tierces, publiques ou privées, est totalement contraire à l'article 7 de la directive 2006/24/CE (protection et sécurité des données), qui oblige en effet les fournisseurs de services de communications électroniques à respecter un minimum de principes pour assurer la sécurité des traitements des données, notamment le principe de sécurité organisationnelle et technique et de limitation de l'accès aux données.

Comme le projet de loi reste totalement muet sur les conditions de la délégation prévue, de même que sur le statut et la surveillance d'un tel "*gestionnaire-bis*" des données, et comme il permet même une multiplication des acteurs appelés à gérer les données, la confidentialité est sérieusement menacée, ceci d'autant plus que même une exportation des données auprès d'un ou de plusieurs gestionnaires en dehors du territoire national n'est pas exclue.

4. Projet de règlement grand-ducal

Étant donné que les technologies des communications électroniques se développent rapidement, en particulier en ce qui concerne la téléphonie et Internet, il est primordial que, dans la lutte contre la grande criminalité, le cadre légal puisse rapidement suivre l'évolution des protocoles techniques. Le recours à un règlement grand-ducal semble donc, en principe, de mise.

En ce qui concerne toutefois le règlement grand-ducal annexé au projet de loi sous avis, la Chambre des fonctionnaires et employés publics se pose des questions sur la technique législative appliquée en l'occurrence.

Ainsi, une partie des définitions des notions en la matière figurent dans une loi, notamment celle du 30 mai 2005 – et non pas du "5" mai 2005, comme il est erronément écrit au 3^e alinéa du préambule – alors que les définitions complémentaires issues de la directive 2006/24/CE (à l'exception de celle de "*l'utilisateur*", qui figure déjà dans la loi précitée) sont reprises dans le projet de règlement grand-ducal sous avis.

* * * * *

À la lumière des réflexions qui précèdent, la Chambre des fonctionnaires et employés publics ne se voit pas en mesure de marquer son accord avec les projets de loi et de règlement grand-ducal lui soumis pour avis.

Ainsi délibéré en séance plénière le 8 juin 2010.

Le Directeur,

G. MULLER

Le Président,

E. HAAG