



CHAMBRE DES DÉPUTÉS

Session ordinaire 2009-2010

AT/vg

Commission de l'Enseignement supérieur, de la Recherche, des Media et des Communications

Procès-verbal de la réunion du 28 juin 2010

ORDRE DU JOUR :

1. Adoption des projets de procès-verbal des réunions des 7 et 16 juin 2010
2. 6113 Projet de loi portant modification des articles 5 et 9 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
- Rapporteur : Madame Christine Doerner
- Examen de l'avis du Conseil d'Etat
3. COM (2010) 253
COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN, AU CONSEIL, AU COMITE ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS

RAPPORT D'AVANCEMENT SUR LE MARCHE UNIQUE EUROPEEN DES COMMUNICATIONS ELECTRONIQUES DE 2009 (15e RAPPORT)
- Rapporteur : Monsieur Lucien Thiel
- Examen du document
4. Divers

*

Présents : M. Claude Adam, Mme Sylvie Andrich-Duval, M. Eugène Berger, Mme Anne Brasseur, Mme Claudia Dall'Agnol, M. Ben Fayot, M. Claude Haagen, M. Norbert Hauptert, M. Lucien Thiel

M. François Biltgen, Ministre des Communications et des Médias
M. Luc Reding, du Ministère de la Justice
Mme Michèle Bram, du Ministère d'Etat, Service des Médias et des Communications

Mme Anne Tescher, de l'Administration parlementaire

Excusés : M. Jean Colombera, Mme Christine Doerner, M. Marcel Oberweis

*

Présidence : M. Lucien Thiel, Président de la Commission

*

1. Adoption des projets de procès-verbal des réunions des 7 et 16 juin 2010

Les projets de procès-verbal des réunions des 7 et 16 juin 2010 sont adoptés.

2. 6113 Projet de loi portant modification des articles 5 et 9 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

M. le Ministre rappelle en guise d'introduction que le projet de loi sous rubrique revêt une certaine urgence, puisque le Luxembourg a un retard sérieux dans la transposition de la directive 2006/24/CE. L'orateur explique que l'élaboration du projet de loi a été assez complexe puisqu'il fallait concilier les intérêts divergents du domaine des télécommunications et de celui de la justice.

La Commission procède à l'examen de l'avis du Conseil de l'Etat du 22 juin 2010.

Article 1^{er} - Paragraphe 1^{er}

Le **Conseil d'Etat** prend note que les modifications engendrées par le paragraphe 1 de l'article 1^{er} consistent à :

1. limiter l'accès des autorités judiciaires aux données conservées pour les infractions qui emportent une peine égale ou supérieure à un an; comme ceci relève du Code d'instruction criminelle et comme les opérateurs devront de toute façon tout conserver, ne sachant *a priori* ni aux fins de recherche de quelles infractions serviront les données ni quelle donnée sera utile à cette même fin, le Conseil d'Etat recommande de supprimer cet ajout, qui fait d'ailleurs l'objet de l'article 2;
2. préciser la durée de conservation des données de 6 mois qui débute avec la date de la communication;
3. étendre l'obligation de conservation aux appels infructueux; étant donné que ceci reflète les dispositions de l'article 3, paragraphe 2 de la directive, le Conseil d'Etat peut se déclarer d'accord avec cette précision, même si, dans une approche juridique, elle est superflue car peu importe si un appel est fructueux ou infructueux, il constitue une donnée du trafic;
4. prévoir un mécanisme de délégation d'exécution des obligations légales des opérateurs vers des tiers. Le Conseil d'Etat s'interroge sur la portée de cette disposition. Les auteurs du projet de loi prévoient-ils avec la sous-traitance un transfert de responsabilité? Ou s'agirait-il d'un simple rapport de droit privé? L'Institut luxembourgeois de régulation aurait-il éventuellement ce rôle de sous-traitant? Quels sont les risques liés à une centralisation auprès d'un seul sous-traitant, qui serait en plus une entité de droit public? Si le législateur

veut prévoir un système de sous-traitance, n'y aurait-il pas lieu d'en prévoir un encadrement législatif spécifique? D'après le Conseil d'Etat, les opérateurs seront les seuls responsables de la conservation des données, même s'ils organisent un régime technique de sous-traitance régi par le droit privé. En l'absence de précisions suffisantes quant aux organismes concernés, pour des raisons d'insécurité juridique et dans le souci de la préservation de la protection en cascade des données, le Conseil d'Etat doit s'opposer formellement à cette disposition qui ne répond pas aux prescriptions de l'article 32(3) de la Constitution et qu'il demande de supprimer.

5. ajouter au règlement grand-ducal sur les catégories de données les formes et les modalités suivant lesquelles les données sont à mettre à disposition des autorités judiciaires. Comme la loi ne renvoie ni à un règlement sur cette question ni à un système d'accès direct comme prévu à d'autres banques de données, le Conseil d'Etat insiste à ce que la dernière phrase de l'article sous avis soit supprimée. En outre, il a une préférence pour les procédures généralement applicables en cette matière et prévues par le Code d'instruction criminelle.

La **Commission** de l'Enseignement supérieur, de la Recherche, des Media et des Communications formule les observations suivantes :

- Quant au point 1 - les infractions graves

Le Conseil d'Etat accepte la définition de l'infraction grave qui emporte une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

La Commission s'est interrogée sur la nature des infractions tombant ainsi sous l'application de la loi.

La **Chambre des Fonctionnaires et Employés publics** critique cette définition de l'infraction grave dans son avis du 9 juin 2010, estimant 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, à savoir la répression des infractions relevant de la grande criminalité et du terrorisme, et les moyens mis en œuvre pour y arriver.

A la demande des membres de la Commission, M. le Ministre s'engage à fournir une **liste des différentes infractions et des peines y relatives** en vue d'intégrer ces précisions dans le rapport de la Commission.

M. le Ministre informe dans ce contexte, qu'il envisage de toute façon de revoir la durée des peines pour différentes infractions dans une prochaine étape. Le problème persiste surtout au niveau des lois spéciales, lesquelles prévoient le plus souvent des peines très dures.

L'expert gouvernemental explique en outre que le contexte de la directive est le financement du terrorisme, la criminalité organisée et le blanchiment d'argent. Or, ces infractions graves ne sont pas des infractions primaires, mais sont détectées par le biais d'infractions mineures. C'est n'est que dans une seconde étape qu'un lien vers la criminalité organisée ou le terrorisme est constaté. Voilà pourquoi il n'est pas opportun d'élever le seuil des peines à deux ans, puisque les infractions mineures menant éventuellement vers la criminalité organisée, le terrorisme ou encore le blanchiment d'argent, ne tomberont plus sous l'application de la législation sur la rétention des données. En augmentant le seuil de peine à

2 ans, le Luxembourg serait certainement soumis aux critiques de la part du Groupe d'Action financière (GAFI).

- Quant au point 4 – Sous-traitance du stockage des données

Le Conseil d'Etat a émis une opposition formelle quant à la possibilité de la sous-traitance du stockage de données.

La délégation d'exécution des obligations légales des opérateurs vers des tiers aurait eu l'avantage de centraliser le stockage et de garantir ainsi un certain standard de sécurité au niveau de la conservation des données. De même, l'accès des autorités judiciaires aurait été facilité. Par ailleurs, les fournisseurs de communications électroniques auraient été ainsi dispensés des frais supplémentaires engendrés par la conservation des données. Or, il faut souligner à ce propos que les fournisseurs touchés par la conservation des données n'ont jamais manifesté leur opposition à cette obligation qui leur incombe en vertu de cette législation.

La **Commission nationale pour la protection des données** se déclare réservée à la question de la sous-traitance dans son avis du 26 avril 2010, et ceci pour les raisons suivantes : D'abord, une telle sous-traitance n'est pas prévue par la directive 2006/24/CE. De même, la CNPD s'interroge sur l'opportunité de prévoir la faculté d'externalisation du stockage des données confidentielles concernant des millions de communications. Elle est d'avis 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 des autorités policières et judiciaires.

En tenant compte de l'opposition formelle du Conseil d'Etat, ainsi que des réticences de la Commission nationale pour la protection des données, **la Commission de l'Enseignement supérieur, de la Recherche, des Media et des Communications** décide de supprimer **la disposition autorisant la sous-traitance** du stockage des données.

En ce qui concerne la sécurité de la conservation des données auprès des fournisseurs de communications électroniques, la Commission nationale pour la protection des données est d'ores et déjà en charge d'assurer l'application des dispositions de la loi modifiée du 30 mai concernant la protection de la vie privée dans le secteur des communications électroniques et de ses règlements d'exécution par le biais de l'article 12 de la loi modifiée précitée.

Article 1^{er} – paragraphe 2

- Quant à l'exigence d'une autorisation judiciaire préalable

La **Commission nationale pour la protection des données** insiste dans son avis à ce que l'accès aux données conservées soit soumis à une autorisation judiciaire préalable. La CNPD invoque que le projet de loi laisse inchangés 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.

Selon la CNPD, 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 surveillée à son insu, les données de connexion et de localisation de tout un chacun étant librement disponibles pour la police.

Il est souligné que la cour constitutionnelle allemande, dans un arrêt du 2 mars 2010, se prononce également pour une autorisation judiciaire préalable.

La CNPD donne 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, il en résulterait 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 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 1er 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. » (Arrêt 106/08 V du 26 février 2008).

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* ». Dès lors, dans les deux cas, le repérage est impossible en enquête de flagrance.

La CNPD 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.» 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.

Dans son avis du 22 juin 2010, le **Conseil d'Etat** reprend la recommandation de la CNPD, qui exige une autorisation judiciaire préalable pour donner accès aux données du trafic. A cet effet, la Haute Corporation propose de modifier le paragraphe 2 des articles 5 et 9 pour en assurer la cohérence avec 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, en renvoyant également à l'arrêt de la Cour d'appel précité.

Puisqu'il s'agit d'une critique substantielle de la CNPD et à la lumière de la recommandation du Conseil d'Etat, **la Commission se rallie à cette proposition.**

L'expert gouvernemental examinera en détail l'envergure de cette modification en vue de la prochaine réunion de la Commission du 1^{er} juillet.

Le règlement grand-ducal

Le **Conseil d'Etat** formule certaines critiques à l'égard du règlement grand-ducal afférent. La Haute Corporation insiste à ce que ce règlement se limite à sa base légale, à savoir les catégories de données. Les autres dispositions de la directive telles que les **nouvelles notions à définir**, la **sécurité des données** et l'**établissement des statistiques (articles 4 à 6** du règlement grand-ducal) seront ainsi à introduire dans la loi.

Quant aux exigences relatives à la **sécurité du stockage** des données, plutôt que de prévoir une référence aux dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel au sein du règlement grand-ducal précité, le **Conseil d'Etat insiste** à ce qu'elles soient inscrites **au sein du projet de loi.**

M. le Ministre est en principe d'accord avec cette proposition. La Commission s'interroge sur les implications du terme « insiste » employé par le Conseil d'Etat. Le ministère analysera s'il est envisageable de se rallier à la proposition du Conseil d'Etat sans emprunter la voie d'un amendement. M. le Ministre souligne que, vu l'urgence de la transposition de la directive, il est préférable d'éviter le recours aux amendements. La Commission tranchera sur ce point dans sa réunion du 1^{er} juillet.

Dans le contexte de la sécurité des données, M. le Ministre informe que la mise en vigueur du traité de Lisbonne permet dorénavant une législation horizontale au sujet de la protection des données, ce qui est par ailleurs un projet de la Commissaire Viviane Reding. Il s'en suit que les lois sectorielles de la protection de données seront de toute façon revues dans les prochaines années.

Tableau de concordance

Comme il s'agit de transposer une directive européenne, le Conseil d'Etat déplore que les auteurs du projet de loi sous avis n'aient pas ajouté un tableau de concordance permettant de voir dans quels textes législatifs les « autres éléments » de la directive sont ou seront transposés.

L'expert gouvernemental souligne que le principe de la rétention de données a déjà été retenu dans la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques. Le projet de loi sous examen n'entraîne que quelques ajustements ponctuels en vue de la transposition intégrale de la directive.

A la demande de la Commission, M. le Ministre s'engage à fournir un tableau de concordance qui pourra être intégré dans le rapport de la Commission.

*

La Commission rediscutera les propositions du Conseil d'Etat dans sa réunion du 1^{er} juillet. L'adoption d'un projet de rapport est prévue pour la réunion du 5 juillet 2010.

3. COM (2010) 253 - Rapport d'avancement sur le marché unique européen des communications électroniques de 2009 (15^e rapport)

- Rapporteur : Monsieur Lucien Thiel

En favorisant l'apparition de services de communications électroniques novateurs, la réglementation européenne a apporté aux Européens un certain nombre d'avantages, mais il reste encore des obstacles sérieux à surmonter, comme par exemple l'indépendance et l'efficacité des autorités réglementaires nationales (ARN) ou les différences notables observées entre les Etats membres en ce qui concerne les prix de gros et les prix de détail. Ainsi, en ce qui concerne les tarifs de gros de terminaison d'appel mobile, on observe en moyenne un rapport de 1 à 2,5 entre les Etats membres où ils sont les plus élevés et ceux où ils sont les plus bas. Les consommateurs et les entreprises restent confrontés à 27 marchés différents et ne peuvent donc pas tirer parti du potentiel économique d'un marché unique.

Certains marchés des communications électroniques, tels que celui de la téléphonie vocale, atteignent le stade de la maturité et la croissance dans le secteur ralentit. A l'avenir, seuls de nouveaux modèles d'activité et des innovations dans le domaine des services permettront de garantir une croissance durable.

Dans le cadre de la stratégie «Europe 2020», la Commission a adopté une stratégie numérique pour l'Europe exposant un certain nombre de mesures stratégiques destinées à stimuler l'économie numérique, à favoriser la transition vers un environnement à haut débit et à renforcer le marché unique en ligne. Ces mesures doivent être associées à des approches réglementaires cohérentes et à une mise en œuvre efficace des mesures correctrices.

Dans le droit fil de l'agenda numérique et des mesures que ce dernier prévoit en ce qui concerne le spectre radioélectrique, le service universel, le traitement réglementaire des NGA et la protection de la vie privée, la Commission va également adopter un certain nombre de mesures ciblées:

- (1) pour régler les problèmes liés à la disparité des approches réglementaires et à l'application des mesures correctrices, qui ne se fait pas de manière efficace et en temps opportun;
- (2) pour établir des bases solides afin que la mise en œuvre du cadre réglementaire révisé se déroule correctement et en temps voulu;
- (3) pour garantir le fonctionnement efficace de l'Organe des régulateurs européens des communications électroniques (ORECE).

4. **Divers**

- M. le Ministre informe que l'avant-projet de loi sur les services postaux a été adopté lors du Conseil de Gouvernement du 25 juin 2010. Il est retenu de présenter cet avant-projet de loi à la Commission lors de la réunion du 12 juillet 2010.

- Les prochaines réunions de la Commission auront lieu les 1^{er}, 5, 8, 12 et 19 juillet 2010.

Luxembourg, le 30 juin 2010

La secrétaire,
Anne Tescher

Le Président,
Lucien Thiel