N° 201

SÉNAT

SESSION ORDINAIRE DE 2004-2005

Annexe au procès-verbal de la séance du 16 février 2005

RAPPORT

FAIT

au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de résolution présentée au nom de la délégation pour l'Union européenne en application de l'article 73 bis *du Règlement par M. Alex TÜRK sur le projet de décision-cadre sur la* **rétention** *de* **données** *traitées et stockées en rapport avec la* **fourniture** *de* **services** *de* **communications électroniques** *accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la* **prévention**, *la* **recherche**, *la* **détection**, *la* **poursuite** *des* **délits** *et d'***infractions pénales**, *y compris du terrorisme (E 2616),*

Par M. Hugues PORTELLI,

Sénateur.

(1) Cette commission est composée de : M. Jean-Jacques Hyest, *président* ; MM. Patrice Gélard, Bernard Saugey, Jean-Claude Peyronnet, François Zocchetto, Mme Nicole Borvo Cohen-Seat, M. Georges Othily, *vice-présidents* ; MM. Christian Cointat, Pierre Jarlier, Jacques Mahéas, Simon Sutour, *secrétaires* ; M. Nicolas Alfonsi, Mme Michèle André, M. Philippe Arnaud, Mme Eliane Assassi, MM. Robert Badinter, José Balarello, Laurent Béteille, Mme Alima Boumediene-Thiery, MM. François-Noël Buffet, Christian Cambon, Marcel-Pierre Cléach, Pierre-Yves Collombat, Raymond Courrière, Jean-Patrick Courtois, Yves Détraigne, Michel Dreyfus-Schmidt, Pierre Fauchon, Gaston Flosse, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Charles Gautier, Philippe Goujon, Mme Jacqueline Gourault, MM. Charles Guené, Hubert Haenel, Jean-René Lecerf, Mme Josiane Mathon, MM. Hugues Portelli, Henri de Richemont, Jean-Pierre Sueur, Alex Türk, Jean-Paul Virapoullé, Richard Yung.

Voir le numéro :

Sénat : 128 (2004-2005)

Union européenne.

S O M M A I R E

LES CONCLUSIONS DE LA COMMISSION

Réunie le mercredi 16 février 2005 sous la présidence de M. Jean-Jacques Hyest, président, la commission des Lois a examiné, sur le rapport de M. Hugues Portelli, la proposition de résolution (n° 128) présentée par M. Alex Türk au nom de la délégation pour l'Union européenne sur le projet de décision-cadre sur la **rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques** accessibles au public ou de données transmises via des réseaux de communication publics, aux fins de la **prévention, la recherche, la détection, la poursuite des délits et d'infractions pénales, y compris du terrorisme** (E-2616).

Le rapporteur a d'abord indiqué que le projet de décision-cadre répondait aux **engagements pris par le Conseil européen** le 25 mars 2004 dans sa déclaration sur la lutte contre le terrorisme, après les attentats de Madrid du 11 mars 2004.

Soulignant que les législations relatives à la conservation des données de trafic variaient considérablement entre les Etats membres, il a estimé une **harmonisation indispensable** à l'efficacité des enquêtes sur les activités criminelles transnationales. Il a rappelé qu'une telle harmonisation devait respecter les critères fixés par l'article 8 de la Convention européenne des droits de l'Homme s'agissant de l'ingérence des autorités publiques dans la vie privée des personnes.

Sur proposition de son rapporteur, la commission a adopté, sous réserve d'une modification rédactionnelle, la proposition de résolution qui tend à :

- **approuver le principe d'une harmonisation européenne** en matière de conservation, par les opérateurs économiques, des données stockées et traitées dans le cadre de la fourniture de services de communications électroniques ;

- souligner que le projet de décision-cadre ne permet pas, dans sa version actuelle, de réaliser cette harmonisation et de **concilier le besoin d'efficacité des enquêtes et la protection des droits individuels** ;

- inviter le Gouvernement à :

● œuvrer au sein du Conseil pour **rétablir une durée maximale de conservation des données** ;

● demander à la Commission européenne de **procéder à une évaluation du surcoût** de la conservation des données de trafic pour les fournisseurs de services et à une étude sur les différentes possibilités concernant le régime d'indemnisation de ces opérateurs.

EXPOSÉ GÉNÉRAL

Mesdames, Messieurs,

Le Sénat a été saisi, le 21 juin 2004, en application de l'article 88-4 de la Constitution, d'un projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communication publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme (texte E-2616).

Ce projet de décision-cadre est issu d'une proposition de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni, le droit d'initiative étant partagé, dans le domaine de la coopération policière et judiciaire en matière pénale, entre la Commission européenne et les Etats membres.

Le recours croissant à des services de communications électroniques ignorant les frontières pour commettre des délits et leur utilisation avérée dans les attentats de Madrid le 11 mars 2004 ont conduit le Conseil européen, lors de sa réunion du 25 mars 2004, à envisager l'adoption, d'ici juin 2005, de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications. Les Etats membres ont ainsi réaffirmé leur engagement à renforcer la coopération judiciaire.

Le projet de décision-cadre, conformément à l'objectif fixé par le Conseil européen, tend à garantir les moyens de la prévention, de la recherche, de la détection ou de la poursuite de délits et d'infractions pénales grâce à la rétention de données de connexion. Il ne concerne que les données de communication générées par les fournisseurs de services de communications dans le cadre de la prestation de leurs services, et non le contenu des communications.

Si de nombreux Etats, tels la France, ont mis en place des dispositifs prévoyant la conservation de ces données par les opérateurs, le nécessaire développement de la coopération judiciaire et policière appelle une harmonisation des catégories de données et de leurs délais de conservation.

Le projet de décision-cadre soulève certaines questions de principe qui ont conduit la délégation pour l'Union européenne du Sénat à adopter, à l'unanimité, sur l'initiative de notre collègue M. Alex Türk, une proposition de résolution renvoyée à votre commission.

I. LES PROGRÈS DE LA COOPÉRATION POLICIÈRE ET JUDICIAIRE EUROPÉENNE FACE AU DÉVELOPPEMENT DU TERRORISME

L'Union européenne a mis en place plusieurs dispositifs pour renforcer la lutte contre le terrorisme et la criminalité organisée depuis le 11 septembre 2001.

A. UNE LUTTE RENFORCÉE CONTRE LA CRIMINALITÉ TRANSNATIONALE APRÈS LES ATTENTATS DU 11 SEPTEMBRE 2001

1. Un cadre de coopération judiciaire plus adapté depuis le traité d'Amsterdam

L'action concertée des Etats membres dans la lutte contre le terrorisme se situe dans le cadre de la coopération judiciaire en matière pénale, qui a connu des progrès notables depuis les attentats perpétrés aux Etats-Unis.

La coopération dans les domaines de la justice et des affaires intérieures s'appuie sur une méthode intergouvernementale. L'ajout d'un troisième pilier à l'édifice communautaire (titre VI du traité sur l'Union européenne, TUE), puis la création d'un espace de liberté, de sécurité et de justice par le traité d'Amsterdam, ont donné à l'Union européenne les moyens d'une politique cohérente dans ces domaines. Parmi les instruments juridiques de cette coopération, la décision-cadre, substituée à l'action commune, se rapproche dans son esprit de la directive et de ses mesures d'application[1].

C'est en application de l'article 31, 1, c, du traité sur l'Union européenne, aux termes duquel l'action en commun dans le domaine de la coopération judiciaire en matière pénale vise notamment à « *assurer, dans la mesure nécessaire à l'amélioration de cette coopération, la* ***compatibilité des règles applicables dans les Etats membres*** », que la France, l'Irlande, le

[1] *Aux termes de l'article 34, paragraphe 2, b, du traité sur l'Union européenne, les décisions-cadres visent à rapprocher les dispositions législatives et réglementaires des Etats membres, qu'elles lient quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. Le Conseil doit statuer à* ***l'unanimité*** *sur le projet qui fait l'objet d'un avis du Parlement européen (art. 39 TUE).*

Royaume-Uni et la Suède ont présenté un projet de décision-cadre sur la rétention des données de connexion.

Suivant une appréciation inverse à celle de ces quatre Etats, **la Commission européenne a estimé que cette initiative était dépourvue de fondement juridique**, au motif qu'elle ne relèverait pas de la coopération judiciaire, mais de la réglementation du marché intérieur (art. 95 du traité instituant la Communauté européenne, TCE), c'est-à-dire du premier pilier. Dans une telle hypothèse, seule la Commission pourrait déposer une proposition en la matière (art. 251 TCE).

L'appréciation de la Commission s'appuie sur le précédent de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, adoptée sur le fondement de l'article 95 du traité instituant la Communauté européenne[1]. Si la décision-cadre était adoptée définitivement, la Commission pourrait former un recours pour incompétence devant la Cour de justice des communautés européennes (art. 35 TUE). Elle pourrait auparavant présenter une initiative concurrente à celle des Etats membres. Le texte de la Commission suivrait alors une procédure d'adoption différente, le Conseil statuant à la majorité qualifiée et le Parlement exerçant un pouvoir de codécision.

2. L'accélération des efforts de coopération depuis les attentats du 11 septembre 2001

Au cours des réunions qui ont suivi les attentats du 11 septembre 2001, les Etats membres ont pris de nouvelles initiatives pour renforcer leur lutte contre la criminalité transnationale, accélérant le processus décisionnel initié lors du Conseil européen de Tampere, les 15 et 16 octobre 1999, consacré à la création de l'espace de liberté, de sécurité et de justice.

Ce Conseil avait invité les Etats membres à mettre en œuvre le principe de reconnaissance mutuelle des décisions judiciaires. Ainsi, la décision-cadre du 13 juin 2002 a substitué au système de l'extradition un **mandat d'arrêt européen**, chaque autorité judiciaire nationale devant par conséquent reconnaître, moyennant des contrôles minimaux, la demande de remise d'une personne formulée par l'autorité judiciaire d'un autre Etat membre[2].

---

[1] *La Commission estime que le projet de décision-cadre se situe dans le prolongement de l'article 15 de la directive 2002/58/CE, qui prévoit que les Etats membres «* peuvent adopter des mesures législatives prévoyant la conservation des données pendant une durée limitée *» pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.*

[2] *L'application du mandat d'arrêt européen par la France a nécessité une révision constitutionnelle (loi constitutionnelle n° 2003-267 du 25 mars 2003 relative au mandat d'arrêt européen), préalable à son inscription dans le code de procédure pénale, à l'initiative de notre collègue M. Pierre Fauchon, par l'article 17 de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*

La **décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme** vise à rapprocher les définitions d'infractions terroristes dans tous les Etats membres et les oblige à prendre les mesures nécessaires pour rendre punissables la direction d'un groupe terroriste et la participation aux activités d'un tel groupe.

L'Union européenne a par ailleurs adopté la décision-cadre relative aux **équipes communes d'enquête**, celle concernant le blanchiment d'argent, l'identification, le dépistage, le gel ou la saisie et la confiscation des instruments et des produits du crime, la décision portant création d'**Eurojust** et celle relative à l'application de mesures spécifiques de coopération policière et judiciaire en matière de lutte contre le terrorisme.

Eurojust, unité de coopération judiciaire

Eurojust, organe de l'Union européenne doté de la personnalité juridique créé par la décision du Conseil du 28 février 2002[1], exerce ses missions depuis le 29 avril 2003, en luttant contre toutes les formes de criminalité organisée.

Composée de procureurs, magistrats ou officiers de police des Etats membres de l'Union, cette unité est chargée d'**améliorer la coordination des enquêtes et des poursuites entre les autorités compétentes** et de **promouvoir la coopération** par la mise en œuvre de l'entraide judiciaire internationale et l'exécution des demandes d'extradition.

Eurojust peut à cette fin échanger des informations avec les Etats membres et assure leur information réciproque. Elle peut leur suggérer d'entreprendre une enquête ou des poursuites sur des faits précis et apporte son concours pour la traduction, l'interprétation et l'organisation de réunions de coordination. Eurojust s'appuie sur le réseau judiciaire européen, qui fournit des informations sur l'application des règles communautaires par les Etats et le fonctionnement de la justice dans chacun d'eux.

Un accord entre Eurojust et Europol a été signé le 9 juin 2004 pour améliorer la coopération de ces offices dans la lutte contre les formes graves de criminalité transfrontalière, en particulier lorsqu'il s'agit de criminalité organisée, par l'échange d'informations opérationnelles, stratégiques et techniques, et la coordination de leurs activités.

Europol, office européen de police

Issu d'un office né en janvier 1994 et dont les activités se limitaient à la lutte contre la drogue, Europol a été créé par une convention entrée en vigueur le 1er octobre 1998. L'office, dont le mandat a été étendu le 1er janvier 2002 à **toutes les formes graves de la criminalité internationale** visées à l'annexe de la convention Europol, a pour objet d'améliorer l'efficacité des services compétents des Etats membres et leur coopération dans le cadre de la prévention et de la lutte contre ces activités.

Europol soutient ainsi les actions répressives des Etats membres dans des domaines tels que les réseaux d'immigration clandestine, le terrorisme, la traite des êtres humains, la pornographie enfantine, le faux monnayage et le blanchiment d'argent, dans la mesure où existe une organisation criminelle affectant au moins deux Etats membres.

---

[1] *Cette décision a été transposée dans le code de procédure pénale (art. 695-4 à 695-7) par la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*

L'office intervient en **facilitant l'échange d'informations** entre les officiers de liaison Europol détachés auprès de lui par les Etats membres, en établissant des rapports stratégiques et en apportant son expertise et son assistance technique aux enquêtes.

Europol emploie près de 500 personnes, dont 60 officiers de liaison représentant notamment les services de police, de douane, de gendarmerie et d'immigration des Etats membres.

Enfin, le Centre de situation conjoint de l'Union (SITCEN) doit fournir au Conseil, depuis le 1er janvier 2005, des évaluations stratégiques des menaces terroristes à partir des renseignements communiqués par les services nationaux.

B. UN BILAN CONTRASTÉ ET DE NOUVELLES INITIATIVES APRÈS LES ATTENTATS DE MADRID

1. Un bilan contrasté des actions de lutte contre le terrorisme de l'Union européenne

L'évaluation conduite après les attentats de Madrid des actions européennes de lutte contre le terrorisme a mis en lumière les difficultés et les lacunes qui subsistent dans l'application de plusieurs de ces mesures.

Dans son rapport du 8 juin 2004 sur la mise en œuvre de la décision-cadre du 13 juin 2002 relative à la lutte contre le terrorisme, la Commission a relevé que les dispositions de ce texte avaient été très inégalement appliquées par les Etats membres. Ainsi, seuls quatre Etats membres disposaient alors d'une législation répondant aux obligations fixées par l'article 3 de la décision-cadre relatif aux infractions liées aux activités terroristes.

De même, au 29 novembre 2004, cinq Etats sur vingt-cinq n'avaient pas encore pris de mesures d'application de la décision établissant Eurojust[1].

2. Les objectifs prioritaires définis après les attentats du 11 mars 2004

Le 17 juin 2004, le Conseil européen a adopté un plan d'action révisé reprenant les mesures décidées au lendemain des attentats de New-York et Washington. Les cinq objectifs prioritaires de ce plan visent à :

- intensifier le dialogue avec les pays tiers ;

---

[1] *D'après l'annexe au plan d'action de l'Union européenne pour la lutte contre le terrorisme, mise à jour du 14 décembre 2004, DOC 16090/04. Ces cinq Etats sont l'Espagne, la Grèce, l'Italie, le Luxembourg et Chypre.*

- réduire l'accès des terroristes aux ressources financières et économiques ;

- améliorer la coopération entre les autorités chargées de la sécurité intérieure ;

- protéger les infrastructures publiques et assurer la sécurité des populations en cas d'attaque ;

- contrer les facteurs de développement du terrorisme.

En outre, le Conseil européen a adopté le 5 novembre 2004 le **programme de La Haye** tendant à renforcer la liberté, la sécurité et la justice dans l'Union européenne. Ce programme pluriannuel, qui affirme la volonté de l'Union de **lutter contre le terrorisme dans le respect de l'Etat de droit**, énonce en particulier deux principes concernant l'échange d'informations : la **disponibilité** de l'information à travers l'accès mutuel[1] ou l'intéropérabilité des systèmes, et le **strict respect des règles sur la protection des données**.

Le **coordinateur de la lutte contre le terrorisme** nommé par le Conseil européen le 25 mars 2004, M. Gijs de Vries, devra suivre la mise en œuvre du plan d'action et coordonner les travaux du Conseil de l'Union en matière de lutte contre le terrorisme.

3. La référence au terrorisme dans le traité établissant une Constitution pour l'Europe

L'article I-43 du traité établissant une Constitution pour l'Europe définit une **clause de solidarité entre les Etats membres en cas d'attaque terroriste**. Les modalités de mise en œuvre de cette clause sont fixées par l'article III-329, aux termes duquel « *si un Etat membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine, les autres Etats membres lui portent assistance à la demande de ses autorités politiques* ». Une décision européenne adoptée par le Conseil sur proposition conjointe de la Commission et du ministre des affaires étrangères de l'Union devrait préciser ces modalités.

L'article III-261 du traité prévoit en outre la création au sein du Conseil d'un **comité permanent** chargé d'assurer à l'intérieur de l'Union la promotion et le renforcement de la coopération opérationnelle en matière de sécurité intérieure.

---

[1] *Selon le **principe de disponibilité**, dans l'ensemble de l'Union, tout agent des services répressifs d'un Etat membre qui a besoin de certaines informations dans l'exercice de ses fonctions pourra les obtenir d'un autre Etat membre, l'administration répressive de l'autre Etat membre qui détient ces informations les mettant à sa disposition aux fins indiquées et en tenant compte des exigences des enquêtes en cours dans cet autre Etat.*

II. LA NÉCESSAIRE HARMONISATION DES RÈGLES DE RÉTENTION DES DONNÉES DE COMMUNICATION

L'utilisation des données relatives au trafic des communications s'est révélée très utile dans certaines enquêtes, permettant de remonter à la source de contenus illégaux, tels que des matériaux à caractère pédophile, raciste et xénophobe, ainsi qu'à l'origine d'attaques informatiques, et d'identifier les individus utilisant des réseaux de communications électroniques à des fins criminelles ou terroristes.

A. UNE POSSIBILITÉ ENCADRÉE PAR LE DROIT COMMUNAUTAIRE

Aux termes de l'article 6 du traité sur l'Union européenne, celle-ci respecte les droits fondamentaux tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH). L'**article 8** de cette convention consacre le droit de toute personne au « ***respect de sa vie privée*** *et familiale, de son domicile et de sa correspondance* », une autorité publique ne pouvant s'ingérer dans l'exercice de ce droit que si la loi le permet et s'il s'agit d'une mesure nécessaire, notamment, à la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales[1].

L'article 13, paragraphe 1, de la **directive 95/46/CE** du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données permet aux Etats membres de prendre des mesures législatives visant à limiter la portée des obligations et des droits qu'elle énonce, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder « *la prévention, la recherche, la détection et la poursuite d'infractions pénales* »[2].

En outre, tenant compte du développement de la société de l'information, la **directive 2002/58/CE** du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) précise l'application de l'article 13, paragraphe 1, de la directive 95/46/CE. Son article 15 prévoit ainsi que « *les Etats membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié* », notamment par la nécessité de prévenir, rechercher, détecter ou poursuivre des infractions pénales ou des utilisations non autorisées du système de communications électroniques.

---

[1] *Aux termes de l'article II-67 du traité établissant une Constitution pour l'Europe (partie II relative à la Charte des droits fondamentaux de l'Union) «* toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications *».*

[2] *L'article II-68 du traité établissant une Constitution pour l'Europe prévoit que toute personne a droit à la protection des données à caractère personnel la concernant.*

Dans le programme de La Haye, adopté le 5 novembre 2004, le Conseil européen a soumis le principe de disponibilité, qui s'appliquera à l'échange d'informations en matière répressive à compter du 1er janvier 2008, à une série de conditions reprenant les règles énoncées par ces directives[1].

B. LES DISPARITÉS ENTRE ÉTATS MEMBRES, ENTRAVES À LA COOPÉRATION POLICIÈRE ET JUDICIAIRE

Si tous les Etats membres n'ont pas mis en place une législation obligeant les opérateurs à conserver les données de trafic, on observe, par surcroît, d'importantes variations entre les pays qui ont adopté de tels dispositifs.

1. Le régime français : la conservation des données, dérogation au principe général d'effacement

a) Le caractère dérogatoire de l'obligation de conservation des données de connexion

Comme le rappelle la Commission nationale de l'informatique et des libertés (CNIL) dans son avis sur le projet de décret relatif à la conservation des données de communication[2], la **finalité du traitement** des données à caractère personnel détermine les catégories de données collectées et traitées et leur durée de conservation. Conformément à ce principe de finalité, certaines données de connexion doivent pouvoir être conservées dans un but commercial. En revanche, les traitements justifiés par la sécurité publique et la recherche des infractions pénales sont **dérogatoires** à ce principe.

Aux termes du I de l'article L. 34-1 du code des postes et des communications électroniques, créé par l'article 29 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, « *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic* ».

Ces **données techniques** se distinguent des données administratives relatives aux clients (nom, prénom, adresse, mode de paiement de l'abonnement…). Elles désignent les informations liées à l'utilisation des

---

[1] L'échange d'informations ne peut avoir lieu que pour permettre l'accomplissement de tâches légales, l'intégrité et la confidentialité des données échangées doivent être garanties, des normes communes d'accès aux données et des normes techniques communes doivent être appliquées, le contrôle du respect de la protection des données doit être assuré et les particuliers doivent être protégés contre les utilisations abusives des données et disposer d'un droit de rectification des données inexactes.

[2] Délibération n° 03-056 du 9 décembre 2003 portant avis sur le projet de décret relatif à la conservation des données relatives à une communication par les opérateurs de télécommunications.

réseaux, qu'il s'agisse de communications téléphoniques, de courriers électroniques, d'accès à un site Internet, des services de messages courts (SMS) ou des services de messageries multimédias (MMS)[1], et permettent d'identifier les interlocuteurs, leur localisation et la durée de leur communication.

Les **trois possibilités de dérogation** au principe général d'effacement sont strictement encadrées par l'article L. 34-1 :

- les opérateurs peuvent utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement les données relatives au trafic **pour les besoins de la facturation** et du paiement des prestations de communications électroniques, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, soit au maximum un an[2] ;

- les opérateurs peuvent conserver certaines données en vue d'**assurer la sécurité de leurs réseaux**[3] ;

- l'effacement des données relatives au trafic **peut être différé pour une durée maximale d'un an**, **pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales**, et seulement afin de mettre à disposition de l'autorité judiciaire des informations.

Conformément au principe de finalité, ces trois dérogations visent des catégories de données et des durées de conservation différentes, dont la détermination est renvoyée à un décret en Conseil d'Etat, pris après avis de la CNIL, en cours de finalisation (art. L. 34-1, II, du code des postes et des communications électroniques). Aux termes du projet de décret, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, les opérateurs seraient tenus de conserver les données pendant **un an à compter du jour de leur enregistrement**.

Pour les besoins de la **facturation**, les fournisseurs de services seraient autorisés à conserver certaines données pendant le temps strictement nécessaire à cette finalité, **sans excéder un an à compter du jour de l'enregistrement**. Enfin, la conservation des données nécessaires à la sécurité des réseaux et des installations ne pourrait dépasser **trois mois après l'enregistrement**. Une fois expirés les délais de conservation des données pour les besoins de la facturation ou de la sécurité des réseaux, les opérateurs ne pourront pas utiliser dans ces

---

[1] La nouvelle définition des communications électroniques inscrite à l'article L. 32 du code des postes et des communications électroniques par l'article 2 de la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle permet d'englober toutes les technologies existantes.

[2] Aux termes de l'article L. 34-2, second alinéa, du code des postes et des communications électroniques : « La prescription est acquise, au profit de l'usager, pour les sommes dues en paiement des prestations de communications électroniques d'un opérateur appartenant aux catégories visées au précédent alinéa lorsque celui-ci ne les a pas réclamées dans un délai d'un an courant à compter de la date de leur exigibilité. *»*

[3] Disposition introduite à l'article L. 34-1 du code des postes et des communications électroniques par l'article 20 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

finalités les données conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Les exceptions au principe d'effacement ne visent que les données relatives au trafic, soit exclusivement celles qui portent sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux (art. L. 34-1, V, du code précité)[1].

Le tableau suivant présente les catégories de données qui devraient ou pourraient, selon la finalité, être conservées par les opérateurs, telles que les définit le projet de décret :

	Données conservées pour la recherche, la constatation et la poursuite d'infractions pénales (un an)	**Données conservées pour les besoins de la facturation (un an maximum)**	**Données conservées pour la sécurité des réseaux (trois mois maximum)**
Identification de l'utilisateur	Oui	Oui	Non[2]
Equipements terminaux utilisés	Oui	Oui	Non
Date, horaire et durée de chaque communication	Oui	Oui	Oui
Services complémentaires demandés ou utilisés	Oui	Oui	Oui
Identification des destinataires	Oui	Non	Oui
Origine et localisation (activités de téléphonie)	Oui	Non	Non

Enfin, la conservation et le traitement des données doivent s'effectuer **dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés (art. L. 34-1, avant-dernier alinéa, du code des postes et des communications électroniques).

b) La compensation des surcoûts spécifiques pour les opérateurs

S'agissant des interceptions de sécurité qui portent sur le contenu même des communications, l'article L. 35-6 du code des postes et communications électroniques dispose que « *les prescriptions exigées par la défense et la sécurité publique et les garanties d'une juste rémunération des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs, sont déterminées par décret* ».

---

[1] Les données conservées ne peuvent porter sur le contenu des correspondances échangées ou des informations consultées. En effet, l'interception du contenu des communications, pour les échanges téléphoniques comme pour les courriers électroniques, reste encadrée par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

[2] Les opérateurs pourraient néanmoins, pour la sécurité des réseaux, conserver les données permettant d'identifier l'origine de la communication.

Le Conseil constitutionnel a précisé la nécessité pour l'Etat d'assurer une telle rémunération lorsque l'appui offert par les opérateurs ne correspond pas directement à leur activité de fournisseur de service, afin d'éviter toute rupture caractérisée de l'**égalité devant les charges publiques**[1].

Il a en effet jugé, dans sa décision du 28 décembre 2000[2], que si le législateur pouvait, dans le respect des libertés constitutionnellement garanties, imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, « *le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est* ***étranger à l'exploitation des réseaux de télécommunications*** » et que les dépenses en résultant ne sauraient dès lors incomber directement aux opérateurs.

Une telle indemnisation par l'Etat est également requise pour les surcoûts engendrés par le traitement des données de connexion, que les opérateurs peuvent également conserver pendant un an pour les besoins de la facturation et du paiement des prestations de communications, (art. L. 34-1, III, du code des postes et des communications électroniques).

Aussi l'article L. 34-1, II, du code précité renvoie-t-il à un décret en Conseil d'Etat la définition des modalités de compensation, le cas échéant, des « ***surcoûts identifiables et spécifiques*** » **des prestations assurées par les opérateurs à la demande de l'Etat** pour mettre certaines informations à la disposition de l'autorité judiciaire.

En réponse au questionnaire adressé par le Conseil de l'Union à chaque Etat membre sur la rétention des données de trafic, la France a indiqué avoir préféré, pour la compensation des surcoûts, la voie réglementaire à la voie conventionnelle en raison du nombre d'opérateurs concernés, afin de limiter le risque d'un traitement inégalitaire.

Le décret, en cours d'élaboration, devrait ainsi prévoir la compensation des surcoûts identifiables et spécifiques supportés par les opérateurs pour chacune des réquisitions portant sur une ou plusieurs des catégories de données conservées[3]. Cette compensation serait ajoutée à la liste des **frais de justice** criminelle, correctionnelle et de police établie à l'article R. 92 du code de procédure pénale.

---

[1] *Principe énoncé à l'article 13 de la Déclaration des droits de l'Homme de 1789 : «* pour l'entretien de la force publique et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés *».*

[2] *Décision n° 2000-441 DC du 28 décembre 2000, loi de finances rectificative pour 2000.*

[3] *Deux tarifs seraient institués, selon que les réquisitions portent sur des informations d'origine contractuelle ou des données relatives aux communications. L'énumération des données relevant de chacune de ces catégories devrait faire l'objet d'un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux.*

A titre indicatif, l'association des fournisseurs d'accès et de services Internet, répondant à un questionnaire adressé par les directions générales « société de l'information » et « justice, liberté et sécurité » de la Commission européenne[1], a estimé que ses membres avaient procédé au traitement d'environ 10.000 demandes d'identification d'utilisateurs de l'Internet de la part des services judiciaires au cours des douze derniers mois.

2. Des régimes nationaux très disparates

De nombreux Etats membres ont voté ou sont en voie de voter des lois sur la rétention de données relatives au trafic des communications afin de permettre la prévention, le recherche, la détection ou la poursuite de délits et d'infractions pénales. Mais ces législations, quant elles existent, diffèrent considérablement d'un Etat à l'autre, comme l'illustre le tableau suivant :

Réglementation des Etats membres de l'Union européenne en matière de rétention des données relatives au trafic des communications[2]

Etat membre	Législation relative à la conservation des données de trafic	Obligation de conservation de données de trafic pour les besoins de la recherche des infractions pénales		Durée de conservation	Compensation du coût de la conservation des données pour les opérateurs
		Données téléphoniques	Données électroniques		
Allemagne	Non[3]	Non	Non	-	Compensation des frais de personnel si les services répressifs utilisent des données conservées pour des besoins de facturation
Autriche	Loi de 2003 sur les télécommunications	Non	Non	-	Non
Belgique	Art. 109 ter E de la loi Belgacom (21 mars 1991)	Oui	Oui	Un an minimum	Remboursement du coût des réquisitions judiciaires
Chypre	Loi 112/2004 pour la régulation des communications électroniques	Non	Non	-	Non
France	Art. L. 34-1 du code des postes et des communications électroniques	Oui	Oui	Un an maximum	Oui, décret et arrêté à paraître

[1] *Réponse en date du 15 septembre 2004.*

[2] *Source: réponses au questionnaire du Conseil n° 12076/04 du 17 septembre 2004.*

[3] *La législation allemande permet seulement aux opérateurs de conserver les données relatives au trafic pendant les six mois suivant la facturation et pour les besoins de celle-ci. Les autorités judiciaires ne peuvent donc obtenir de telles données, en application des sections 100g et 100h du code de procédure criminelle, que dans la mesure où elles ont été conservées par l'opérateur pour des raisons commerciales.*

Etat membre	Législation relative à la conservation des données de trafic	Obligation de conservation de données de trafic pour les besoins de la recherche des infractions pénales		Durée de conservation	Compensation du coût de la conservation des données pour les opérateurs
		Données téléphoniques	Données électroniques		
Grèce	Loi 2774/99, seulement pour les besoins de la facturation	Non	Non	-	Non
Hongrie	Loi de 2003 sur les communications électroniques	Oui	Oui	Trois ans	Non
Irlande	Directives temporaires du ministère chargé des télécommunications[1]	Oui	Oui	Trois ans minimum	Non
Italie	Décret législatif n° 196, 2003	Oui	Non (envisagé)	Deux ans, renouvelables une fois	Remboursement du coût engendré par les requêtes
Finlande	-	Non	Non	-	Non
Lettonie	Art. 19 de la loi sur les communications électroniques du 1er mai 2004	Oui	Oui	Trois ans	Non
Lituanie	Art. 64 de la loi sur les communications électroniques du 1er mai 2004	Oui	Oui	Un an maximum	Oui
Malte	Notice légale n° 16 de 2003 sur le traitement des données personnelles	Non	Non	-	Non
Pays-Bas	Art. 13-1 à 13-4 de la loi sur les télécommunications	Oui	Non	Trois mois	Remboursement des frais de personnel liés au traitement des requêtes
Pologne	Loi sur les télécommunications du 21 juillet 2000	Oui	Oui	Un an	Non
Portugal	Art. 8 de la loi n° 69/98 du 28 octobre 1998	Non	Non	-	Non
République tchèque	Loi n° 151/2000	Oui	Oui	Deux mois, sauf requête des services répressifs	Non
Royaume-Uni	Anti-Terrorism, Crime and Security Act de 2001	Oui	Oui	Six à douze mois selon les données	Contribution aux frais de stockage et de recherche des données
Slovaquie	Loi sur les communi-cations électroniques n° 610-2003	Non	Non	-	Non

[1] *Directives prises, dans l'attente d'une législation, sur le fondement de la section 110 du Postal and Telecommunications Services Act de 1983.*

Ces disparités constituent un obstacle à la coopération entre les autorités compétentes, rendant indispensable une harmonisation de la durée de rétention *a priori* des données relatives au trafic des communications et des catégories de données à retenir.

C. LE PROJET DE DÉCISION-CADRE : POUR UNE HARMONISATION DES DISPOSITIFS

Lors de sa réunion du 25 mars 2004, le Conseil européen a décidé d'accorder une priorité notamment à la proposition concernant la conservation des données relatives au trafic des communications, en vue de son adoption d'ici juin 2005[1].

1. Le champ des données concernées

Le projet de décision-cadre porte sur les données relatives au **trafic**[2], les données de **localisation**[3], celles relatives à **l'utilisateur** et celles relatives à **l'abonné** (art. 2). Il ne s'applique pas au contenu des communications échangées (art. 1er).

Les données visées devraient ainsi permettre d'identifier la source d'une communication et les services pour lesquels un abonnement a été souscrit, de déterminer l'acheminement, la destination, l'heure, la date et la durée d'une communication, d'identifier le dispositif utilisé et de localiser la communication.

Ces données peuvent être générées par des services de téléphonie fixe ou mobile, des services de messages courts (SMS), de médias électroniques (EMS) et de messages multimédias (MMS), par des protocoles Internet ou par des développements technologiques futurs dans le domaine des communications.

La question de la **nature des données conservées** a opposé les Etats membres au début des négociations. En effet, l'Allemagne et plusieurs pays d'Europe centrale et orientale souhaitaient que l'obligation de stockage ne porte que sur les données déjà conservées par les opérateurs à des fins commerciales. En revanche, d'autres Etats comme la France tenaient à une harmonisation portant sur l'ensemble des données nécessaires aux enquêtes.

---

[1] *Déclaration sur la lutte contre le terrorisme, DOC 7906/04.*

[2] *Au sens de l'article 2 de la directive 2002/58/CE : les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation.*

[3] *Au sens de l'article 2 de la directive 2002/58/CE : les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public.*

Lors du Conseil « justice et affaires intérieures » du 2 décembre 2004, une nette majorité des représentants des Etats membres s'est prononcée en faveur d'un champ d'application large, correspondant aux besoins des services judiciaires.

2. L'obligation de rétention et d'accès aux données aux fins de la coopération judiciaire en matière pénale

La version initiale de l'article 4 du projet de décision-cadre prévoyait que les Etats membres prendraient les mesures nécessaires afin de veiller à ce que les données soient retenues **pendant une période d'au moins douze mois** et au maximum de trente-six mois après leur création. **La référence à une durée maximale a été supprimée lors des négociations au Conseil, à la demande de l'Italie et de l'Irlande**[1].

Il serait en outre possible aux Etats de fixer des **périodes de rétention plus longues** en fonction de critères nationaux, s'il s'agit d'une mesure nécessaire, appropriée et proportionnée dans une société démocratique.

Les Etats pourraient **déroger à la durée minimale d'un an** et prévoir des durées de rétention plus courtes pour les données produites par les services de messages courts, de médias électroniques, de messagerie multimédias ou par les protocoles Internet, ces dérogations devant être réexaminées chaque année.

Tout Etat membre devrait donner suite à la demande d'un autre Etat membre d'avoir accès aux données conservées dans les conditions prévues par les instruments de la coopération judiciaire en matière pénale, en subordonnant le cas échéant son consentement au respect des conditions qui seraient imposées dans un cas similaire au niveau national (art. 5).

3. Les garanties de protection et de sécurité des données

L'article 6 du projet de décision-cadre prévoit que les Etats membres respectent les principes de la protection des données, en établissant notamment des voies de recours conformément aux dispositions du chapitre III de la directive 95/46/CE.

L'accès aux données devrait être défini en fonction de **finalités déterminées, explicites et légitimes**, au cas par cas et dans le respect du droit national. Les données devraient être « *adéquates, pertinentes et non excessives au regard des finalités poursuivies* » et ne pas être conservées sous une forme

---

[1] *Ces deux Etats appliquent en effet des délais de rétention plus longs, s'élevant respectivement à trois ans minimum et vingt-quatre mois renouvelables une fois.*

permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

La **confidentialité** et **l'intégrité** des données devraient être garanties, des mesures devant être prises pour effacer ou rectifier les données à caractère personnel qui seraient inexactes.

Aux termes de l'article 7 qui énonce les principes de sécurité des données, les Etats membres devraient assurer que celles-ci :

- sont de la même qualité que les données sur le réseau ;

- font l'objet de mesures destinées à les protéger contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération ou toute forme de traitement illicite ;

- sont détruites à la fin de la période de rétention.

III. LA PROPOSITION DE RÉSOLUTION SOUMISE À VOTRE COMMISSION : PROTÉGER LES DROITS FONDAMENTAUX ET ÉVITER LES DISTORSIONS DE CONCURRENCE

Réunie le 15 décembre 2004, la délégation pour l'Union européenne du Sénat a adopté, à l'initiative de notre collègue M. Alex Türk, une proposition de résolution relative au projet de décision-cadre soumis au Sénat.

Cette proposition de résolution, tend d'abord à **approuver le principe d'une harmonisation européenne en matière de conservation**, par les opérateurs économiques, **des données** stockées et traitées dans le cadre de la fourniture de services de communications électroniques.

Votre commission, sous réserve d'une modification rédactionnelle, est en plein accord sur ce point avec la délégation pour l'Union européenne.

En effet, les infractions commises par des organisations criminelles transnationales requièrent en général des investigations longues et complexes. L'aboutissement de ces enquêtes suppose que les services compétents puissent disposer de données relatives aux communications échangées par les réseaux criminels, parfois plusieurs mois après leur enregistrement[1].

La proposition de résolution considère par ailleurs que le projet de décision-cadre ne permet pas, dans sa version actuelle, « *de répondre à cet*

---

[1] *Ainsi, selon le ministère de la justice, le délai d'instruction en matière criminelle s'élevait à 22,7 mois en France en 2002.*

objectif et de concilier le besoin d'efficacité des enquêtes et la protection des droits individuels » et vise à attirer l'attention du Gouvernement sur la nécessité de **prévoir une durée maximale de conservation des données de trafic**. Elle tend enfin à demander au Gouvernement que soit réalisée une évaluation du surcoût de la conservation des données pour les fournisseurs de services.

A. UN DÉLAI MAXIMAL DE CONSERVATION DES DONNÉES POUR CONCILIER PROTECTION DES DROITS FONDAMENTAUX ET EFFICACITÉ DES ENQUÊTES

Le principal enjeu de la proposition de résolution soumise à votre commission est de concilier la nécessité de lutter contre le terrorisme et le respect des droits fondamentaux.

L'obligation de protection des personnes ne justifie pas la violation du principe du respect des droits de ces personnes. En outre, cette première obligation préventive est subsidiaire et subordonnée à la seconde.

Ce double devoir trouve sa justification dans l'interprétation des droits fondamentaux par la Cour européenne des droits de l'Homme.

En effet, deux interprétations s'opposent. La première, qualifiée de classique et libérale, considère que les droits de l'Homme sont des droits négatifs, l'Etat étant seulement tenu de les faire respecter. La seconde, qui est celle de la Cour européenne des droits de l'Homme, suppose **que les Etats ont des obligations positives** et doivent agir afin de sauvegarder les libertés garanties par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH).

Dans le domaine visé par la proposition de résolution qui est soumise à votre commission, c'est-à-dire celui de la rétention d'informations relatives aux communications électroniques, l'obligation positive des Etats parties à la CEDH est de préserver les droits et libertés visés par l'article 8 de cette convention, **en limitant et encadrant strictement l'ingérence commise dans la vie privée des personnes**.

Cette **juste proportion** est possible en suivant **les critères fixés par la Cour européenne des droits de l'Homme**, dans son interprétation de l'article 8.

1. Le respect des exigences de l'article 8 de la CEDH

Les données de trafic peuvent comporter des détails quant à l'heure et au lieu des communications, ainsi qu'aux numéros utilisés. Elles entrent par

conséquent dans la sphère privée des citoyens et dans le champ d'application de l'article 8, paragraphe 1 de la CEDH[1]. D'ailleurs, suivant une jurisprudence constante, la Cour de Strasbourg estime que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une **ingérence** au sens de cet article[2].

Dans sa recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications, adoptée le 3 mai 1999, **le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel**[3] définit l'interception comme « *la prise de connaissance par un tiers du contenu et/ou des données afférentes aux communications privées entre deux ou plusieurs correspondants, en particulier les données de trafic liées à l'utilisation des services de télécommunications* ».

Le groupe de l'article 29 reprend cette analyse dans son avis 9/2004 adopté le 9 novembre 2004 sur le projet de décision-cadre, estimant que « *les mêmes critères fondamentaux s'appliquent à la conservation des données de trafic au-delà de ce qui est nécessaire pour la fourniture des services de communications et d'autres objectifs commerciaux légitimes, et pour tout accès à des données pour le respect du droit* ».

Une telle conservation constitue en effet, selon ses membres, une violation du droit à la vie privée des individus et du secret de la correspondance.

Aussi le groupe de l'article 29 considère-t-il que la conservation des données de trafic est inacceptable, à moins qu'elle ne réponde à **trois critères fondamentaux** énoncés à l'article 8, paragraphe 2, de la CEDH et à l'interprétation qu'en donne la Cour. Ces trois critères sont :

- la base légale de la mesure ;

- la conformité de la mesure à l'un des buts légitimes énumérés dans la Convention ;

- la nécessité de cette mesure dans une société démocratique.

---

[1] *Cf supra, II, A.*

[2] *Arrêts Leander contre Suède du 26 mars 1987, § 48 et Kopp contre Suisse du 25 mars 1998, § 53.*

[3] *Ce groupe de travail, dit « **groupe de l'article 29** », a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un **organe consultatif européen indépendant** sur la protection des données et de la vie privée. Il est composé d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque Etat membre (pour la France, il s'agit de la CNIL), d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.*

2. Le critère de la base légale

L'ingérence doit être prévue par la loi, conformément au paragraphe 2 de l'article 8 de la CEDH: « *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit [à la vie privée] que pour autant que cette ingérence est prévue par la loi* ».

Le terme de loi est à prendre ici au sens le plus large, c'est-à-dire l'ensemble du droit interne de l'Etat membre concerné.

Mais cette exigence vise également **la qualité de la loi** (accessibilité de la loi à la personne concernée, prévisibilité des conséquences de la loi). Ainsi, dans l'arrêt *Malone* du 2 août 1984 (§ 67), la Cour de Strasbourg a jugé que la loi devait « *user de termes assez clairs pour indiquer à tous de manière suffisante* ***en quelles circonstances et sous quelles conditions*** *elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance* ».

En l'espèce, votre commission estime que le champ des données visées et la définition d'une durée de conservation minimale commune constituent une base légale suffisante.

3. La légitimité du but de l'ingérence

L'article 8, paragraphe 2, de la CEDH énonce les buts légitimes susceptibles de fonder l'ingérence d'une autorité publique dans la vie privée.

L'ingérence que vise à permettre et encadrer le projet de décision-cadre recouvre ainsi trois objectifs légitimes : **la sécurité nationale, la sûreté publique et la prévention des infractions pénales**. La lutte contre le terrorisme s'inscrit dans ces objectifs.

Il existe en effet **un impératif de défense** évident depuis les attentats terroristes qui ont frappé les Etats-Unis et l'Espagne. Les menaces terroristes persistantes font apparaître un indispensable besoin d'harmonisation pour assurer une coopération judiciaire efficace.

4. La nécessité de la mesure

Le paragraphe 2 de l'article 8 de la CEDH stipule que l'ingérence n'est acceptable que si 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 ».

La Cour de Strasbourg a notamment donné une interprétation de ce critère dans l'arrêt *Klass* du 6 septembre 1978 (§ 59), en jugeant nécessaire de concilier « *les impératifs de la défense de la société démocratique et ceux de la sauvegarde des droits individuels* »[1]. Par conséquent, les autorités doivent mettre en place des moyens suffisants afin de contrôler **les éventuels dysfonctionnements du système** qui porteraient une atteinte trop importante et non proportionnée au principe du respect de la vie privée des personnes.

Le projet de décision-cadre définit des règles de protection et de sécurité des données propres à éviter de tels dysfonctionnements.

Toutefois**,** comme l'a rappelé la Cour européenne des droits de l'Homme dans l'arrêt *Klass* (§ 49), **les Etats ne disposent pas « *d'une latitude illimitée* *pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction* ».

Le groupe de l'article 29 a considéré que la conservation des données de trafic ferait de la « *surveillance autorisée dans des circonstances exceptionnelles la règle générale* », et qu'imposer aux opérateurs de conserver des données « *dont ils n'ont pas besoin à des fins propres constituerait* ***une dérogation sans précédent au principe de finalité*** ».

En l'espèce, la durée de conservation des données relatives au trafic des communications est un **paramètre essentiel** de la protection des droits fondamentaux. Par conséquent, s'il est démontré que la conservation de ces données pendant un an constitue une nécessité pour l'efficacité des enquêtes relatives à la criminalité transnationale, il ne paraît pas acceptable de laisser les Etats membres fixer des périodes de rétention plus longues, sans aucune limitation.

Ainsi, l'ingérence qui serait commise par le stockage des données de trafic ne serait justement proportionnée que si la décision-cadre fixait une durée maximale de conservation.

Votre commission partage donc entièrement le souhait de la délégation pour l'Union européenne de **rétablir une durée maximale de conservation des données** et de **demander au Gouvernement d'œuvrer en ce sens au sein du Conseil.**

Les Etats membres pourraient en outre, comme le prévoit le projet dans sa version actuelle, fixer des périodes de rétention plus longues en fonction de critères nationaux « *pour autant qu'une rétention plus longue*

---

[1] *Cf également l'arreî du 23 juillet 1968, Affaire "linguistique belge", § 5.*

constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique ».

B. L'ÉVALUATION DU SURCOÛT DE LA CONSERVATION DES DONNÉES POUR LES FOURNISSEURS DE SERVICES

Comme le relève notre collègue M. Alex Türk dans l'exposé des motifs de sa proposition de résolution, les opérateurs devront supporter un coût supplémentaire s'il leur est demandé de stocker des données pendant une durée supérieure à la durée de conservation des données de facturation ou s'il s'agit de données qu'ils ne conservaient pas auparavant.

Mais plus encore, c'est **le traitement de ces données** par un personnel qualifié qui devrait se révéler coûteux pour les fournisseurs de services de communications[1].

Les Etats membres imposant d'ores et déjà aux fournisseurs de services de communications de conserver les données de trafic afin de permettre aux juridictions de prévenir et rechercher les infractions pénales ont d'ailleurs, pour la plupart, choisi de leur rembourser les frais engendrés par chaque réquisition.

Cependant, tous les Etats membres dotés de dispositifs législatifs imposant de telles obligations aux opérateurs n'ont pas prévu un régime d'indemnisation[2]. L'absence d'harmonisation de la prise en charge par les Etats des coûts suscités par les réquisitions pourrait engendrer des **distorsions de concurrence** entre les opérateurs au sein de l'Union européenne[3].

Le projet de décision-cadre ne comporte aucune disposition relative à la participation de l'Etat aux coûts supportés par les opérateurs. En effet, les quatre Etats membres à l'initiative de ce projet ne pouvaient se fonder sur le titre VI du traité sur l'Union européenne, qui énonce les dispositions relatives à la coopération policière et judiciaire en matière pénale (troisième pilier), pour prévoir un régime d'indemnisation qui relève en fait de la réglementation du marché intérieur.

La proposition de résolution soumise à votre commission tend par conséquent à inviter le Gouvernement à « *demander à la Commission européenne*

---

[1] *Dans sa réponse du 15 septembre 2004 au questionnaire de la Commission européenne, l'association européenne des fournisseurs de services Internet (European Internet Services Providers Association (EuroISPA) souligne également que la recherche de données de trafic des communications est particulièrement complexe et coûteuse.*

[2] *Cf tableau supra.*

[3] *Aux termes de l'article 87, paragraphe 1, TCE, «* sauf dérogations prévues par le présent traité, sont incompatibles avec le marché commun, dans la mesure où elles affectent les échanges entre Etats membres, les aides accordées par les Etats ou au moyen de ressources d'Etat sous quelque forme que ce soit qui faussent ou qui menacent de fausser la concurrence en favorisant certaines entreprises ou certaines productions. *»*

de ***procéder à une évaluation du surcoût*** *de la conservation des données de trafic pour les fournisseurs de services et à une* ***étude sur les différentes possibilités concernant le régime d'indemnisation des opérateurs*** ».

Votre commission approuve cette solution, qui permettra la réalisation d'un diagnostic complet avant l'adoption, le cas échéant, d'un instrument assurant l'harmonisation des règles d'indemnisation des fournisseurs de services de communications.

*

* *

Au bénéfice de l'ensemble de ces observations, votre commission a adopté une proposition de résolution dont le texte est reproduit ci-après.

PROPOSITION DE RÉSOLUTION

(texte adopté par la commission des Lois en application
de l'article 73 *bis* du règlement du Sénat)

Le Sénat,

Vu l'article 88-4 de la Constitution,

Vu le projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme (texte E 2616) ;

Approuve le principe d'une harmonisation européenne en matière de conservation, par les opérateurs économiques, des données stockées et traitées dans le cadre de la fourniture de services de communications électroniques, mais considère que le projet ne permet pas, dans sa version actuelle, de répondre à cet objectif et de concilier le besoin d'efficacité des enquêtes et la protection des droits individuels ;

Juge indispensable que le texte prévoie une durée maximale de conservation des données et demande, par conséquent, au Gouvernement d'œuvrer au sein du Conseil en ce sens ;

Invite, en outre, le Gouvernement à demander à la Commission européenne de procéder à une évaluation du surcoût de la conservation des données de trafic pour les fournisseurs de services et à une étude sur les différentes possibilités concernant le régime d'indemnisation de ces opérateurs.

TABLEAU COMPARATIF

Texte de la proposition de résolution	Proposition du rapporteur
Le Sénat,	*(Alinéa sans modification).*
Vu l'article 88-4 de la Constitution,	*(Alinéa sans modification).*
Vu le projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme (texte E 2616) ;	*(Alinéa sans modification).*
Approuve le principe d'une harmonisation européenne en matière de conservation, par les opérateurs économiques, des données stockées et traitées dans le cadre de la fourniture de services de *télécommunication*, mais considère que le projet ne permet pas, dans sa version actuelle, de répondre à cet objectif et de concilier le besoin d'efficacité des enquêtes et la protection des droits individuels ;	Approuve… …services de *communications électroniques*, mais… …individuels ;
Juge indispensable que le texte prévoie une durée maximale de conservation des données et demande, par conséquent, au gouvernement d'œuvrer au sein du Conseil en ce sens ;	*(Alinéa sans modification).*
Invite, en outre, le Gouvernement à demander à la Commission européenne de procéder à une évaluation du surcoût de la conservation des données de trafic pour les fournisseurs de services et à une étude sur les différentes possibilités concernant le régime d'indemnisation de ces opérateurs.	*(Alinéa sans modification).*