AVIS N° 33 / 1999 du 13 décembre 1999

N. Réf. : 10 / A / 1999 / 036

OBJET : Projets de loi relatifs à la criminalité informatique.

La Commission de la protection de la vie privée,

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998 transposant la directive du 24 octobre 1995 du Parlement européen et du Conseil 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, en particulier l'article 29;

Vu le rapport de MM. DE SCHUTTER et POULLET;

Emet d'initiative, le 13 décembre 1999, l'avis suivant:

1. Antécédents

Le 30 novembre 1999, le Président de la Commission de la protection de la vie privée a été invité à s'exprimer devant la Commission de la Justice du Parlement à propos de deux projets de loi relatifs à la criminalité informatique déposés conjointement par le ministre de la Justice, le ministre des Télécommunications et des Entreprises et Participations publiques et le ministre de l'Economie (Doc. Parl., Ch., sess. ord. 1999-2000, n° 213/1 et n° 214/1)[1]. Le présent avis fait suite à cette audition.

2. Présentation des projets de loi

Les projets de loi relatifs à la criminalité informatique visent à ériger en infraction le fait de porter atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques ou des données qui sont stockées, traitées ou transmises par le biais de ces systèmes[2].

A cet effet, il est prévu d'ajouter un nouveau titre au Code pénal incriminant certains délits comme le faux en informatique, l'accès non-autorisé à un système ou encore le sabotage de données informatisées.

Par ailleurs, les projets de loi prévoient de nouvelles techniques de dépistage comme la confiscation de données, l'obligation de coopération, la recherche de réseau et l'interception de communications.

3. Observations de la Commission

A. Observations générales

1. La Commission souligne que les deux projets de loi qui font l'objet du présent avis complètent une série d'autres dispositions déjà prises et pour lesquelles son avis avait été sollicité.

On citera en particulier :

- les articles 202 et 203 de la loi du 21 décembre 1994, relatifs entre autres à la collaboration technique des opérateurs à l'exécution de mesures judiciaires d'écoute (avis n° 17/97 du 9 juillet 1997) ;

- le projet de loi concernant l'identification et le repérage des numéros de postes de communication ou de télécommunication et portant modification des articles 90ter, 90quater, 90sexties et 90septies du Code d'instruction criminelle (avis n° 09/97 du 20 mars 1997) ;

- les amendements de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées (avis n° 34/97 du 27 novembre 1997) ;

[1] Ci-après, n° 213/1 et n° 214/1.
[2] Voir à ce sujet les travaux du Conseil de l'Europe (notamment *La criminalité informatique*, Préface d'August Bequai, Strasbourg, 1990) et des Nations Unies.

- l'arrêté royal portant exécution des dispositions de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance, l'enregistrement de communications et télécommunications privées et l'article 109ter, E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (avis n° 12/99 du 24 mars 1999).

  Dans ce contexte**,** la Commission s'étonne de ne pas avoir été saisie des projets de loi n° 213/1 et n° 214/1 à un stade antérieur à la discussion au Parlement. Les précédents avis émis par la Commission soulignaient en effet l'importance des enjeux en termes de protection de la vie privée de certaines dispositions en projet[3].

  La Commission souhaite attirer l'attention du législateur sur le fait que tant certaines dispositions du projet de loi n° 213/1 que la quasi-totalité de celles du projet n° 214/1 peuvent avoir des implications en matière de protection de la vie privée. En effet, nombre de dispositions en projet (recherche et saisie de données, repérage et interception des télécommunications...) peuvent impliquer des données à caractère personnel. Les dispositions pertinentes en matière de protection de la vie privée s'appliquent à toutes ces données.

  2. Soulignons d'emblée l'importance du principe de proportionnalité.

  Tant les textes internationaux relatifs à la protection des données à caractère personnel que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après, la loi du 8 décembre 1992[4]) mettent l'accent sur le respect strict de ce principe.

  A cet égard, et dans un contexte similaire, la Commission avait déjà rappelé que "les mesures à prévoir ne peuvent avoir pour effet de légitimer les pratiques de repérage ou d'interception préventives (…) elles ne peuvent conduire les autorités publiques à disposer d'informations disproportionnées par rapport à celles nécessaires dans le cadre de l'instruction, et (…) doivent respecter le caractère strictement d'exception de l'écoute" (avis n° 09/97, n° 12/99). Cette remarque vaut en particulier pour les articles 39bis, 88ter, 88quater et 109ter en projet du Code d'instruction criminelle (projet de loi n° 214/1, développement *infra*).

  La Commission rappelle que l'accès à des systèmes d'information (article 88ter en projet), à des informations permettant de lever les procédés garantissant la confidentialité des données (cryptographie) (article 88quater en projet) ou aux bases de données d'utilisation des services (article 109ter, E projet de modification) ne devrait pas permettre de rassembler quantité d'informations au-delà de ce qui est strictement nécessaire pour une instruction ; ces dispositions n'autorisent pas des méthodes de surveillance globale indépendamment d'une instruction relative à des infractions précises. Ainsi, en consultant la base de données des accès d'une personne à son fournisseur d'accès, il est possible de retracer l'ensemble des sites visités par cette personne, alors que seule la question de sa connexion à un site particulier serait visée. De la même manière, en disposant de la clé de cryptage utilisée par une personne, il est possible d'accéder à tous les messages émis par cette personne ou encore, en disposant du code d'accès d'un médecin, on peut avoir accès à toutes données figurant sur une "carte à puce" de santé.

[3] Dans le cadre des avis cités sur les textes visant l'interception des télécommunications et des écoutes, la Commission a systématiquement émis le désir d'être consultée.

[4] Cette loi a été modifiée par la loi du 11 décembre 1998 transposant la directive du 24 octobre 1995 du Parlement européen et du Conseil 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. Cette loi n'est pas encore entrée en vigueur à cette date mais la Commission préconise d'anticiper autant que possible certains changements apportés par cette loi, vu le principe de l'effet direct de la directive européenne dont le délai de transposition est dépassé. En particulier dans ce cas-ci, c'est essentiellement la terminologie qui se voit modifiée.

3. De plus, il doit être clair que c'est l'ensemble des dispositions de la loi du 8 décembre 1992 qui s'applique à toutes les données à caractère personnel concernées par les dispositions en projet : non seulement le prescrit de l'article 4 (finalité, proportionnalité, pertinence, durée limitée de conservation), mais également celui de l'article 16 (sécurité). La Commission est d'avis que l'applicabilité de cette loi devrait être clairement énoncée dans le texte en projet[5]. A tout le moins, une telle mention devrait être reprise dans l'exposé des motifs. Elle note toutefois que le projet lui-même reconnaît indirectement l'aspect « protection des données à caractère personnel » en prévoyant des mesures limitant l'accès (article 39bis, § 2), ou encore de garanties en termes d'intégrité et de confidentialité (article 39bis, § 6).

4. Eu égard à l'applicabilité de la loi du 8 décembre 1992, se pose encore la question de l'utilisation des concepts utilisés dans le texte en projet par rapport à ceux de la loi du 8 décembre 1992 (cf. *infra*) ou de savoir comment articuler les délits prévus par les textes en projet et à ceux prévus et sanctionnés par la loi du 8 décembre 1992[6]. La Commission se demande si le législateur envisage le cumul des qualifications et peut-être des peines ou s'il envisage d'accorder la priorité à une législation par rapport l'autre, et dans ce cas, à laquelle.

5. Par ailleurs, la Commission souhaite attirer l'attention du législateur sur le fait que les textes en projet ne règlent pas la question de savoir dans quelle mesure certains responsables de systèmes informatiques pourront invoquer la règle du secret professionnel (avocats, médecins,...). Les précautions particulières qu'implique la sauvegarde du secret professionnel face à une perquisition nécessitant l'accès à un système informatique devraient également être réglées.

A ce propos, la Commission rappelle le prescrit de l'article 90octies du Code d'instruction criminelle libellé comme suit « la mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence ou les moyens de communication ou de télécommunication d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90ter, utilisent ses locaux, sa résidence ou ses moyens de communications ou de télécommunication. La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. (…) ».

La Commission estime d'une part que des mécanismes d'intervention de ce type incluant les instances professionnelles[7] devraient être légalement prévus dans tous les cas d'espèce visés par les projets de loi qui font l'objet du présent avis (cf. *infra*) et d'autre part que des mesures de précautions devraient être prévues pour d'autres catégories professionnelles que les seuls médecins et avocats[8].

---

[5] Cf. *infra,* article 2.

[6] Ainsi, le faux informatique de l'article 210bis du Code pénal en projet pourrait correspondre, s'il porte sur des données à caractère personnel, avec le traitement de données à caractère personnel inexactes (article 39, 1° de la loi du 8 décembre 1992), ou encore la communication de renseignements inexacts lorsque l'intéressé exerce sont droit d'accès (article 39, 5°).
La fraude informatique (article 504quater en projet) ou le hacking (article 550bis en projet) pourrait correspondre à une intrusion dans un fichier, à un traitement illicite, voire à un détournement de finalité.

[7] Ainsi, on pourrait imaginer qu'un membre du Conseil de l'Ordre des médecins ou des avocats soit présent lors de l'intervention des autorités judiciaires.

[8] Voir toutefois à ce propos la jurisprudence de la Cour d'arbitrage qui a déclaré conforme au principe d'égalité la non extension de la protection à d'autres professions également soumises au secret professionnel (arrêt n° 26/96 du 27 mars 1996)

6. En bref, les risques de dérapage et la possibilité de mettre en place un système de surveillance policière générale sur la base des dispositions en projet nécessitent de rappeler strictement les principes de légalité (cf. *infra*) et de proportionnalité. Il paraît également souhaitable que cette pratique judiciaire spécifique fasse l'objet d'une évaluation et que celle-ci soit reprise dans un rapport à élaborer dans les trois ans, rapport qui devrait être communiqué à la Commission afin de mettre celle-ci en état de réagir en fonction des principes légaux dont elle est instituée la gardienne. L'instance ou le service chargé de cette évaluation devrait tenir compte de critères spécifiques qu'il appartiendrait à la Commission de formuler au préalable.

B. Observations par article

En ce qui concerne le projet n° 213/1, la Commission se contente de souligner l'importance de ce projet de loi qui contribue à la protection des données à caractère personnel et en particulier à leur sécurité.

Les observations de la Commission effectuées sous cette partie B se concentrent sur le projet n° 214/1.

Article 2

L'article 2 du projet insère un nouvel article 39bis dans le Code d'instruction criminelle.

Du point de vue de la protection des données à caractère personnel, la Commission est d'avis que le problème créé par la saisie ou la copie de données stockées dans un système informatique sur certains supports est le suivant. En pratique, il sera souvent difficile lors d'une saisie ou d'une copie de se limiter aux seules données relatives aux personnes, objet des poursuites, comme l'exige l'application stricte du principe de proportionnalité.

La Commission estime dès lors indispensable que :

1) la mesure ordonnant la saisie ou la copie indique précisément les infractions dont la poursuite requiert la saisie ou la copie ainsi que, dans toute la mesure du possible, les personnes soupçonnées ;

2) dans toute la mesure du possible, la copie ou la saisie devraient être limitées à ces seules données ;

3) si cela n'est pas possible, l'effacement des autres données devrait être opéré dans la banque de données judiciaires ou des garanties de non utilisation de celles-ci par les autorités judiciaires devraient être prévus.

   La Commission suggère en outre d'inclure dans cet article une référence explicite à l'applicabilité de la loi du 8 décembre 1992.

Article 3

L'article 3 insère un article 88ter dans le Code d'instruction criminelle.

La Commission est d'avis que l'extension de la perquisition à d'autres systèmes informatiques ne devrait pouvoir être effectuée que si les trois conditions énoncées dans la disposition proposée sont présentes de façon cumulative. Une motivation de la présence de ces trois conditions devrait être établie et pouvoir être examinée dans les cas où la mesure d'extension serait contestée.

La Commission relève que le 2ème alinéa de cet article manque de précision dans la mesure où via des réseaux ouverts comme Internet, les personnes visées par cet alinéa ont accès à une multitude de sites. Il serait par conséquent utile de préciser que seule est visée l'extension à des systèmes auxquels les personnes autorisées ont *"spécifiquement"* accès en vertu d'une autorisation particulière.

La notion de *"responsable du système informatique"* utilisée au 3ème alinéa n'est définie nulle part. Pareille imprécision risque de créer des inexactitudes et des malentendus. S'agit-il du responsable technique, civil ou du responsable vis-à-vis d'une législation particulière comme celle relative à la protection des données à caractère personnel ? Ainsi, l'article 1er, §4 de la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 définit le responsable du traitement comme “la personne physique ou morale, l’association de fait ou l’administration publique qui, seule ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données à caractère personnel”. La Commission estime que le projet de loi devrait fournir certaines indications à propos de la notion de « responsable du système informatique ».

La Commission note enfin que l'extension de la recherche permettra de collecter des données *"utiles"* pour les mêmes finalités que celles prévues pour la saisie. Cette possibilité étendue de collecter des données ne paraît pas conforme au principe de proportionnalité. La loi du 8 décembre 1992 prévoit des critères de pertinence, d'adéquation et de non-excessivité qui paraissent plus exigeants en termes de protection des données à caractère personnel.

Article 4

L'article 4 insère un article 88quater dans le Code d'instruction criminelle.

La Commission note que cet article prévoit une délégation par le juge d'instruction à un officier de police judiciaire. Elle suggère d'ajouter qu'elle doit être faite par écrit.

En vertu du 2ème alinéa, l'obligation de collaboration s'étend "à toute personne pertinente", sauf l'inculpé et ses proches. La Commission se demande quelles seront les conséquences si l'inculpé est une personne morale. Un organe ou un préposé est-il protégé par la règle de l'auto-incrimination ? Les exemples donnés dans l'exposé des motifs[9] sont souvent externes à la société et la situation des personnes précitées reste peu claire.

Enfin, la Commission estime également que, tant pour le premier que pour le second alinéa, il serait important de veiller au respect du secret professionnel (cf. *supra*).

Article 7

L'article 7 complète l'article 90quater du Code d'instruction criminelle en ajoutant un 4ème alinéa.

Cette disposition règle la collaboration des personnes liées à un service de télécommunication, qui doivent fournir des informations afin d'informer sur le fonctionnement du système ou sur la manière d'accéder au contenu de la télécommunication, sous une forme compréhensible. Le texte ajoute heureusement *"dans la mesure où c'est dans leurs possibilités"*. On retrouve ici le problème d'une obligation de décryptage qui sera difficile à respecter lorsque l'initiative du cryptage n'émane pas de l'opérateur, mais de l'utilisateur (cf. avis n°12/99, p. 6).

[9] Doc.Parl., Ch. Repr., sess.ord. 1999-2000, n° 213/1 et n° 214/1, p. 27.

En outre, telle qu'elle est rédigée[10], la disposition permet au juge d'instruction d'obtenir les informations nécessaires au décodage ou au décryptage, non seulement des communications suspectes, mais de toutes les télécommunications de l'ensemble des utilisateurs du service de protection ou de cryptage des dossiers.

Dès lors, la Commission estime qu'il faut veiller à ce que le principe de proportionnalité soit respecté et que le décodage ou décryptage soit fait par la personne qui a connaissance du procédé de cryptage ou de codage sans qu'il y ait nécessairement transmission des informations relatives au décodage ou au décryptage.

De plus, la Commission estime qu'il serait utile que seules certaines personnes au sein des organismes permettant de protéger ou de crypter des données, puissent être contactées par le juge d'instruction, et ce de manière à ne pas multiplier les risques de divulgation des mesures prises et des résultats de l'enquête. Ces personnes désignées par les organismes seraient soumises au secret professionnel (cf. la cellule "coordination Justice" proposée par le projet d'arrêté royal en application de l'article 109ter, E de la loi du 21 mars 1991).

Par ailleurs, cette disposition soulève également la question du secret professionnel que certaines personnes pourraient opposer au juge d'instruction (cf. *supra*).

Article 8

L'article 8 étend les modalités de conservation des données au niveau du Parquet.

Des données à caractère personnel n'étant pas exclues de cette conservation, la Commission estime qu'il serait préférable de préciser que les moyens "doivent" être utilisés pour l'intégrité et la confidentialité, au lieu de "peuvent".

La Commission est d'avis qu'il s'agit d'un nouveau traitement de données à caractère personnel soumis à la loi du 8 décembre 1992. Dès lors, étant donné la nature de certaines données à conserver, l'arrêté royal déterminant les moyens devrait être soumis à l'avis de la Commission.

Article 9

L'article 9 modifie l'article 109ter, E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

La disposition légale proposée complète une disposition récemment modifiée par la loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. Cette disposition veut que le Roi détermine, après avis de la Commission de la protection de la vie privée, par arrêté délibéré en Conseil des Ministres *"les moyens techniques par lesquels les opérateurs de réseaux et les fournisseurs de services de télécommunications doivent permettre le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement de télécommunications privées"*.

[10] " Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.
Si nécessaire, il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure où c'est dans leurs possibilités. […]"

La Commission rappelle qu'un projet d'arrêté royal relatif à la transposition de cette disposition, qui lui avait été soumis en son temps, avait fait l'objet de critiques sévères de sa part (dans son avis n° 12/99 du 24 mars 1999).

En outre, l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales garantit le caractère confidentiel des télécommunications en ce compris les données relatives à l'utilisation des services de télécommunication[11]. L'article 5 de la directive 97/66/CE[12] s'inscrit dans la même logique. Le principe est donc l'interdiction de prise de connaissance, sauf exceptions, qui doivent être strictement délimitées.

Le Groupe établi par l'article 29 de la directive 95/46/CE[13] (ci-après, le Groupe 29) a rappelé les principes applicables en l'espèce dans le cadre des recommandations n° 2/99 et n° 3/99 (cf. *supra*).

Sur la base des critiques et principes énoncés par ces différents textes, la Commission estime que les mesures instituées par l'article 109ter en projet entraîneront la création obligatoire de banques de données à caractère personnel et ont des conséquences importantes en matière de vie privée. Cet article a fait l'objet de remarques du Conseil d'Etat.

1. Base légale

L'article 22 de la Constitution énonce que "chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit". En d'autres termes, seule la loi peut apporter des restrictions au droit à la vie privée et familiale. Les différentes mesures contribuant à faciliter la tâche des autorités compétentes doivent dès lors trouver leur fondement direct dans la loi (dans le même sens, avis du Conseil d'Etat, Doc. Parl., Ch., sess. ord.1999-2000, n° 213/1 et n° 214/1, p. 55).

Cette obligation ressort également de divers textes internationaux. L'application des articles 8 de la Convention européenne précitée, ainsi que de l'article 9, §2 de la Convention n° 108 du Conseil de l'Europe, de l'article 13 de la directive 95/46/CE et de l'article 14 de la directive 97/66/CE, a pour conséquence que les Etats doivent établir des conditions précises pour permettre des mesures d'ingérence par les services de police, de justice et de sûreté. Trois critères prévalent : la base légale, la nécessité dans une société démocratique et la finalité légitime.

A la critique émise par le Conseil d'Etat tenant au fait que les atteintes à la vie privée résultant des obligations d'enregistrement et de conservation des données doivent trouver leur origine dans un texte de loi, le rédacteur du texte répond aux objections du Conseil d'Etat que la technicité de la question s'oppose à ce type de solution.

Indépendamment du risque de censure d'un tel choix par la Cour d'arbitrage, la Commission souhaite faire remarquer que rien n'empêche de figer la durée et les garanties en termes de protection de la vie privée dans un texte légal (ce qui n'a rien de technique et a déjà été fait dans la loi sur le Casier judiciaire central, par exemple) et de prévoir les modalités de nature exclusivement "techniques" par arrêté royal[14].

[11] Arrêt Malone du 2 août 1984, publ. Cour, Série A, n° 82, pp. 30 et s.
[12] Directive 97/66/CE du 15 décembre 1997 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (ci-après, la directive 97/66/CE).
[13] Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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 (ci-après, la directive 95/46/CE).
[14] Dans son avis n° 12/99 sur les écoutes téléphoniques, la Commission avait suggéré une loi, ou un arrêté royal délibéré en Conseil des Ministres et préalablement soumis à la Commission.

Si le choix actuel devait être maintenu, il devrait s'agir en tout état de cause d'un arrêté royal délibéré en Conseil des Ministres et l'avis de la Commission devrait à tout le moins être requis pour le § 2 du 109ter (obligation pour les fournisseurs de services d'enregistrer et de conserver des données) et pas uniquement pour le § 4 de cet article (modalités et moyens de garantir la confidentialité et l'intégrité des données).

2. Proportionnalité

i) Critère de nécessité

Les données visées permettent de constituer des bases de données de personnes non soupçonnées *a priori* (voyez, pour analogie, l'avis n° 17/98 de la Commission portant sur un avant-projet de loi relatif à l'analyse ADN en matière pénale et l'avis n° 40/97 concernant un projet proactif relatif aux ravisseurs potentiels d'enfants). Or, la Commission rappelle que ni les textes internationaux mentionnés ci-dessus, ni la loi du 8 décembre 1992 (principes de proportionnalité, durée limitée, …) n'autorisent les méthodes de surveillance globale indépendamment d'instructions relatives à des infractions particulières (si l'on excepte le cas très particulier de la recherche proactive, qui est strictement encadrée).

A cet égard, la Commission souhaite encore se référer à la jurisprudence de la Cour européenne des droits de l'homme[15] qui conduit à proscrire les mesures de surveillance exploratoire ou générale des télécommunications mises en œuvre sur une grande échelle.

Ainsi, il ne pourrait être question d'obliger un fournisseur d'accès à enregistrer systématiquement tous les appels en provenance de ses clients mais uniquement lorsqu'une instruction est ordonnée vis-à-vis d'une personne en particulier. Il ne pourrait non plus être question de contraindre un fournisseur d'accès à tenir un log book des accès susceptibles de conforter l'instruction[16].

Dans ce contexte, la Commission estime également utile de rappeler l'article 2, § 2, 2° de la Recommandation n° R (95) 4 du Conseil de l'Europe en vertu duquel des dispositifs anonymes d'accès au réseau et aux services de télécommunication devraient être mis à la disposition des utilisateurs.

ii) Champ d'application

Le champ d'application est très large : les données visées ont trait à quiconque utilise des services de télécommunication. Il s'agit potentiellement de toute la population, et l'ensemble des services de télécommunication est couvert (catégorie extrêmement large : fournisseurs d'accès, portails, services dits « intermédiaires », certificateurs, serveurs dits « d'anonymisation »…). En effet, dans notre société qui évolue de plus en plus vers une «société de l'information», l'utilisation des services de télécommunications est de plus en plus répandue.

De plus, les catégories de données ne sont pas circonscrites de manière précise (cf. l'exposé des motifs, qui ne contribue pas à la clarté en mentionnant *a priori* certaines données sans exclure les autres de manière définitive[17]).

[15] Arrêts Klass (arrêt du 6 septembre 1978, Publ. Cour, Série A, n° 28, p. 23 et s) et Malone (cité). Voir sur ce point la recommandation du groupe institué à l'article 29 de la directive 95/46/CE n° 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications.

[16] Voir la formulation extrêmement large de l'exposé des motifs, p. 31.

[17] Voir par exemple les données relatives aux sites consultés par un Internaute qui ne devraient être conservées que dans certaines situations "exceptionnelles". En outre, d'autres données *a priori* exclues, comme la localisation en cas d'utilisation d'un GSM seront généralement conservées jusqu'au moment où la facturation ne peut plus être contestée. On ne peut dès lors exclure de manière définitive leur communication aux autorités durant ce délai.

iii) Durée de conservation

La Recommandation n° 3/99 du Groupe 29 demande de fixer un délai de conservation aligné sur la norme de protection la plus élevée observée dans les Etats membres[18]. Il semble, par exemple, qu'un délai de trois mois, tel qu'appliqué en Allemagne, soit suffisant en pratique. La Commission devrait en tout état de cause pouvoir se prononcer quant à ce délai.

En outre, la Commission ne peut se rallier aux critères avancés dans l'exposé des motifs à savoir, d'une part, un critère extrêmement large constitué par les besoins de l'action publique et, d'autre part, les possibilités des fournisseurs de services sur les plans technique et pratique. Ce dernier critère équivaut à admettre une extension des mesures en fonction des possibilités pratique et technique. Or deux caractéristiques ont toujours marqué l'évolution des technologies de l'information et de la communication : l'augmentation de la rapidité de traitement de l'information et la réduction des espaces nécessaires pour la traiter et la conserver. Si l'on suit ce raisonnement, dès que la technique le permettra, une durée plus longue devrait être admise.

3. Incitation à la création de nouveaux traitements

On notera que le texte en projet permet de contraindre les fournisseurs de services à enregistrer des données relatives aux données d'appel (qui appelle, qui est appelé, données d'identification de l'appelé, adresse Internet, …) qu'ils n'enregistreraient pas forcément pour la mise en œuvre de leurs services (en ce compris leur facturation). Ainsi des services de mobilophonie sans abonnement pourraient être soumis à l'obligation d'enregistrement.

Cette évolution a été stigmatisée par la Commission dans ses avis précédents (avis n° 34/97 et n° 12/99) qui a considéré "qu'au regard de l'évolution des technologies, la collaboration des opérateurs de réseaux de télécommunications et des fournisseurs de services sera dorénavant requise pour rendre efficaces les mesures ordonnées. Elle attire cependant l'attention du législateur sur le fait qu'une telle collaboration peut créer des risques nouveaux d'atteinte à la vie privée, dans la mesure où la réponse aux demandes de l'autorité publique peut requérir des traitements nouveaux dans le chef des opérateurs et des fournisseurs".

La Commission note encore que les justifications apportées dans l'exposé des motifs, et en particulier la facilité d'utiliser les réseaux de façon anonyme, ne lui apparaissent pas satisfaisantes et ne correspondent pas à la réalité. Il existe actuellement de nombreuses possibilités de repérer les utilisateurs de service de télécommunication sur la base des identifiants uniques, notamment dans le contexte d'Internet.

En application tant de l'article 4 de la loi du 8 décembre 1992 que de l'article 6, § 1er et 2 de la directive 95/46/CE, la finalité de tout nouveau traitement doit être suffisamment définie et explicite et le traitement doit être proportionnel par rapport à cette finalité.

En conclusion, la Commission est d'avis que le principe de proportionnalité devrait être appliqué strictement afin d'éviter la création d'un réservoir dans lequel de plus en plus de données pourraient être collectées dans des hypothèses de plus en plus diverses.

[18] Recommandation n° 3/99 du 7 septembre 1999 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit.

Conclusions

La Commission estime :

- qu'une législation réprimant la criminalité informatique participe indirectement à la protection de la vie privée dans la mesure où elle contribue à améliorer la sécurité des données à caractère personnel (en particulier, le projet n° 213/1) ;

- que les textes (en particulier, le projet n° 214/1) devraient néanmoins être amendés pour tenir compte des remarques énoncées dans le présent avis ;

- qu'une référence explicite à l'application de la loi du 8 décembre 1992 devrait exister dans le projet de loi ou à tout le moins dans l'exposé des motifs ;

- qu'un système de suivi des mesures envisagées devrait être mis en place incluant la Commission et qu'en tout état de cause une évaluation devrait être réalisée dans un délai maximum de 3 ans, évaluation à laquelle la Commission devrait être associée (formulation de critères spécifiques à l'instance chargée de l'évaluation, communication du rapport d'évaluation à la Commission) ;

- qu'elle devrait être saisie de tout projet d'arrêté royal adopté en exécution de ces textes.

Le secrétaire, Le président,

(sé) M.-H. BOULANGER (sé) P. THOMAS