AVIS N° 17 / 1997 du 9 juillet 1997

N. Réf. : 10 / A / 1997 / 009

OBJET : Application des articles 202 et 203 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses (collaboration technique des opérateurs à l'exécution de mesures judiciaires d'écoute entre autres).

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, en particulier l'article 29;

Vu la demande orale de M. le Chef de Cabinet adjoint du Ministre de la Justice du 2 avril 1997;

Vu le rapport de M. B. DE SCHUTTER,

Emet, le 9 juillet 1997, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS :

1. Le Ministre de la Justice a sollicité l'avis de la Commission sur la manière dont pourraient être exécutés les articles 70bis et 95, 5° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, insérés par la loi du 21 décembre 1994 portant des dispositions sociales et diverses.

La demande d'avis semble s'inspirer notamment de la question écrite, posée le 24 janvier 1997, par M. le député Decroly au Ministre à propos de l'interprétation des articles précités.[1]

II. LES DISPOSITIONS QUI CONSTITUENT L'OBJET DE L'AVIS :

2. L'article 70 bis de la loi du 21 mars 1991 concernant la réforme de certaines entreprises publiques économiques, inséré par l'article 202 de la loi du 21 décembre 1994, est libellé comme suit :

> *"Le Roi fixe, par arrêté délibéré en Conseil des ministres, les moyens techniques par lesquels Belgacom et les exploitants des services non réservés qu'il désigne doivent permettre, le cas échéant, éventuellement conjointement, le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées dans les conditions prévues par 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."*

L'article 95 de la loi du 21 mars 1991 dispose que le Ministre qui a les télécommunications dans ses attributions, peut, dans certains cas, sur proposition de l'Institut belge des postes et télécommunications, retirer l'agrément d'un appareil terminal ou imposer une interdiction de maintenir le raccordement à l'infrastructure publique de télécommunications. L'article 203 de la loi du 21 décembre 1994 a ajouté une cinquième hypothèse (art. 95, 5°) à la liste des cas énumérés. Dorénavant, le retrait et l'interdiction susvisés sont également possibles "lorsqu'il s'avère que :... 5° l'appareil terminal rend inefficaces les moyens permettant, dans les conditions prévues aux articles 88 bis et 90 ter à 90 decies du Code d'instruction criminelle, le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées".

3. Les deux dispositions précitées entendent garantir l'exécution des articles 88 bis et 90 ter à 90 decies du Code d'instruction criminelle, insérés par la loi du 30 juin 1994. Ces dernières dispositions confient au juge d'instruction la compétence de repérer, à certaines conditions, des numéros d'appels entrants et sortants (art. 88 bis) ou d'écouter les communications et les télécommunications privées, d'en prendre connaissance et de les enregistrer (articles 90 ter à 90 decies). L'article 70 bis de la loi du 21 mars 1991 vise à obliger les opérateurs à collaborer afin d'assurer l'"écoutabilité" de leur infrastructure, de leurs appareils et services.[2] L'article 95, 5° de la loi du 21 mars 1991 entend éviter que le matériel de chiffrement disponible sur le marché n'entrave l'exécution d'une mesure d'instruction ordonnée par le juge d'instruction.[3]

---

1 Question n°474, Bull. Q. R., Chambre, 1996-97, p. 9634.

2 Exposé des motifs du projet ayant donné lieu à la loi du 21 décembre 1994, Doc Parl., Sénat, 1994-95, n°1218-1, p.88.

3 Exposé des motifs précité, p. 89.

Au vu notamment de la question écrite de M. Decroly, la question est de savoir s'il est possible, voire souhaitable, eu égard à l'application des dispositions légales citées, d'interdire complètement l'utilisation de systèmes de chiffrement (la cryptographie), ou d'assurer l'exécution d'une mesure d'écoute par d'autres moyens.[4]

Cette question constitue l'objet du présent avis.

III. LA CRYPTOGRAPHIE : GENERALITES

A. Concepts

4. Le chiffrement (ou cryptage) est la procédure permettant de chiffrer au moyen d'un calcul mathématique des données claires et lisibles (texte, données, figures) en données codées, et ce, quel que soit le support d'information. Le déchiffrement (ou décryptage) est la procédure en sens inverse. Le chiffrement et le déchiffrement se réalisent au moyen de certaines clés et de certains algorithmes, à savoir des règles mathématiques exactement définies permettant d'obtenir un résultat déterminé à partir d'un nombre fini d'opérations.

5. En général, on distingue trois types de cryptosystèmes (terme désignant la combinaison de l'algorithme et de la clé). Ils sont succinctement passés en revue ci-dessous.

5.1. Le cryptosystème symétrique (clé secrète ou secret key)

Dans ce cas, la même clé sert au chiffrement et au déchiffrement. Cette clé doit dès lors rester secrète. Ces systèmes ont l'avantage d'être rapides, mais ne fonctionnent, en raison de la clé unique, que dans un système fermé dans lequel les parties se connaissent et se font confiance.

IDEA et DES sont des exemples d'algorithmes bien connus.

5.2. Le système asymétrique (clé publique ou public key)

Dans ce cas, des clés différentes servent au chiffrement et au déchiffrement, à savoir une clé privée et une clé publique. Cette méthode a l'avantage de révéler la clé publique, de façon à ce que chacun puisse envoyer des messages chiffrés à l'aide de la clé publique du destinataire, tandis que seul le destinataire peut les déchiffrer (à l'aide de sa clé privée). Cette méthode peut être utilisée dans un réseau ouvert, et ce, en raison de la stricte confidentialité de la clé privée. Ce système a toutefois le désavantage de fonctionner plus lentement qu'un système symétrique et d'être également plus coûteux.

Cette méthode est utilisée pour générer des signatures numériques qui permettent d'authentifier le message et son expéditeur. Dans ce cas, l'information est chiffrée à l'aide de la clé privée et déchiffrée au moyen de la clé publique.

Le RSA (algorithme de la clé publique Rivest-Shamir-Adelman) est un exemple de système de chiffrement asymétrique.

[4] Voir, outre la question de M. Decroly, la question orale de Mme Bribosia-Picard et la réponse de M. De Clerck, Ministre de la Justice, Ann. Parl., Sénat, 9 mai 1996, pp. 1032-1033 (*infra* n°17)

5.3. Les systèmes hybrides

En raison des avantages et des inconvénients que présente chacun des deux systèmes susmentionnés, on constate en pratique qu'ils sont souvent utilisés de manière complémentaire dans des systèmes qui combinent les avantages des deux systèmes.

Le progiciel PGP (Pretty Good Privacy) de Phil Zimmerman, qui est une illustration de ce système hybride, peut être obtenu et utilisé sur l'Internet.

6. Il est également important que les systèmes de chiffrement puissent être obtenus tant au niveau du matériel que du logiciel, certains étant même une combinaison des deux, et qu'en ce qui concerne les systèmes de clés, on puisse encore faire d'autres subdivisions: il existe notamment des systèmes qui utilisent des clés aléatoires (ou "random keys"), ce qui implique qu'ils changent de clé après quelques secondes, ou des clés de session (ou "session keys"), ce qui signifie que l'on change de clé (symétrique) après chaque session de communication.

B. Les fonctions de la cryptographie

7. Le présent avis se limite aux possibilités offertes par la cryptographie dans le but d'assurer la confidentialité d'un message. Le débat sur le chiffrement nécessite une prise en compte des autres fonctions que peut remplir la cryptographie dans la société de l'information, à savoir :

- garantir l'intégrité du message, c'est-à-dire veiller à ce que le message reçu soit identique au message expédié;
- assurer l'identification et l'authenticité du message et de son expéditeur : certifier l'identité de l'expéditeur et vérifier qu'il est bien l'expéditeur du message; la signature numérique joue un rôle important à cet égard;
- veiller à la non-répudiation (non-rejet) du message, ce qui est important d'un point de vue juridique, dans la mesure où l'on peut ainsi prouver un certain nombre de qualités du message vis-à-vis de tiers.

On évolue dès lors vers l'instauration de clés à double usage ("dual-use keys") qui seront utilisées tant à des fins d'authenticité, d'identification qu'à des fins de confidentialité.

Lorsque l'on examine la question de savoir comment éviter que le chiffrement n'entrave ou ne rende impossible la mission des pouvoirs publics de lutte contre la criminalité, il convient de ne pas uniquement s'attacher aux tensions existant entre, d'une part, la sécurité de l'information et, d'autre part, la protection de la vie privée, lesquelles constituent l'objet essentiel du présent avis. Comme indiqué précédemment, les systèmes de chiffrement asymétriques sont de plus en plus utilisés pour générer des signatures électroniques qui permettent de certifier qu'une personne déterminée a bien envoyé un message. Si les algorithmes et les clés permettant de générer ces signatures électroniques pouvaient être connus d'autres personnes que celles à qui appartient la signature électronique, celles-ci pourraient se faire passer pour elles et poser des actes juridiques au nom du titulaire de la signature électronique, ce qui pourrait susciter nombre d'incertitudes dans les relations juridiques.

C'est pourquoi l'utilisation du chiffrement est devenue un élément essentiel dans le cadre de la circulation des données, et ce, en vue de prévenir tout accès illicite aux données. La prévention de tels abus est notamment dictée par la protection de la vie privée. Le chiffrement est toutefois utilisé dans tous les secteurs du traitement des données, entre autres dans le commerce électronique, les transactions internationales ou sur l'Internet.

8. La garantie de confidentialité offerte par le chiffrement - et, dès lors, sa faculté de protéger la vie privée du citoyen - s'oppose toutefois directement à l'impuissance des pouvoirs publics d'obtenir dans certaines situations des informations utilisables, c'est-à-dire lisibles, dans l'exercice de leurs missions, en particulier dans le cadre de la lutte contre des formes graves de criminalité, et ce, essentiellement au niveau international. En effet, le crime organisé (trafic de drogue, activités de blanchiment de l'argent,...) a recours à des méthodes de chiffrement pour effectuer certaines transactions ou envoyer des messages.
La question est donc de savoir comment trouver un équilibre dans une société démocratique entre, d'une part, le droit au respect de la vie privée, et, d'autre part, la nécessité d'ingérence des autorités publiques, et ce, dans l'intérêt de la sécurité et de l'ordre publics et de la prévention des infractions.

IV. CADRE NORMATIF :

A. Le droit fondamental au respect de la vie privée

9. Le droit au respect de la vie privée est garanti par l'article 17 du Pacte international relatif aux droits civils et politiques, par l'article 8 de la Convention européenne des droits de l'Homme (ci-après C.E.D.H.) et par l'article 22 de la Constitution.

C'est plus particulièrement l'article 8 de la Convention européenne, en ce compris la jurisprudence développée par la Cour européenne des droits de l'Homme sur la base de cet article, notamment en ce qui concerne les écoutes, qui établit un certain nombre de fondements en vue de parvenir à l'équilibre évoqué ci-dessus entre le droit de l'individu à la protection de sa vie privée et l'intérêt d'une société démocratique de lutter efficacement contre la criminalité.

10. Pour qu'une ingérence dans le droit au respect de la vie privée soit licite, il faut qu'elle réponde à un certain nombre de conditions.

10.1. L'ingérence doit tout d'abord être "prévue par la loi". En ce qui concerne les mesures d'écoute, la loi doit ainsi contenir les dispositions suivantes :

1°- indiquer les catégories de personnes dont le téléphone peut être mis sur table d'écoute ainsi que les délits pour lesquels cette mesure peut être prise;
2°- limiter dans le temps l'autorisation de mettre le téléphone sur écoute;
3°- prévoir des règles en vue de dresser procès-verbal des écoutes téléphoniques;
4°- veiller à ce que le juge et la défense disposent des écoutes intégrales et intactes;
5°- prévoir des mesures de contrôle et des voies de recours nécessaires contre la mesure d'instruction;
6°- déterminer la tâche et la responsabilité du juge ordonnant la mesure;
7°- interdire le truquage, les tromperies et les provocations au moyen d'écoutes;
8°- respecter la relation confidentielle entre un prévenu et son conseil (avocat, médecin).

10.2. L'ingérence doit en outre rencontrer un ou plusieurs objectifs énumérés à l'article 8, alinéa 2.

En ce qui concerne la lutte contre la criminalité, il y a lieu notamment de faire référence à la protection de l'ordre public et à la prévention des infractions.

10.3. Enfin, l'ingérence doit être "indispensable" dans une société démocratique afin d'atteindre un des objectifs légaux susmentionnés.

La Cour européenne estime ainsi que la limitation du droit au respect de la vie privée doit répondre à un besoin social impérieux et satisfaire à l'exigence de proportionnalité: il doit exister, selon elle, un juste équilibre entre les droits de l'individu et les intérêts de la société.[5]

B. Les articles 90 ter à 90 decies du Code d'instruction criminelle

11. La faculté d'écouter et d'enregistrer des communications et des télécommunications privées (art. 90 ter à 90 decies du Code d'instruction criminelle) a été introduite (voir *supra*) par 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.

Les dispositions légales précitées, d'une part, précisent et renforcent l'interdiction d'écouter les conversations téléphoniques et, d'autre part, déterminent les possibilités et les conditions de dérogation à cette interdiction.

Les exigences prescrites à l'article 8, alinéa 2, de la C.E.D.H. relatives à la qualité d'une loi offrant un fondement juridique à l'ingérence dans la vie privée, semblent être rencontrées. Les dispositions légales précitées prévoient en effet un certain nombre de garanties pour la personne qui fait l'objet d'une mesure d'écoute judiciaire :

- en ce qui concerne la spécificité: l'ordonnance du juge d'instruction doit faire mention de la personne, du moyen de communication ou de télécommunication, ou du lieu soumis à la surveillance (art. 90 quater, § 1er, alinéa 2, 3°) et la mesure ne peut être ordonnée qu'à l'égard d'une liste limitative d'infractions (art. 90 ter, § 2);
- en ce qui concerne la limitation dans le temps : la mesure de surveillance ne peut excéder un mois à compter de la décision ordonnant la mesure (art. 90 quater, § 1er, alinéa 2, 4°). Cette mesure peut toutefois être prolongée à plusieurs reprises (art. 90 quinquies);
- en ce qui concerne le procès-verbal: les données recueillies lors de l'exécution de la mesure ne sont consignées dans le procès-verbal que si elles présentent un intérêt pour l'instruction (art. 90 sexies);
- en ce qui concerne la mise à disposition : les enregistrements, même les passages des conversations recueillies qui ne présentent aucun intérêt pour l'instruction, doivent être transcrits;
- la transcription intégrale et sa traduction éventuelle sont conservées au greffe sous pli scellé, il en est fait mention dans un registre (art. 90 septies);[6]
- en ce qui concerne le contrôle : l'autorisation accordée par le juge d'instruction doit être motivée, et doit, à peine de nullité, porter un certain nombre d'indications (art. 90 quater, § 1er) permettant un contrôle judiciaire. Un contrôle parlementaire est en outre possible, étant donné que le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des dispositions concernées (art. 90 decies);
- en ce qui concerne la mission du juge: le juge d'instruction se voit confier un rôle primordial;
- en ce qui concerne l'exactitude de l'enregistrement : les parties peuvent éventuellement contester l'exactitude de l'enregistrement sur la base de l'enregistrement même et de sa transcription (art. 90 septies);
- en ce qui concerne la confidentialité : sauf exception, la mesure ne peut s'appliquer aux médecins et aux avocats (art. 90 octies), et les données couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal (art. 90 sexies).

[5] Voir notamment, Cour eur. D.H., 19 février 1997, Laskey, Jaggard et Brown, § 42, à paraître dans Rec., 1997.
[6] L'intention est de supprimer, à l'avenir, l'obligation de transcrire intégralement les conversations recueillies (voir les articles 8 et 9 du projet de loi modifiant la loi du 30 juin 1994, Doc. Parl., Chambre, 1996-97, n° 1075-1). Dans l'avis n°09/97 du 20 mars 1997 relatif au projet de loi en question, la Commission n'a vu aucune objection à cette simplification.

12. L'interdiction des écoutes de "reconnaissance" (ou écoutes préventives) du fait même de la structure et de l'organisation de la législation belge est un élément pertinent pour l'évaluation des différentes options politiques en matière de cryptographie, interdiction qui ressort du fait que le juge d'instruction ne peut ordonner cette mesure qu'après avoir été chargé d'une instruction et lorsque les personnes concernées sont soupçonnées d'avoir commis des faits pouvant être considérés comme une des infractions citées explicitement à l'article 90 ter, §§ 1er et 2.

C. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

13. La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel est pertinente, même après la promulgation de la loi du 30 juin 1994.

L'article 16, § 3, de la loi du 8 décembre 1992 est libellé comme suit:

> *"Afin de garantir la sécurité des données à caractère personnel, le maître du fichier ou, le cas échéant son représentant en Belgique, doit prendre les mesures techniques et organisationnelles requises pour protéger les fichiers contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.*
> *Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.*
> *Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements."*

L'obligation de prendre des mesures de sécurité appropriées est d'ailleurs également prévue à l'article 7 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à l'article 17 (Sécurité des traitements) de la directive 95/46/CE du Parlement européen et du Conseil 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. Ces dispositions se basent également sur le principe "BATNEEC" ("Best available technology not entailing excessive costs").

V. EXECUTION DES ARTICLES 70 BIS ET 95, 5° DE LA LOI DU 21 MARS 1991

A. Dispositions imprécises

14. L'article 70 bis de la loi du 21 mars 1991 doit être lu à la lumière de l'article 90 quater, § 2, alinéa 1er, du Code d'instruction criminelle, lequel dispose que si la mesure comporte une opération sur un réseau de communication, l'opérateur de ce réseau est tenu de prêter son concours technique, quand le juge d'instruction le requiert. On peut déduire de la lecture conjointe de ces deux articles, l'obligation pour les opérateurs de veiller à ce que leur infrastructure, leurs appareils et services puissent être mis sur écoute.

Toutefois, à ce jour, aucun arrêté royal n'a été pris en exécution de l'article 70 bis. Les opérateurs demeurent, dès lors, dans l'incertitude quant aux caractéristiques techniques que doivent présenter leurs appareils pour pouvoir être mis sur écoute.
En outre, la loi ne précise pas davantage l'étendue des obligations de Belgacom et des exploitants des services non réservés. Il est dès lors difficile de contraindre au respect des obligations légalement imposées.

15. L'article 95,5° de la loi du 21 mars 1991 a lui aussi donné lieu à bon nombre de discussions.

Tout d'abord, les dispositions se limitent à mentionner des "appareils terminaux", alors que le chiffrement peut être proposé non seulement sous forme de matériel mais également sous forme de logiciel. A ce propos, le fameux PGP est un progiciel.
Ensuite, à l'instar de l'article 70bis, ces dispositions ne précisent en rien les normes techniques nécessaires afin de permettre la mise sur écoute d'un appareil.[7]
La simple disposition selon laquelle un appareil terminal ne peut rendre "inefficaces" les écoutes, manque de précision.
Force est de constater que le chiffrement ne rend pas inefficaces les moyens permettant l'écoute si l'on peut par la suite déchiffrer une communication enregistrée, et ce, par analogie avec une communication dans une langue étrangère pour laquelle la loi sur les écoutes ne prévoit également aucun régime spécifique, si ce n'est la traduction de l'enregistrement. En outre, l'expression "rendre inefficaces" suscite les mêmes difficultés à l'égard d'autres protocoles de télécommunications (EDIFACT) pour lesquels on peut, selon le point de vue adopté, décider qu'ils rendent ou non inefficaces les moyens permettant les écoutes.

16. L'article 70bis de la loi du 21 mars 1991, lu à la lumière de l'article 90 quater, § 2, du Code d'instruction criminelle, oblige donc Belgacom et les fournisseurs de services non réservés à veiller à ce que leur infrastructure, leurs appareils et services puissent être mis sur écoute. Traduit en termes de cryptographie, cela signifie que Belgacom et les fournisseurs de services non réservés ne peuvent offrir à leurs clients qu'une cryptographie susceptible d'être déchiffrée à tout moment. L'article 95, 5° de la loi du 21 mars 1991 permet, en outre, de mettre fin à l'offre de cryptographie dans des appareils terminaux.
La législation belge laisse ainsi une question importante sans réponse: quid d'un utilisateur qui se procure, par exemple par le biais de l'Internet, un logiciel de chiffrement (comme le PGP, Pretty Good Privacy) et envoie par la suite un signal chiffré chez Belgacom ou chez un autre fournisseur? Peut-on, sur la base d'une interprétation très large de l'article 70 bis, conclure que Belgacom et les autres fournisseurs doivent, dans un tel cas, refuser au signal l'accès à leur réseau ?
Cette conclusion serait naturellement synonyme d'une interdiction partielle de la cryptographie en Belgique et accentuerait le problème de la compatibilité de l'article 70 bis avec l'article 8.2 de la C.E.D.H. La législation en matière de cryptographie doit, en effet, à l'instar de la législation sur les écoutes, répondre aux critères de l'article 8.2 de la C.E.D.H. En revanche, si l'on part du principe que les opérateurs ne doivent pas refuser l'accès à leur réseau dans le cas susvisé, on arrive à la conclusion qu'il existe une différence de traitement difficilement justifiable entre, d'une part, l'utilisateur qui s'est procuré un progiciel de chiffrement par la voie traditionnelle ou par le biais de l'Internet et qui n'est pas inquiété, et, d'autre part, l'utilisateur qui a obtenu ses facilités de chiffrement par l'entremise de son opérateur en télécommunications et qui doit tenir compte du fait que cet opérateur est susceptible à tout moment de mettre à la disposition du pouvoir judiciaire les moyens de déchiffrement.

[7] La Commission fait observer que le Ministre qui a les télécommunications dans ses attributions, pourrait, sur la base de l'article 94, § 2, de la loi du 21 mars 1991, fixer les spécifications techniques auxquelles doivent répondre les appareils terminaux. S'il s'avérait qu'un appareil ne répond plus à de telles spécifications, il pourrait, sur la base de l'article 95, 2°, retirer l'agrément. Dans ce cas, le retrait d'agrément ne devrait pas être basé sur la disposition imprécise de l'article 95, 5°.

B. Position gouvernementale à l'égard de l'exécution des articles 70 bis et 95, 5°

17. Lors des travaux parlementaires préparatoires de la loi du 21 décembre 1994 insérant les articles 70 bis et 95, 5°, dans la loi du 21 mars 1991, le Ministre des Transports a admis que l'on n'avait pas encore d'idée précise quant à la manière d'autoriser les écoutes téléphoniques.[8]

En réponse à une question orale du sénateur Bribosia-Picard, le Ministre de la Justice a donné, le 9 mai 1996, une série d'indications quant aux éventuels moyens, sans toutefois opter clairement pour l'une ou l'autre possibilité. Il ressort de la réponse du Ministre qu'il n'est pas partisan d'une interdiction générale de la cryptographie, et encore moins du dépôt systématique des clés auprès d'une instance désignée à cet effet (l'Institut belge des services postaux et des télécommunications). Selon le Ministre, il serait souhaitable de tendre "à une accessibilité maximale des réseaux en collaboration avec les gestionnaires de clés, le "trusted third party", un tiers qui peut créer une liaison et un accès au réseau, l'opérateur, le gestionnaire du réseau". "L'intention est également de collaborer avec les opérateurs de l'infrastructure des télécommunications."[9]

C. Examen d'un certain nombre d'options politiques éventuelles, plus particulièrement sous l'angle de la protection de la vie privée.

a). Interdiction de la cryptographie

18. L'interdiction de la cryptographie, interdiction qui peut également connaître une certaine gradation[10] au niveau de la sévérité, est difficilement envisageable pour différentes raisons.

D'une part, une telle interdiction serait difficilement défendable, en raison du très grand nombre (sans cesse croissant) de communications, et ce, compte tenu également de la part sans cesse croissante des communications internationales et de la disponibilité de la cryptographie par des canaux, qui, comme l'Internet, échappent (provisoirement ?) au contrôle des autorités. Dans les pays qui connaissent une interdiction totale de la cryptographie (comme l'Arabie Saoudite), voire une interdiction partielle (comme l'Afrique du Sud : interdiction de chiffrer sur le réseau téléphonique public), cette interdiction est largement ignorée. Il paraît donc exclu pour un pays de faire 'cavalier seul' dans ce domaine.

Une telle interdiction entraverait en outre considérablement le développement de la société de l'information, étant donné que la cryptographie joue un rôle important dans ce développement. Cette interdiction mettrait non seulement en péril la garantie de confidentialité des messages, mais le public et le monde des entreprises se verraient également privés d'autres applications de la cryptographie, parmi lesquelles l'authentification.
Une interdiction générerait des désavantages concurrentiels pour les entreprises. Elle pourrait également soulever des problèmes relevant du droit privé, dans la mesure où l'absence de sécurité suffisante peut, en cas de préjudice, être considérée comme un manque de prévoyance ou une négligence (acte licite) et donner lieu à une action en responsabilité, ce qui pourrait finalement engager la responsabilité des pouvoirs publics.
En outre, une telle interdiction ne satisferait ni au critère de pertinence, tel que développé par la jurisprudence de la Cour européenne des droits de l'Homme, sur la base de l'article 8.2. de la C.E.D.H., ni au critère de proportionnalité, développé par la même Cour, sur la base du même article. Une interdiction isolée de la cryptographie n'est, en effet, pas pertinente, étant donné qu'elle serait inefficace (voir *supra*), elle est en outre tout à fait disproportionnée, même s'il ne

[8] Rapport de Mme Cahay-Andre, Doc. Parl., Sénat, 1994-95, n° 1218-9, p. 5; déclaration de M. Di Rupo, Ministre des Transports, Ann. Parl., Sénat, 1er décembre 1994, p. 442.
[9] Déclaration de M. De Clerck, Ministre de la Justice, Ann. Parl., Sénat, 9 mai 1996, p. 1032.
[10] On peut distinguer : l'interdiction de disposer ou d'avoir en réserve de la cryptographie ; l'interdiction de disposer ou d'offrir de la cryptographie à des fins de distribution ; l'interdiction de divulguer ou d'offrir publiquement de la cryptographie.

s'agissait que d'une interdiction de la "cryptographie de confidentialité", étant donné qu'un nombre considérable d'utilisateurs potentiels se verraient privés du moyen de garantir la confidentialité de leurs communications, et ce, dans le but de permettre dans un nombre limité de cas l'écoute de communications.

Dans le cas spécifique de la Belgique, une interdiction de la cryptographie est difficilement conciliable avec les obligations du maître du fichier, telles qu'énoncées à l'article 16, § 3, de la loi du 8 décembre 1992. La Commission estime enfin devoir attirer l'attention sur le fait qu'un avant-projet de loi néerlandais visant à interdire la cryptographie a été retiré par le gouvernement néerlandais à la suite de vives protestations.

b). Interdiction de certaines formes poussées de cryptographie.

19. Les mêmes arguments peuvent grosso modo être invoqués tant contre une interdiction limitée que contre une interdiction totale.

En outre, on court dans ce cas davantage le risque de faire le jeu du crime organisé au lieu de le combattre : les criminels ignoreront cette interdiction et verront leurs communications protégées par des systèmes de chiffrement infaillibles, alors que dans le même temps, il leur sera plus facile d'accéder à l'information des entreprises (et des particuliers) qui, en bons "(corporate) citizens ne pourront chiffrer leurs informations qu'au moyen d'applications de chiffrement moins performantes.

Une approche fondée sur une interdiction limitée nécessiterait en outre un contrôle permanent des évolutions sur le terrain et exigerait la mise en place d'une procédure souple en vue d'adapter les normes en fonction de ces évolutions.

c). Dépôt de clés.

20. Le dépôt de clés, appelé également en anglais "recovery" ou "key escrow", signifie que les clés de déchiffrement sont déposées soit auprès des autorités publiques (voir entre autres la proposition américaine Clipper Chip I), soit auprès d'un tiers (un "trusted third party" (TTP), (TPC), voir entre autres l'actuelle loi française et la proposition américaine Clipper Chip II), soit conservées chez la personne, mais tout à fait indépendamment des utilisateurs au sein de l'entreprise (ce que l'on appelle le "self-escrow", voir entre autres la proposition américaine Clipper Chip III).
Les problèmes techniques et les frais qu'engendrerait un tel système sont énormes. L'ultima ratio de tout système de dépôt de clés doit en effet être une application au niveau mondial de celui-ci. En outre, les problèmes majeurs de gestion des clés sont précisément créés par ces systèmes qui impliquent une ingérence minime dans la vie privée, à savoir les systèmes à clés variables et/ou de session, qui permettent en effet de limiter le déchiffrement à une communication déterminée, voire à une partie de celle-ci.

21. Dans un rapport récent du 27 mai 1997, intitulé "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption",[11] un certain nombre de spécialistes (professeurs, chercheurs au MIT et à Cambridge, et des spécialistes de Sun, Microsoft et d'AT&T) estiment que: "Key recovery as envisioned by law enforcement will require the deployment of secure infrastructures involving thousands of companies, recovery agents, regulatory bodies, and law enforcement agencies worldwide interacting and cooperating on an unprecedented scale", et que: "The commercial and academic world simply does not have the tools to properly analyze or design the complex systems that arise from key recovery".
Il convient également de songer aux frais liés à la gestion des "recovery agents" (ou agents de récupération); ceux-ci devront en effet travailler en équipes, 24 heures sur 24, 7 jours sur 7, afin de parvenir à un temps de réponse tel que suggéré dans différentes propositions - le modèle américain préconise la récupération des clés dans un délai de deux heures, le projet britannique propose même un délai d'une heure.

[11] http://www.crypto.com/key_study/report.shtml.

En outre, il n'est pas impensable que ces "recovery agents" soient eux aussi victimes d'attaques.

Selon les auteurs du rapport, l'argument selon lequel ces "recovery agents" peuvent également être utiles aux entreprises dans le cadre de procédures judiciaires n'est pas pertinent. Les partisans estimaient que les entreprises avaient également besoin de facilités de "récupération des clés", par exemple en cas de perte ou de vol d'une clé ou en cas de refus de la part d'un ancien employé de rendre ses clés. Les auteurs du rapport sous-estiment ce besoin, mais prétendent que la "law enforcement key recovery" ne sera d'aucune aide en la matière, étant donné que les besoins des entreprises et ceux des pouvoirs publics sont totalement différents à cet égard, et que les systèmes n'auraient dès lors que peu de choses en commun.

Ils partent ainsi des principes suivants :

a) le monde des entreprises a tout intérêt à récupérer des clés pour les données enregistrées, tandis que la "law enforcement" (récupération en application de la loi) a tout avantage à pouvoir récupérer toutes les clés, en particulier celles qui sont utilisées pour chiffrer les sessions de communication;
b) le monde des entreprises n'a aucun intérêt à disposer d'une possibilité de récupérer l'authentification ou les clés de la signature numérique, ce qui peut même mettre en péril certains concepts, comme la non-répudiation, alors qu'il est très difficile d'exclure un tel type de clés dans un système de "key recovery", étant donné l'existence de "dual-use keys";

c) le monde des entreprises a besoin pour le commerce électronique d'autorités de certification, chargées de garantir l'identité de l'utilisateur du chiffrement et non de "key recovery agents"[12].

22. Du point de vue juridique, ces systèmes posent également un certain nombre de problèmes. A ce niveau aussi, il est loin d'être certain qu'ils satisfassent aux conditions de l'article 8.2. de la C.E.D.H. Un système national pourrait être considéré comme non pertinent, et, de manière générale, tous les systèmes pourraient être considérés comme disproportionnés. En effet, on donne à l'avance les possibilités aux services d'ordre d'intercepter les communications de tous les utilisateurs, même si l'on ne peut recourir à une telle mesure que dans un nombre de cas strictement limité. Lorsque les clés ne sont pas déposées suffisamment "loin" des services d'écoute, on crée des "incitants" aux écoutes de reconnaissance (ou proactives), ce que le législateur belge a voulu interdire formellement.

Un autre problème concerne les systèmes à basse (key-granularity), ce qui signifie que seul un nombre restreint de types de clés peuvent être récupérés et que les données susceptibles d'être obtenues auprès du "recovery agent" ne peuvent être définies que de manière très large (par exemple toutes les données relatives à un utilisateur déterminé). Le tout est bien entendu de savoir si ce type de système satisfait au principe de proportionnalité prévu à l'article 8.2. de la C.E.D.H.

Dans le cas spécifique de la Belgique, le problème est à nouveau de savoir comment concilier le système de dépôt de clés avec l'obligation de moyens du maître du fichier, aux fins de garantir la sécurité de ses traitements, telle que visée par la loi du 8 décembre 1992.

La Commission doit par ailleurs reconnaître qu'il existe également des avantages liés à cette technique, dans la mesure où un système de licence serait mis en place pour la cryptographie du dépôt de clés. L'utilisation d'une cryptographie non autorisée pourrait dès lors indiquer l'existence d'activités criminelles.

[12] Contrairement aux « key-recovery agents » les autorités de certification ne connaissent pas et ne doivent pas connaître les clés secrètes des utilisateurs. Certaines propositions (ex. Clipper Chip III) s'efforcent de concilier les deux systèmes, ce qui s'avère dangereux, car on court le risque qu'en cas de « law enforcement » les services d'ordre aient également accès aux (clés des) signatures numériques.

23. Etant donné qu'un système de dépôt de clés doit par définition pouvoir fonctionner au-delà des frontières, il serait préférable d'adopter une approche plus internationale.
A l'heure actuelle, des règles de conduite claires font cependant défaut en la matière.
La Commission européenne élabore à l'heure actuelle une directive,[13] la "recommandation n° R (95) du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information"[14] du Conseil de l'Europe permet une immixtion dans des matières liées au droit pénal tandis que la recommandation de l'OCDE "Recommendation of the Council concerning guidelines for cryptography policy"[15] se limite à la formulation suivante: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible. (...) This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access."

24. Compte tenu de tous ces éléments, la Commission estime que la solution du dépôt de clés suscite trop de problèmes organisationnels et qu'elle accorde dans la pondération entre le droit à la protection des données à caractère personnel et l'importance de la lutte contre le crime, un poids disproportionné à ce dernier aspect.

d). Normalisation.

25. Les Etats-Unis, où la cryptographie connaît l'expansion la plus forte, ont pris une série d'initiatives en vue de réglementer l'utilisation de la cryptographie à l'intérieur de leurs frontières. Jusqu'à présent, trois initiatives importantes ont vu le jour.

1. Clipper Chip I

26. Lorsque les pouvoirs publics américains ont pris conscience de l'échec de leur tentative de limiter à l'administration l'utilisation de la norme développée sous leurs auspices, ils se sont efforcés d'introduire cette norme en dehors du domaine public, et ce, par analogie avec la norme Internet TCP/IP, utilisée aujourd'hui au niveau mondial.

Ils ont tenté d'atteindre leur objectif en lançant l'initiative Clipper Chip qui porte création d'une nouvelle norme de chiffrement (EES ou Escrowed Encryption Standard). Cette puce serait incorporée dans le matériel et les deux éléments de la clé seraient déposés auprès des autorités publiques.

L'intention n'était pas d'interdire d'autres formes de chiffrement, mais les autorités voulaient profiter au maximum de leur position de principal client de chiffrement afin de l'élever au rang de norme. En effet, elles n'achèteraient elles-mêmes que du matériel pourvu de cette puce Clipper.
Cette initiative a provoqué une vague de protestations, et ce, essentiellement en raison du fait que les services publics avaient été choisis pour être dépositaires des clés.

[13] COM(94), 128 def, COD 288 et COM (97) 94 def – COD 288.
[14] http://www.privacy.or…e/info-tech—1995.html.
[15] http://www.oecd.org/dsti/iccp/crypto-e.html.

2. Clipper Chip II

27. Le Clipper Chip II fut créé par les autorités américaines en réaction au rejet du Clipper Chip I. L'initiative Clipper Chip II a élargi la possibilité du dépôt de clés à des organismes indépendants choisis par les utilisateurs du chiffrement.

La crainte subsistait toutefois que les autorités, une fois qu'elles auraient conquis une part de marché suffisamment importante, rendent l'"escrowed encryption" légalement obligatoire. Un autre point névralgique de cette initiative concernait le fait que l'algorithme de chiffrement "Skipjack" était gardé secret, tant et si bien que l'on ne pouvait pas tester sa validité.

Pour l'Europe, l'idée que des appareils pour lesquels les autorités américaines disposeraient en permanence de la possibilité de déchiffrement seraient proposés sur le marché européen, était peu attrayante.

Finalement, l'initiative Clipper Chip II devait elle aussi être abandonnée par les autorités américaines.

3. Clipper Chip III

28. En lançant une nouvelle initiative, baptisée Clipper Chip III, les pouvoirs publics américains n'entendent pas imposer une norme. Cette initiative met l'accent sur un système de gestion de clés, la participation à ce système se faisant sur une base volontaire et le choix de l'algorithme étant libre.

Les utilisateurs sont encouragés à participer à ce système, étant donné que la participation au commerce électronique en dépendrait. Selon ce système, les autorités de certification, tant privées que publiques, nationales qu'internationales, ainsi que les "Key recovery agents" (KRA) ou agents de récupération de clés publics ou privés seraient enregistrés. Une autorité de certification enregistrée ne peut délivrer à l'utilisateur un certificat de clé publique, certificat qui à court terme devrait devenir une condition pour pouvoir prendre pleinement part au commerce électronique, que si celui-ci a fait parvenir à un agent de récupération de clés enregistré les informations nécessaires pour permettre le "lawful access" (accès légal). Compte tenu des résistances des experts quant au fait de relier les concepts d'autorité de certification et d'agent de récupération de clés, il y a fort à craindre que cette initiative, qui va de pair avec un soutien massif du "key recovery encryption" au niveau politique, ne puisse marquer un tournant définitif.

La leçon que l'on peut tirer des initiatives américaines est la suivante: toute tentative de réglementation, si elle veut avoir des chances de réussir, doit être élaborée en étroite collaboration avec le monde des entreprises. Il ne fait toutefois pas l'ombre d'un doute que les entreprises ne font preuve que de très peu d'enthousiasme.

e). Autorisation préalable à l'utilisation du chiffrement.

29. Un système d'autorisation préalable met l'accent sur une communication préalable d'informations aux autorités quant à l'utilisation des clés de chiffrement, informations qui doivent principalement viser à justifier cette utilisation.
Là aussi, la question est de savoir si une telle solution peut être opérationnelle. Le monde des entreprises continuera à s'opposer à tout système administratif empreint d'une trop grande lourdeur. Cette solution a toutefois l'avantage, d'une part, d'informer les autorités, et, d'autre part, de protéger l'utilisateur, étant donné qu'il ne doit pas y avoir de remise de clés. Il conviendra toutefois d'attendre les critères qui seront utilisés par les pouvoirs publics pour accorder ou refuser cette autorisation.

Une alternative plus simple pourrait consister à remplacer purement et simplement l'autorisation par une obligation de déclaration.

f). Obligation de collaborer.

30. L'obligation pour les opérateurs en télécommunications de collaborer avec les pouvoirs publics dans le cadre des mesures d'écoute est manifestement le seul point commun de toutes les législations en matière de cryptographie en Europe occidentale. En Belgique, ces obligations sont inscrites à l'article 70bis de la loi du 21 mars 1991 et à l'article 90 quater,§ 2, du Code d'instruction criminelle.

Il est toutefois difficile de respecter cette obligation lorsque l'initiative du chiffrement émane de l'utilisateur et lorsque le chiffrement n'est pas proposé par l'opérateur, en d'autres termes lorsque l'utilisateur fournit le signal chiffré à son opérateur (cf. *supra* n°16).

Une obligation de collaborer formulée de manière beaucoup plus large permettrait toutefois de remédier (partiellement) à ce problème.
En Belgique, une telle obligation, formulée de manière plus large, est au coeur de la proposition de loi du 11 juin 1996 de Mmes Bribosia-Picard et Maximus.[16] Cette proposition entend abroger les articles 70 bis et 95, 5° de la loi du 21 mars 1991 et remplacer la réglementation existante par une obligation générale de collaboration. La disposition clé est l'article 90 duodecies du Code d'instruction criminelle, dont l'alinéa premier est libellé comme suit : "Lorsque les nécessités de l'instruction l'exigent, le juge d'instruction peut, à titre exceptionnel, requérir l'aide au décryptage d'un message, de toute personne susceptible de fournir cette aide, s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées à l'article 90 ter, §§ 2, 3 et 4, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité."

VI. CONCLUSION GENERALE :

31. L'équilibre recherché entre la protection de la communication de données et la mission nécessaire des autorités de lutte contre les infractions graves ne pourra peut-être être atteint que par une intervention du législateur. Une réglementation en matière de chiffrement va au-delà de la seule protection du message. L'authenticité, qui est assurée par ces systèmes de clés asymétriques, est essentielle pour la reconnaissance de la signature électronique et influe sur tous les effets juridiques y afférents, tant en ce qui concerne le message que la personne elle-même.
La Commission estime qu'une solution dans le sens d'une obligation générale de collaboration, fondée sur les limitations et les garanties analogues à celles prévues par les articles 90 ter à 90 decies du Code d'instruction criminelle, semble être à l'heure actuelle l'option la plus opérationnelle.

32. Le présent avis est nécessairement de nature générale. La Commission se réserve dès lors le droit de préciser et d'adapter éventuellement son point de vue dans le cadre d'un projet concret ou d'une proposition concrète qui lui serait soumis.

Le secrétaire — Le président

(sé)J. PAUL — (sé)P. THOMAS

[16] Proposition de loi abrogeant les articles 70 bis et 95, alinéa 1er, 5°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques et complétant le Code d'instruction criminelle par des dispositions relatives au décryptage des messages, Doc. Parl., Sénat, 1995-1996, n° 1-352/1.