ROYAUME DE BELGIQUE

COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

Bruxelles, le

Adresse : Av. de la porte de Hal, 5 - 8, B-1060 Bruxelles
Tél.: +32(0)2/542.72.00 Email : commission@privacy.fgov.be
Fax.: +32(0)2/542.72.12 http://www.privacy.fgov.be/

AVIS N° 08 / 2004 du 14 juin 2004

N. Réf. : SA2 / A / 2004 / 008

OBJET : Avant projet de loi relatif aux communications électroniques

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 d'avis, datée du 19 mai 2004, du Ministre de l'Economie, des PME, des Classes moyennes et de l'Energie;

Vu le rapport du Président ;

Emet, le 14 juin 2004, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS:

La Commission est consultée par le Ministre de l'Economie, des PME, des Classes moyennes et de l'Energie sur un avant-projet de loi relatif aux communications électroniques.
Ce texte a pour objet la transposition en droit national de six directives européennes constituant un nouveau cadre réglementaire européen relatif aux communications électroniques. Ce nouveau cadre réglementaire inclut la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
La Commission est consultée sur les aspects de l'avant-projet de loi qui concernent la protection des données à caractère personnel, et donc plus particulièrement les articles 122, 125, 133 à 144 de l'avant-projet, qui transposent la majeure partie des dispositions de la directive européenne 2002/58.

L'article 13 de la directive 2002/58 relatif à la prospection par courrier électronique peut être considéré comme étant transposé par l'article 14 de la loi du 11 mars 2003 relative à la société de l'information ainsi que par son arrêté royal d'exécution du 4 avril 2003. On relève néanmoins une différence de terminologie entre la directive, qui utilise la notion de prospection directe (ou marketing direct), et la loi belge, qui utilise celle de publicité.
En outre, la prospection par fax ou automate d'appel, également visée par la directive européenne, est toujours réglementée en droit national par la loi relative aux pratiques du commerce[1], qui ne protège que les consommateurs (au lieu des abonnés ou utilisateurs), dans le cas de contrats à distance.
Il s'ensuit une divergence dans le champ d'application des textes de droit belge par rapport à celui de la directive.
La Commission appelle de ses vœux une clarification officielle en ce qui concerne l'objet exact visé par les réglementations relatives à la prospection par courrier électronique, fax ou automate d'appel. Elle ajoute que la solution ne peut s'écarter de celle de la directive européenne et doit englober la sollicitation politique ou venant d' organismes à but non lucratif.

II. LÉGISLATION APPLICABLE :

Le présent avis a pour objet d'analyser les articles de l'avant-projet qui concernent la protection de la vie privée.
Ces articles sont examinés tant au regard des principes de 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 »), qu' au regard des principes de la directive 2002/58 qu'ils sont supposés transposer.

III. EXAMEN DE LA DEMANDE D'AVIS :

L'avant-projet de loi aborde différents aspects de la protection de la vie privée en matière de communications électroniques. Il s'agit, dans l'ordre des articles de la loi, des aspects suivants :

- **Le détail des factures** de télécommunication fournies aux abonnés (article 122) ;
- **La sécurité** des réseaux et services (article 125) ;
- **La confidentialité** des données de trafic (article 133) ;
- La confidentialité des données de localisation (article 134) ;

[1] Loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur.

- La confidentialité des informations et données transmises par voie de télécommunication (articles 135 et 136) ;

- **L'enregistrement et la conservation** de certaines données de communication (article 137) ;
- L'identification de l'appelant, la surveillance et les écoutes des communications privées dans le cadre de procédures judiciaires (article 138) ;

- L'enregistrement de données relatives à des **transactions commerciales** (article 139) ;

- La protection de l'abonné ou utilisateur contre les **cookies et autres fichiers ou logiciels espions** (article 140) ;

- Les conditions de présentation de **l'identification de l'appelant et de l'appelé** (article 141) ;
- Le **renvoi automatique** des appels (article 142) ;
- Les exemptions à ces deux principes (article 143) ;

- Les conditions de collecte et de publication des données relatives aux abonnés dans les **annuaires**.

EXAMEN DES ARTICLES

1. Détail des factures de télécommunication

L'article 122 de l'avant-projet de loi transpose en droit interne le principe selon lequel les abonnés ont le droit de recevoir des factures non détaillées (article 7 de la directive). L'avant-projet de loi précise que ce droit peut s'exercer gratuitement. Conformément au texte européen, il prévoit également des garanties complémentaires en matière de protection des données. Notamment, les appels gratuits ainsi que ceux vers certains numéros d'urgence ne sont pas indiqués sur la facture. Le Roi peut également décider, sur avis de l'institut, que certains autres numéros ne seront pas indiqués sur la facture.
Cette disposition a pour conséquence que certains appels vers des services de détresse ou d'assistance, tels que Child Focus, par exemple, restent confidentiels.

La Commission n'a pas d'observation de fond sur le contenu de cette disposition, conforme au droit européen et protecteur de certains membres de la famille ou du groupe social, utilisateurs des services vis à vis de l'abonné. Il serait néanmoins utile que la finalité de cette exception soit plus clairement précisée : il s'agit de permettre un « non affichage » d'un numéro chaque fois qu' il ressort de la nature du service attaché au numéro appelé qu' il existe un intérêt supérieur à garder la communication secrète. Si telle est la finalité de l'exception, la Commission s'interroge sur la nécessité de prévoir une procédure plus légère d'adaptation de la liste des numéros dits confidentiels. A cet égard, le procédure prévue par la loi à savoir le recours à un arrêté royal pris sur avis de l'IBPT peut apparaître lourde.

La Commission rappelle ensuite qu'elle s'était déjà prononcée, dans le cadre d'échanges de points de vue (informels) avec l'IBPT et Belgacom, sur la problématique consistant à identifier le caractère sensible de certains numéros qui ne sont pas des numéros d'urgence, et qui ne bénéficient pas de la gratuité. On cite par exemple les numéros à taxation partagée de type 078 / 15… et certains numéros à taxation normale, de type 02/…, tel que celui d'infor-drogues par exemple.
La Commission s'était prononcée pour un élargissement de la gratuité des numéros d'assistance, qui seraient ainsi supprimés automatiquement des factures. Les numéros ayant trait à la protection de l'enfance devraient constituer une priorité.
En outre, la Commission avait insisté pour que des informations claires soient fournies non seulement aux abonnés mais au public en général sur les modalités de présentation du détail des factures, ainsi que sur les numéros qui n'apparaissent pas sur ces factures.

2. Sécurité des réseaux et services de télécommunication

L'article 125 de l'avant-projet transpose l'article 4 de la directive européenne. Il impose aux opérateurs de prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de leurs réseaux et services.
La Commission relève que la directive impose cette obligation à tout *fournisseur de services* de communication électronique, alors que le texte belge adresse cette obligation uniquement aux *opérateurs*.
Toutefois, la Commission note que la notion d'opérateur, telle que définie dans l'avant-projet de loi, vise toute personne ayant notifié à l'IBPT une série d'éléments détaillés par la loi en vue de fournir en nom propre et pour son propre compte *des services ou des réseaux de communication électronique*.
La notion d'opérateur en droit belge est ainsi particulièrement large, et s'applique au fournisseur d'un service de communication électronique tel que visé par la directive. La Commission demande cependant que ce point soit vérifié.

La Commission note que la directive prévoit également en son article 4.2 l'obligation des fournisseurs de service d'informer les abonnés des risques de violation de leur vie privée encourus du fait de l'utilisation des services offerts. Cette disposition doit être reprise. Elle oblige par exemple les fournisseurs d'accès à avertir leurs clients des possibilités d'interception de mails, de cookies ou spyware et à indiquer les moyens de s'en protéger (logiciels d'anonymisation, d'encryptage, possibilités d'activer des anti-cookies ou -spyware) et le cas échéant les coûts de telle protection.

3. Confidentialité des communications

L'avant-projet de loi prévoit, conformément au texte européen, une obligation générale de suppression ou d'anonymisation des données de communication dès qu'elles ne sont plus nécessaires à la transmission de la communication. Contrairement à une idée généralement reçue, le principe général n'est donc pas la rétention des données de communication.
Le texte prévoit néanmoins un certain nombre d'exceptions, dans le cadre de la recherche ou la poursuite d'infractions pénales, l'utilisation malveillante du système de communication, ou, dans le chef de l'opérateur, lorsque ce dernier a besoin des données pour l'établissement de la facturation ou les paiements d'interconnexion, ou, moyennant le consentement de l'intéressé, pour lui offrir certains services de communication.

Le texte opère une distinction entre les données de trafic au sens propre, qui sont nécessaires au service de communication (acheminement de la communication, ou facturation), et les données qui ne sont pas strictement nécessaires à ce service, mais qui sont utilisées dans le cadre de services à valeur ajoutée (tels que les services de localisation).

a. En ce qui concerne les données de trafic au sens strict (article 133)

- *Limitation des données qui peuvent être traitées par les opérateurs*

Le paragraphe 2 de l'article 133 énumère les données qui peuvent être traitées par les opérateurs dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion.

La Commission souligne qu'en vertu de l'article 6 de la directive européenne, seules les données *nécessaires* à la facturation et/ou le cas échéant aux interconnexions peuvent être traitées : il ne peut donc s'agir, pour les opérateurs, de traiter systématiquement toutes les données figurant sur la liste de l'article 133 en projet. Un examen devra être effectué par l'opérateur, au cas par cas et selon les besoins propres au service presté, afin d'identifier parmi les données figurant sur la liste celles qui sont nécessaires au traitement.

- *Protection de l'abonné ou de l'utilisateur*

La Commission note en outre que le paragraphe 2 *in fine* apporte une restriction à la protection prévue par la directive européenne lorsque l'utilisateur final est une personne morale (le plus souvent un employeur) : dans la plupart des cas, seule la personne morale doit être systématiquement informée et consultée, et non les utilisateurs (les employés). L'exposé des motifs explique que l'opérateur est ainsi dispensé, pour des raisons pratiques, de communiquer les informations relatives au traitement des données à tous les utilisateurs finals individuels.
La Commission s'interroge sur la compatibilité de cette restriction avec le principe de confidentialité tel que prévu par la directive européenne. Si dans certains articles la protection est explicitement limitée aux abonnés (facturation détaillée, annuaires…), ce n'est pas le cas en ce qui concerne les dispositions relatives à la confidentialité des communications. Le texte européen s'applique aux utilisateurs *ou* aux abonnés, en fonction de la qualité de celui qui est concerné par les données (« pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement »).
Il apparaît dès lors douteux que le texte de transposition en droit belge puisse exclure de la protection prévue par la directive les utilisateurs d'un service de communication dans le cas où l'abonné est une personne morale.

Lorsque le texte prévoit l'information « *le cas échéant* » de l'abonné ou de l'utilisateur, des précisions sur la notion de *« cas échéant »* seraient souhaitables[2].
Par ailleurs, l'alinéa 2 du paragraphe 2 prévoit la fourniture de l'information à l'abonné ou à l'utilisateur, avant le traitement. La Commission s'interroge sur la façon dont l'information pourra ainsi être transmise avant le traitement à la personne concernée.

La Commission souligne que lorsque l'opérateur offre à l'abonné des services à valeur ajoutée relatives à des données propres aux utilisateurs couverts par l'abonnement (par exemple aide pour la facturation interne, détection de trafics anormaux en provenance d'un poste, fréquence d'appels à partir des différents postes) soit ces services sont offerts dans le cadre d'une pure sous-traitance, soit ils sont offerts par l'opérateur en tant que responsable de traitement. Suivant les hypothèses, des obligations d'information différentes existeront dans le chef de l'abonné vis-à-vis de ses utilisateurs.

- *Marketing des services de l'opérateur*

Le paragraphe 3 de l'article 133 autorise le marketing de services de communication électronique ou de services à données de trafic ou de localisation moyennant information et consentement préalable de l'intéressé.
Ici également, la Commission relève la portée limitée des garanties lorsque l'abonné est une personne morale.
Par ailleurs, elle constate que, au regard de la directive européenne, il n'est pas indiqué de façon suffisamment explicite que seuls sont autorisés les services *propres offerts par l'opérateur*.

[2] La directive européenne donne les précisions suivantes à ce sujet : « la question de savoir si c'est de l'utilisateur ou de l'abonné qu'il convient d'obtenir le consentement pour pouvoir traiter des données à caractère personnel en vue de fournir un service donné à valeur ajoutée sera fonction des données à traiter et du type de service à fournir mais aussi de la possibilité ou non, sur les plans technique, procédural et contractuel, de distinguer le particulier qui utilise un service de communication électroniques de la personne, physique ou morale, qui s'y est abonnée ».

- *Détection des fraudes*

En vertu du paragraphe 4 de l'article 133, les données de communication peuvent être utilisées pour déceler les fraudes .
L'avant-projet ne précise pas ce qu'il faut entendre par fraude, ni qui a qualité pour traiter ces données.
La Commission souligne à cet égard que la directive européenne vise en son article 15, 1° les « utilisations non autorisées du système de communications électroniques ». Il s'agit donc d'une acceptation restreinte de la notion de fraude.
Par ailleurs, sur la base des précisions fournies par le paragraphe 5 développé supra, il faut considérer que seul l'opérateur, à l'exclusion de tiers, est habilité à traiter ces données.

- *Personnes habilitées à traiter les données de communication*

L'avant-projet de loi indique (article 133 paragraphe 5) que les données ne peuvent être traitées que par les personnes « *chargées* par l'opérateur de la facturation ou de la gestion du trafic (…) ».
La directive indique en son article 6 §5 que sont autorisées les personnes qui travaillent *sous l'autorité* de l'opérateur ou du tiers qui fournit les données de trafic et de localisation. Ce qui exclut en principe la transmission de ces données à d'éventuels sous-traitants chargés de la récupération de créances. L'exposé des motifs confirme cette interprétation, lorsqu'il mentionne les personnes habilitées à traiter ces données « au sein de la société de l'opérateur »[3].

b. En ce qui concerne les données de localisation (article 134)

En vertu de l'exposé des motifs, sont visées ici des données plus précises que les informations relatives au trafic qui sont nécessaires dans les réseaux numériques mobiles pour la transmission de communications.
La Commission réitère l'observation formulée sous « a » en ce qui concerne le défaut d'information des utilisateurs lorsque l'abonné est une personne morale.

c. En ce qui concerne la confidentialité des informations et données transmises par voie de télécommunication (articles 135 et 136)

- *Le principe (article 135) :*

Cet article vise à remplacer l'actuel article 109terD de la loi du 21 mars 1991 relative aux entreprises publiques économiques : il en reprend les dispositions, pour les adapter au prescrit de la directive européenne.
Il vise à protéger les communications (contenu et données de trafic) de toute prise de connaissance ou manipulation par une personne autre que les parties à la communication, sauf consentement de toutes les parties directement ou indirectement concernées.
La Commission remarque néanmoins que la terminologie employée n'est pas strictement conforme à celle du texte européen.
En particulier, le texte belge ne transpose pas l'interdiction de *stockage* des communications, prévue à l'article 5 de la directive européenne. Il limite l'interdiction aux accès *intentionnels* aux communications, alors que l'objectif de la directive européenne est d'empêcher « tout accès non autorisé aux communications » afin d'en protéger la confidentialité.

[3] On relève qu'à l'article 134 §4 de l'avant-projet, sont employés les termes « sous l'autorité de », alors que le texte néerlandais utilise la même terminologie dans les articles 133 et 134 : « in opdracht van » (sur ordre de, par ordre de). Il s'agit donc vraisemblablement d'une erreur de traduction, mais qui a des conséquences importantes quant à la signification des dispositions de fond du texte.

Enfin, pour lever l'interdiction d'accès, il exige le consentement, de façon plus étendue que le texte européen, de toutes les personnes directement *ou indirectement* concernées par la communication. Il serait souhaitable que cette notion soit définie, afin de clarifier le champ d'application du principe. On peut par exemple se demander si une personne mentionnée dans le contenu d'un message est *indirectement concernée* par la communication aux termes de la loi.

La Commission note enfin que l'article 5.1 de la directive demande que les Etats membres
1. garantissent la confidentialité des communications ;
2. interdisent les écoutes.

Si le point 2 est couvert par l'avant-projet de loi, le 1er point ne l'est pas.
La Commission s'interroge sur l'opportunité de prévoir la possibilité de prendre par arrêté royal pris après avis de la Commission des mesures réglementaires plus spécifiques en matière de confidentialité des communications, afin par exemple de prévoir une obligation de cryptage de certains messages ou de sécurisation de certains réseaux, lorsque l'absence de sécurité de ces réseaux crée des risques pour les utilisateurs[4].

- *Les exceptions (Article 136) :*

Le paragraphe 1er 1° permet à *toute loi* de déroger à la protection de la confidentialité des communications. Le législateur pouvant toujours déroger à des normes qu'il a lui-même antérieurement adoptées, cette dérogation n'a de sens qu'en ce qu'elle devrait être interprétée comme étant limitée conformément à l'article 15 de la directive européenne. Selon cet article, "ces lois doivent constituer « une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la *sécurité nationale* (…), la *défense et la sécurité publique* ou assurer la prévention, la recherche la détection et la poursuite d'*infractions pénales* ou d'utilisations non autorisées du système de communications électroniques ».

Le paragraphe 1er 2° garantit aux opérateurs la possibilité de traiter certaines données de communication, sans le consentement des personnes concernées, dans la mesure où ce traitement est nécessaire à la vérification du bon fonctionnement du réseau et à la bonne exécution d'un service de communications électroniques.
La Commission remarque à cet égard que, si le principe de l'article 136 (de même que l'actuel article 314bis du Code pénal) vise à garantir la confidentialité des communications, il doit ainsi être appliqué de façon compatible avec les principes garantissant la sécurité des réseaux, la prestation des services de communication et le contrôle de l'accès à certaines bases de données. L'interdiction de principe de prendre connaissance de données de communication ne peut dès lors empêcher l'opérateur d'accéder à certaines données (par exemple dans le cadre d'envois électroniques recommandés) dans la mesure où celles-ci sont nécessaires à l'exécution du service de communication qu'il offre au public.

Le paragraphe 1er 3°, 4°, 5 prévoit des exceptions complémentaires à l'intention des services de secours et d'urgence, de l'Institut Belge Postes et Télécommunications et du service de médiation. En ce qui concerne les services de secours et d'urgence, la directive européenne prévoit la possibilité pour ces services de passer outre à la suppression de la présentation du numéro appelant (c'est à dire de toujours pouvoir identifier ce numéro), mais cette exception ne s'étend pas à la prise de connaissance du contenu et des données de communication au sens large.
En ce qui concerne l'Institut Belge Postes et Télécommunications et le service de médiation, l'exception, conformément au prescrit de la directive européenne, doit être limitée aux utilisations non autorisées (« malveillantes » dans l'exposé des motifs de l'avant-projet de loi »).

[4] Voy. par exemple le rapport du Parlement européen du 11 juillet 2001 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON), A5-0264/2001 Final.

Le paragraphe 1er 6° autorise l'opérateur à utiliser des services de filtres contre les courriers non sollicités, uniquement sous condition de *l'autorisation* préalable (le texte n'utilise pas la notion de *consentement*) de l'utilisateur.
La Commission observe que la question s'est déjà posée de savoir si les opérateurs pouvaient se baser sur l'exception de « bon fonctionnement du réseau » déjà prévue au paragraphe 1er 2° de l'article 109terD de la loi actuelle, afin d'utiliser des filtres « anti-spam » sans le consentement des utilisateurs.
La Commission constate que la nouvelle disposition implique que l'opérateur ne peut en principe se baser sur cette exception de « bon fonctionnement du réseau », puisque l'obtention du consentement du *destinataire* est désormais explicitement requise avant l'utilisation de filtres par l'opérateur.
La Commission considère néanmoins qu'il s'agit d'opérer une distinction entre de simples courriers non sollicités et une attaque via envoi massif d'e-mails visant à provoquer la saturation d'un système ou d'un réseau. Dans ce dernier cas, l'opérateur devrait pouvoir prendre des mesures visant à assurer le bon fonctionnement du réseau, sans obtenir préalablement le consentement des utilisateurs.
La Commission constate par ailleurs que l'article en projet dispense l'opérateur de l'obtention du consentement de *l'expéditeur.*
La Commission rappelle que, en vertu du libellé de la directive européenne, le consentement devra être libre, spécifique et informé. S'il est donné dans le cadre de la souscription d'un service de communication, il devra donc être distinct de l'acceptation des conditions générales du service souscrit, et comporter des indications suffisamment précises sur les modalités du filtrage envisagé.

Les paragraphes 3 et 4 de l'article 136 prévoient l'obligation pour les opérateurs de participer à l'identification, au repérage, à la localisation, aux écoutes, à la prise de connaissance et à l'enregistrement des communications privées dans le cadre d'une instruction criminelle. Les modalités concrètes de cette participation doivent être fixées par arrêté royal[5].
La Commission rappelle qu'une exception protège les communications couvertes par le secret professionnel.
Elle rappelle également l'interdiction de principe de toute recherche proactive.
Enfin, elle souligne que les opérateurs doivent pouvoir refuser l'accès aux données de communication si la demande n'est pas suffisamment précise ou semble heurter le principe de proportionnalité. La demande du juge d'instruction devrait dans ce cas faire l'objet de vérifications complémentaires.

4. Conservation des données de communication, surveillance des communications

a. Enregistrement et conservation de certaines données de communication (article 137)

L'avant-projet de loi reprend le principe de l'enregistrement et de la conservation *a priori* de certaines données par les opérateurs. Ce principe figure déjà à l'article 109terE de la loi du 21 mars 1991 précitée, mais sous une formulation différente. La Commission note ainsi avec satisfaction que sont désormais seules mentionnées les données permettant l'identification des utilisateurs, et non plus l'ensemble des données d'appel.

Les finalités pouvant justifier l'enregistrement et la conservation de ces données sont la poursuite et la répression d'infractions pénales et la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques.

[5] Ces modalités sont actuellement fixées par un arrêté royal du 9 janvier 2003 portant exécution des articles 46bis, §2, alinéa 1er, 88bis, §2, alinéas 1er et 3, et 90quater, §2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109terE, §2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

La Commission juge nécessaire de préciser que les données peuvent être utilisées uniquement en vue des seules poursuite et répression d'infractions telles que prévues par l'article en projet. L'exposé des motifs devrait à cet égard préciser que toute autre utilisation serait punissable, compte tenu de sa finalité incompatible.

La Commission note encore que l'opérateur qui stocke les données pour le compte de l'Etat agit en tant que sous-traitant de celui-ci au sens de la loi. L'Etat est ici le responsable du traitement.

L'avant-projet de loi reprend le délai de conservation déjà prévu à l'article 109terE, et qui ne peut être inférieur à un an. Celui-ci sera fixé par arrêté royal.
La Commission rappelle les observations déjà formulées dans son avis 33/99 du 13 décembre 1999 et réitérées au niveau européen à plusieurs reprises par le groupe des commissaires européens à la protection des données[6], quant à la compatibilité d'une rétention a priori des données de communication avec les principes fondamentaux de protection des données à caractère personnel.

La Commission avait ainsi rappelé que « ni les textes internationaux (…), 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). »
La Commission se référait encore à la jurisprudence de la Cour européenne des droits de l'homme[7] « 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 ».

b. Identification de l'appelant, surveillance et écoute des communications privées (article 138)

L'article 109terE actuel de la loi du 21 mars 1991 laisse au Roi la possibilité d'interdire, partiellement ou entièrement, l'exploitation de services ou équipements qui rendent difficile ou impossible l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées dans les conditions prévues par le Code d'instruction criminelle.
Le paragraphe 2 de l'article en projet ne laisse plus cette possibilité au Roi : le type de services mentionné ci-dessus est interdit par principe, à l'exception des systèmes d'encryptage utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

La Commission constate que le libellé de l'article est particulièrement large en ce qu'il vise non seulement les services ou équipements qui rendent *impossible* l'identification, mais également ceux qui la *rendent difficile*.
Elle observe en outre que cette disposition a pour conséquence de limiter considérablement, sinon de supprimer, toute possibilité d'utiliser de façon anonyme les moyens de communication. L'exposé des motifs précise d'ailleurs que les cartes pré-payées, qui font l'objet de dispositions transitoires, sont également visées par le texte en projet.

---

[6] Recommandation 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 ; Avis 5/2002 du 11 octobre 2002 sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications : « *Lorsque des données de trafic doivent être conservées, [la] nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus. La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable*. »

[7] Arrêts Klass (arrêt du 6 septembre 1978, Publ. Cour, Série A, n° 28, p. 23 et s) et Malone (cité).

La Commission s'interroge sur l'application du principe aux terminaux publics de communication, tels que les cabines téléphoniques.
Elle rappelle les observations déjà formulées dans son avis 33/99 cité supra, et les dispositions internationales sur le sujet, notamment 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.

5. Enregistrement de données relatives à des transactions commerciales (article 139)

Cet article transpose l'article 5 §2 de la directive. Il permet l'enregistrement de communications et de données de communication dans le cadre de transactions commerciales licites, afin d'apporter la preuve d'une transaction commerciale ou d'une communication professionnelle (N.B. la directive européenne utilise le terme de communication *commerciale*, ce qui est plus restrictif).

La Commission considère cette disposition comme bienvenue, compte tenu des impératifs existant dans certains secteurs, notamment bancaire. Elle rappelle à cet égard les conclusions de sa recommandation 1/2002 du 22 août 2002 sur l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, selon lesquelles, outre une information précise des personnes concernées, *il importe que des terminaux de communication non soumis à écoute ou enregistrement leur soient accessibles*.

Ce principe devrait également être mis en œuvre dans le cadre des call centers, et de façon plus générale pour l'ensemble des entreprises offrant des transactions commerciales via le réseau de communication.

6. Protection de l'abonné ou utilisateur contre les cookies et autres fichiers ou logiciels espions (article 140)

L'objectif de cette mesure est de conditionner le stockage de données sur le terminal de l'abonné ou de l'utilisateur à son information préalable ; l'intéressé doit également se voir offrir la faculté de refuser le stockage des données.
Cette disposition explicite les principes de la loi du 8 décembre 1992 relative à la protection de la vie privée, qui prévoit déjà une information préalable et un droit d'opposition en faveur de la personne concernée en cas de traitement de ses données à caractère personnel.
Mais alors que ce droit d'opposition doit en vertu de la loi du 8 décembre 1992 être conditionné par des raisons sérieuses et légitimes, le texte en projet, sur le modèle de la directive européenne, ne prévoit pas de conditions additionnelles.

La Commission observe toutefois que l'alinéa 2 de l'article 140 peut être considéré comme vidant le principe de protection de tout sons sens lorsqu'il est interprété à la lumière de l'exposé des motifs: celui-ci précise que l'accès à certains sites web peut être subordonné à l'acceptation d'un cookie si celui-ci est utilisé à des fins légitimes. Supprimer la possibilité de refuser un cookie dans une telle hypothèse revient à donner à l'exception une étendue aussi large que le principe lui-même.
La Commission considère dès lors que devrait être supprimé, dans l'exposé des motifs, l'avant dernier paragraphe commentant l'article 140.

7. Identification de l'appelant et de l'appelé (article 141), renvoi automatique des appels (article 142)

- *Identification de l'appelant (article 141) :*

Le paragraphe 1er règle les conditions auxquelles l'appelant et l'appelé peuvent dans différents contextes décider de la présentation ou de la suppression de la présentation du numéro appelant ou appelé.

La Commission note que le paragraphe 3 prévoit un moyen de refuser les appels entrants non identifiés, mais sur demande, alors que la directive européenne précise qu'il doit s'agit d'un *moyen* simple (en principe technique) et *gratuit*.

- *Renvoi automatique des appels (article 142) :*

La Commission n'a pas d'observations à formuler sur cette disposition.

8. Conditions de collecte et de publication des données relatives aux abonnés dans les annuaires (article 143)

L'article 143 précise en particulier les informations à fournir aux abonnés dont les données seront reprises dans un annuaire. Il consacre enfin la gratuité de la non-inscription dans l'annuaire, et prévoit en outre l'obligation pour l'opérateur de demander le consentement distinct de l'abonné dans certains cas où les données pourront faire l'objet de recherches inversées.
La Commission relève néanmoins que selon le libellé du paragraphe 1 3 , la protection en cas de recherche inversée semble être limitée à la recherche sur la base du numéro de téléphone : en cas de recherche sur base géographique, le consentement ne semble pas requis, ce que la Commission déplore.

La Commission prend enfin acte des mesures transitoires (article 174) prévues en ce qui concerne les données à caractère personnel des abonnés qui ont été insérées dans un annuaire avant l'entrée en vigueur des dispositions ici analysées. Ces mesures visent à fournir aux personnes concernées une information détaillée sur les objectifs et les possibilités d'utilisation de l'annuaire, et un droit d'opposition à ces utilisations.
La Commission a pu constater que les abonnés ne sont pas, à l'heure actuelle, informés des diverses utilisations des coordonnées qu'ils ont communiquées à leur opérateur, et de leur mise à disposition notamment sur CDrom ou sur l'Internet. L'article 174 en projet vient sanctionner la demande déjà formulée par le passé par la Commission[8] de voir les abonnés informés de façon explicite et spécifique de ces diverses utilisations. Le contenu de ces supports d'information devrait être modifié à la première mise à jour de ces derniers et immédiatement lorsqu'il y a diffusion sur l'Internet.

[8] Recommandation 1/99 du 23 juin 1999 relative à l'utilisation des données contenues dans les annuaires téléphoniques.

PAR CES MOTIFS,

, La Commission émet un avis favorable, sous réserve des observations formulées dans le présent avis, et qui concernent en particulier :

- La procédure d'identification des numéros de téléphone confidentiels n'apparaissant pas sur les factures, et les modalités d'information du public ;
- La clarification du champ d'application de l'avant-projet de loi aux fournisseurs de services de communication électronique ;
- L'application du principe de nécessité au traitement des données de télécommunication par les opérateurs ;
- Les conditions de protection des utilisateurs lorsque l'abonné est une personne morale ;
- L'acceptation restreinte des conditions auxquelles les opérateurs peuvent traiter les données de communication en cas de marketing et de détection des fraudes ;
- La conformité du principe de confidentialité des communications, et des exceptions à ce principe, avec le libellé de la directive européenne ;
- La compatibilité du principe de rétention a priori des données de télécommunication avec les principes fondamentaux de protection des données à caractère personnel ;
- La question de l'utilisation anonyme des moyens de communication ;
- Les garanties devant entourer l'enregistrement de transactions commerciales ou les communications des call centers ;
- La portée du principe de protection de l'utilisateur contre les cookies et autres spywares ;
- Les conditions d'utilisation des données figurant dans les annuaires dans le cadre de recherches inversées sur un critère autre que le numéro de téléphone ; les mesures transitoires visant à informer les personnes dont les données figurent déjà dans un annuaire.

Le secrétaire, Le président,

(sé) J. BARET (sé) P. THOMAS