

Loi portant réforme de certaines entreprises publiques économiques :

Chapitre Xbis : Secret des communications et protection de la vie privée

21 mars 1991

A retenir :

Le présent commentaire se concentre sur quelques dispositions importantes qui protègent le secret des télécommunications. Il s'agit de règles qui ont été inscrites dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (la 'loi Belgacom').

La loi Belgacom emprunte son nom au fait que cette loi avait aussi - et même essentiellement - l'intention de régir le statut notamment de Belgacom et de son personnel. De plus, la loi contient les règles de base en matière de télécommunication, dont la partie de la loi que nous commentons ici, à savoir le secret des télécommunications. Ce volet ne constitue qu'une petite partie de la loi. Il s'agit plus particulièrement du chapitre 10bis du titre III, intitulé « Secret des communications et protection de la vie privée ».

L'article central de ce chapitre est l'article 109terD, qui interdit notamment de prendre connaissance de l'existence de communications d'autres personnes sans l'autorisation préalable de toutes les parties à la communication.

Mots-clés :

Télécommunications – Libertés fondamentales – Vie Privée – Secret de Télécommunications

Table des matières :

A. Introduction

- Historique de la loi Belgacom
- Protection de la vie privée
- Fondement et intention
- Délimitation

B. La prise de connaissance de l'existence de communications en provenance d'autres personnes

- Article 109terD, 1°
- Article 109terD, 3°

C. Usage et annulation des données de télécommunication relatives à une autre personne

- Article 109terD, 2°
- Article 109terD, 4°

D. Exceptions

- Autorisation légale

- Nécessité
 - Recherche et localisation
 - Cryptographie
- E. [Pour en savoir plus](#)
- Liens utiles
 - Doctrine

Commentaire :

A. Introduction

La Belgique jouit d'une riche tradition juridique dans le domaine de la protection de la vie privée. Dans la première version de la Constitution déjà, étaient inscrites des garanties qui visaient à protéger la vie privée du citoyen¹. L'une des principales dispositions était la protection du secret des lettres², avec sa sanction pénale³. Cette réglementation est nécessaire pour la sauvegarde des libertés et droits fondamentaux et de l'Etat de droit démocratique en général.

Il va de soi que ces garanties doivent évoluer avec l'état de la technique. Il est donc logique que cette protection se soit étendue progressivement à la télégraphie et à la téléphonie (le secret du téléphone) et, dans des années plus récentes, à la télécommunication en général. Le présent commentaire se concentre donc sur quelques dispositions importantes qui protègent le secret des télécommunications, à savoir les règles qui ont été inscrites dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques⁴ (la 'loi Belgacom').

La loi Belgacom emprunte son nom au fait que cette loi avait aussi - et même essentiellement - l'intention de régir le statut notamment de Belgacom et de son personnel. De plus, la loi contient les règles de base en matière de télécommunication, dont la partie de la loi que nous commentons ici, à savoir le secret des télécommunications. Ce volet ne constitue qu'une petite partie de la loi. Il s'agit plus particulièrement du chapitre 10bis du titre III, intitulé « Secret des communications et protection de la vie privée », comportant les art. 109terC à 109terF. Il ressort de la numérotation que cette matière a été modifiée au fil des ans. Nous approfondirons quelque peu cette évolution plus loin dans ce commentaire.

L'une des premières lois⁵ sur la protection du secret des télécommunications est la loi du 13 octobre 1930 coordonnant les diverses dispositions légales sur la télégraphie et la téléphonie par fil⁶. Ainsi que le nom le suggère, cette loi ne pouvait être appliquée à la communication sans fil. Cette lacune a été comblée plus tard par l'art. 4c de la loi du 30 juillet 1979 relative aux radiocommunications⁷ qui interdisait notamment de capter des radiocommunications qui n'étaient pas destinées au récepteur.

L'année 1991 a vu naître la première version de la loi Belgacom, quoique dans une toute autre forme que celle d'aujourd'hui. Au départ, la réglementation qu'elle mettait en place pour la télécommunication en Belgique n'était pas beaucoup plus qu'une copie carbone des dispositions de la loi RTT de 1930. Plus tard, plusieurs modifications importantes ont toutefois été apportées, dont les principales en 1994⁸ (par la loi sur les écoutes téléphoniques), en 1997⁹ (qui lui a donné sa numérotation actuelle), en 1999¹⁰ (pour une adaptation à la directive ISDN) et, enfin, en 2000 (par la loi sur la Criminalité informatique¹¹).

Naturellement, nous n'avons pas l'intention d'analyser toutes ces adaptations en détail. Le présent commentaire vise surtout à parcourir les grandes lignes de la protection de la vie privée dans la loi Belgacom et indiquer de quelle façon ces dispositions sont particulièrement importantes dans la société de l'information moderne¹².

Nous analysons donc en premier lieu avec précision le contenu et la portée des principales dispositions, avec quelques exemples concrets pour démontrer le large champ d'application de ces règles.

B. La prise de connaissance de l'existence de communications en provenance d'autres personnes

La signification fondamentale du secret des télécommunications est le fait que le contenu et même l'existence d'un échange spécifique d'informations entre deux personnes doit pouvoir rester secret. La protection du contenu est l'aspect le plus évident : personne n'apprécierait, en effet, qu'un tiers écoute une communication téléphonique sans autorisation préalable, par exemple. Cet aspect n'est toutefois pas abordé dans la loi Belgacom, mais est réglé, depuis l'introduction de la loi sur les écoutes téléphoniques¹³, par deux articles spécifiques du Code pénal (articles 259bis et 314bis C. pén.). Nous ne nous y attarderons donc pas.

La loi Belgacom règle uniquement le deuxième aspect, à savoir la prise de connaissance frauduleuse de l'existence de télécommunications. Le fait que ces deux aspects soient sanctionnés dans deux lois distinctes est souvent critiqué par la doctrine. En effet, il n'est pas possible de prendre connaissance du contenu de certaines communications, sans avoir aussi connaissance de leur existence. L'inverse est naturellement possible. Cependant, l'existence d'une règle simple dans une loi spécifique unique clarifierait la législation.

La prise de connaissance de l'existence de communications en provenance d'autres personnes est réglée dans deux points distincts de l'article 109terD, à savoir les points 1 et 3. Pour ces deux points, la prise de connaissance n'est punissable que si elle se produit sans l'autorisation de toutes les parties à la communication. C'est tout à fait logique, car l'intention du législateur est de garantir la vie privée des parties participant à la communication.

Nous allons quelque peu approfondir ces deux points.

- Article 109terD, 1° : [il est interdit] «de prendre frauduleusement connaissance de l'existence (...) de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci ».

La première pénalisation porte sur l'enregistrement de la communication d'autres personnes et donc pas sur la prise de connaissance du contenu, comme nous l'avons déjà indiqué précédemment. On ne peut donc en aucun cas confondre l'enregistrement dans cette article avec l'enregistrement du contenu d'une communication spécifique.

L'objet de la télécommunication à laquelle cette disposition est applicable, est décrit comme les 'signes, signaux, écrits, images, sons ou données de toute nature'. L'objet est ainsi défini de manière très large, surtout avec la catégorie restante « données de

toute nature ». Il devient clair d'emblée que presque toute télécommunication peut être enregistrée.

Le terme « télécommunications » doit également être interprété d'une façon large, et est défini dans l'article 68, 4° de la loi Belgacom comme 'toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radioélectricité, signalisation optique ou un autre système électromagnétique'. Ceci ne couvre donc pas seulement la téléphonie et la télégraphie, mais aussi les formes de communication un peu plus moderne, comme le courriel, le web, le chat, le *home shopping*, le *télébanking*, les logiciels *peer-to-peer*...

Cependant, deux restrictions sont prévues à cet égard. En premier lieu, il est seulement punissable d'enregistrer une télécommunication en provenance d'autres personnes et destinées à celles-ci. Il doit donc s'agir d'une communication entre au moins deux personnes, où la partie qui enregistre ne participe pas à la communication. Un participant peut donc enregistrer lui-même l'existence de sa propre communication de quelque manière que ce soit et chacun peut enregistrer des données de communication qui sont mises sur les ondes sans destinataire spécifique.

On en trouve un exemple dans l'envoi d'un message à un groupe de discussion accessible au public. Ce type de message n'est pas adressé à un utilisateur déterminé et le procédé choisi par « l'émetteur » indique déjà implicitement qu'il n'attache aucune importance à la confidentialité du message. Il est accessible à tous et son enregistrement par des tiers est donc autorisé. C'est pour cette raison que les émissions radiophoniques et télévisuelles ne relèvent pas non plus du champ d'application de cette loi.

La deuxième restriction se trouve dans la condition d'une intention frauduleuse dans le chef du contrevenant. L'auteur de l'enregistrement doit avoir eu l'intention de violer le secret des télécommunications par ses agissements. Lorsqu'on prend connaissance par inadvertance de l'existence de télécommunications d'autres personnes, cela ne suffit pas.

Un exemple est le contrôle de son courrier électronique sur une adresse partagée par une famille, lors duquel on peut voir le titre et l'expéditeur des e-mails des autres membres de la famille. Il est vrai que l'on prend connaissance ainsi de l'existence de leurs télécommunications, mais si cela ne se produit pas dans l'intention de violer leur vie privée, il ne peut y avoir de pénalité.

- Article 109terD, 3° : [il est interdit] «de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne, ceci sans préjudice des dispositions de l'article 105nonies, § 5, de la présente loi ».

La deuxième pénalisation ressemble fort, de prime abord, à la première. Il s'agit une fois encore de la prise de connaissance de données en matière de télécommunication, où la télécommunication présente un large contenu identique à celui de l'art.109terD, 1°. Cependant, on notera une différence importante, qui consiste surtout en l'applicabilité aux 'données en matière de télécommunication' (contrairement aux 'signes, signaux, écrits, images, sons ou données de toute nature transmis par voie de télécommunications' du point 1°).

Il subsiste une controverse quant à la portée précise de ce terme. Les travaux préparatoires donnent toutefois une définition concrète : il s'agit de données « qui concernent une personne qui fait usage de services pour la télécommunication. Ces données sont toutefois limitées à la partie qui relève de la télécommunication : les télécommunications, la nature et le lieu des installations de télécommunication, un numéro de téléphone secret, etc., de cette personne, mais pas les données généralement connues, comme le nom, le domicile, etc. »¹⁴.

L'article 109terD, 1° concerne donc la prise de connaissance de l'existence de n'importe quelle donnée indiquant une télécommunication, tandis que l'art. 109terD, 3° concerne la prise de connaissance de données plutôt techniques sur la télécommunication.

En ce qui concerne l'internet, on peut penser au moment où l'on se connecte à un système déterminé, aux adresses IP des systèmes en communication, aux sites éventuellement visités, au trajet qu'un paquet de données a suivi pour atteindre sa destination finale, etc.

Des données comme les noms d'utilisateur et les mots de passe ne semblent pas être visées. Elles ne comportent, en effet, aucune information sur l'existence et l'usage de la télécommunication à un moment déterminé¹⁵, mais uniquement des informations générales indiquant le fait qu'une communication est possible entre deux parties. La prise de connaissance d'un nom de login ou d'un mot de passe ne constitue donc pas en soi une violation du secret des télécommunications, ni davantage la connaissance du contenu du répertoire téléphonique d'une autre personne. Toutes deux ne permettent, en effet, que de constater qu'une communication est possible entre deux personnes¹⁶.

Une réglementation peu transparente qui permet difficilement de déterminer ce qui relève du point 1° ou 3°. Cependant, la distinction est d'une grande importance, vu la différence des éléments entre les deux.

La principale différence réside peut-être dans le fait que l'article 109terD, 3° contrairement à l'article 109terD, 1° n'impose aucune intention spéciale, l'intention générale étant suffisante. Toute prise de connaissance intentionnelle de données d'une autre personne en matière de télécommunication est donc punissable, même si l'on n'a pas l'intention de violer la vie privée de l'autre personne.

Une deuxième différence importante entre les deux est que le troisième alinéa contient une exception à la disposition de l'art. 105nonies §5 concernant la facturation par des opérateurs télécom. Nous n'approfondirons pas cette exception.

- C. Usage et annulation des données de télécommunication relatives à une autre personne
- Outre la prise de connaissance des données, certaines formes d'usage de ces données sont interdites. A cet égard, l'objet principal est la protection de l'intégrité des données de télécommunication, notamment en interdisant leur modification et leur annulation.
- Article 109terD, 2° : [il est interdit] « de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes ».

La première disposition prohibitive apparaît d'emblée comme la plus évidente : les données qui démontrent l'existence d'une communication spécifique ne peuvent être modifiées ou supprimées et les participants à la communication ne peuvent être identifiés.

L'interdiction de modification et d'omission de données est une mesure qui vise surtout à garantir l'intégrité de ces données, notamment pour permettre une facturation correcte. En tant que telle, il ne s'agit donc pas d'une mesure de protection de la vie privée.

Par contre, l'interdiction d'identification des personnes l'est bien. On peut même se poser la question de savoir si cette disposition est bien nécessaire. L'identification d'une personne à l'aide de ses données de télécommunication sans son autorisation préalable constituera aussi généralement, en effet, un traitement frauduleux de ses données à caractère personnel. Même sans une disposition distincte dans la loi Belgacom, cela est punissable¹⁷.

Une fois encore, une intention frauduleuse est nécessaire et il n'est question de pénalité que lorsque les données ont été annulées ou supprimées dans l'intention de porter atteinte à leur intégrité ou, lorsque l'identification est intervenue, dans l'intention de violer la vie privée.

Si un gestionnaire de réseau, par exemple, vérifie l'identité de toutes les personnes qui ont téléchargé un fichier déterminé de son site web pour les avertir que ce fichier contient un virus, il ne serait pas question de pénalité au titre de ce point de l'article. L'identification ne se fait pas, en effet, dans le but de violer la vie privée d'une autre personne.

Enfin, l'interdiction ne s'applique que lorsqu'on utilise un « procédé technique ». L'annulation purement manuelle (par exemple, déchirer une facture en papier) ne suffit donc pas.

- Article 109terD, 4° : [il est interdit] « de révéler ou de faire un usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3°, de les modifier ou de les annuler ».

L'interdiction du quatrième alinéa, enfin, porte sur l'information, l'identification et les données mentionnées dans les premier, deuxième ou troisième alinéas. Le délit consiste à abuser de ces données d'une certaine façon. Il est important de noter qu'il n'est pas nécessaire d'être coupable de l'un des délits visés plus haut; il suffit que l'objet du délit soit décrit aux points 1°, 2° ou 3°.

Une première forme d'abus possible consiste à révéler ces données. Cela est conforme à la ratio legis : l'article 109terD vise à protéger le secret des télécommunications et il va de soi que la révélation de données sur la communication d'une autre personne sans son autorisation est constitutive d'une atteinte.

Un deuxième abus que l'on peut faire de ces données consiste en leur usage quelconque. Cela est problématique parce qu'aucune autre condition n'est posée : il n'est spécifié nulle part qu'il faille une intention spéciale ou que l'un des délits des

points 1° - 3° ait été effectivement commis. Ce problème peut être esquissé à l'aide d'un exemple simple.

Dans la plupart des navigateurs d'Internet, des données sur les sites web précédemment visités restent conservées même après la fermeture du programme, de sorte que l'utilisateur peut retrouver ces pages rapidement.

Supposez à présent qu'une personne utilise un ordinateur qui est aussi utilisé par plusieurs autres personnes pour accéder à l'internet, par ex., dans une bibliothèque, et qu'elle essaie, à l'aide de la fonction 'historique', de retrouver les sites où elle s'est rendue précédemment. Inévitablement, elle obtiendra des informations sur tous les sites récemment visités, même sur ceux qui ont été visités par d'autres personnes. Il s'agit indiscutablement d'informations telles que visées à l'alinéa 1 (toute donnée indiquant une télécommunication) et probablement aussi à l'alinéa 3 (données plutôt techniques sur la télécommunication). Pourtant, aucun des deux délits n'a été commis, car ils nécessitent respectivement une intention spéciale et générale.

Si l'on voit, dans cette hypothèse, qu'une autre personne a visité un site web qui pourrait être intéressant pour notre propre centre d'intérêt et que l'on utilise ces données (par ex., en cliquant sur le lien affiché et en arrivant ainsi sur le site web visité par une autre personne), l'on commet alors le délit visé au point 4°. Cependant, l'on n'est pas coupable de l'un des délits des points 1°-3°. C'est là que réside l'importance de la référence 'à l'information, l'identification et les données visées aux points 1°, 2° et 3°', au lieu de 'l'information, l'identification et les données obtenues par l'un des délits visés aux points 1°, 2° ou 3°'. Une nuance importante!

Un troisième abus, enfin, consiste en la modification de l'information, de l'identification et des données visées aux points 1°, 2° et 3°, en ce compris leur annulation.

Pour reprendre l'exemple du navigateur : une mémoire *cache* avec les données des sites les plus récemment visités n'est pas conservée éternellement. La plupart des navigateurs permettent de paramétrer un nombre de jours après lesquels cette mémoire est vidée. Cependant, l'on peut supprimer soi-même ces données. Si l'on utilise cette fonction intentionnellement pour supprimer des données de télécommunication d'une autre personne, l'on se rend coupable du délit visé à l'article 109terD, 4°.

D. Exceptions

La violation de l'une des dispositions de l'article 109terD est réglée à l'article 114 §2 : « Est punie d'une amende de 50 à 50 000 francs, la personne qui enfreint les articles (...) 109ter D (...). ».

Après conversion en Euro et multiplication par les décimes additionnels judiciaires, cela donne entre 250 et 250.000 €¹⁸.

L'article 109terE énumère toutefois plusieurs exceptions aux dispositions prohibitives, que nous parcourons brièvement ici.

- Autorisation légale :
L'article 109terE, 1° comporte une exception évidente : il n'est pas question de violation du secret des télécommunications « lorsque la loi permet ou impose l'accomplissement des actes visés ». Cela va de soi : la loi Belgacom a valeur

de loi la plus générale, à laquelle des lois plus spécifiques peuvent prévoir des exceptions¹⁹.

- Nécessité :

La deuxième exception (article 109terE, 2°) concerne l'hypothèse où l'infraction est nécessaire pour « vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de télécommunications ». Bien que cette exception ait fait l'objet d'une controverse²⁰, il ressort des travaux parlementaires que cette excuse absolutoire ne concerne que les personnes qui agissent dans l'exécution de leur tâche « à l'I.B.P.T., à Belgacom ou chez d'autres fournisseurs de services de télécommunication »²¹. Un hacker qui entre par effraction dans un système informatique et enfreint ainsi l'article 109terD, ne peut donc invoquer cette exception en argumentant qu'il voulait uniquement vérifier si le réseau était suffisamment protégé.

L'exception de l'article 109terE, 3° présente un contexte comparable : les infractions sont également admises « lorsque les actes sont posés en vue de permettre l'intervention des services de Secours et d'Urgence en réponse aux demandes d'aide qui leur sont adressées ». La nécessité de l'infraction résulte ici du caractère urgent de la situation : lorsque des services d'urgence reçoivent une demande d'aide urgente, ils doivent pouvoir vérifier rapidement l'origine de l'appel, sans se soucier d'un risque de pénalité éventuelle.

- Recherche et localisation

Enfin, il est également possible, dans le cadre d'enquêtes pénales, de procéder à l'enregistrement de télécommunications suspectes²². Sur la base des articles 109terE, §2 et suivants, le Roi peut fixer les modalités précises de cet enregistrement. Il peut notamment déterminer les moyens techniques avec lesquels les opérateurs de réseaux de télécommunication et les fournisseurs de services de télécommunication doivent veiller à l'enregistrement, ainsi qu'à la confidentialité et l'intégrité des données en résultant.

Les opérateurs télécom ont également une obligation générale d'enregistrer et de conserver pendant un délai déterminé les données d'appel et d'identification des utilisateurs des services de télécommunication. Le but de cette obligation est de simplifier la recherche et la poursuite de certains faits punissables. La période de cette obligation n'a pas encore été fixée, mais comme la loi stipule que le délai doit être d'au moins 12 mois, la plupart des opérateurs s'y tiennent dans la pratique.

- Cryptographie

La cryptographie est le terme désignant tout procédé pouvant être utilisé pour rendre illisible en principe le contenu d'un message déterminé. La cryptographie est considérée – surtout sur l'internet – comme un instrument fondamental pour protéger la vie privée. Sur l'internet, les utilisateurs font d'ailleurs fréquemment usage de la cryptographie, bien que la plupart des internautes n'en soient souvent pas conscients²³.

Les télécommunications numériques se prêtent par excellence à l'utilisation de la cryptographie. Il existe donc d'innombrables méthodes (les algorithmes) pour crypter des données, qui sont d'une complexité variable. Des algorithmes

suffisamment complexes peuvent rendre presque impossible le décryptage d'un message.

C'est pour cette raison que de nombreux gouvernements imposent une limite à l'utilisation d'algorithmes de cryptographie. Des algorithmes puissants pourraient, en effet, être également utilisés par des criminels ou des terroristes pour planifier leurs délits dans le secret²⁴. Pour permettre malgré tout un contrôle efficient par les pouvoirs publics, l'utilisation d'algorithmes de cryptographie peut être limitée par la loi²⁵.

La réglementation belge est souple sur ce plan : selon l'article 109terF de la loi Belgacom, l'utilisation du cryptage est libre²⁶.

Le Roi peut néanmoins désigner certains services de cryptographie qui ne peuvent être proposés au grand public sans déclaration préalable à l'I.B.P.T. Jusqu'à présent, il n'a pas encore été fait usage de cette possibilité, de sorte que l'utilisation et la diffusion de la cryptographie en Belgique reste provisoirement entièrement libre.

E. Pour en savoir plus

- Liens utiles
 - [Page d'information sur la cryptographie de PISA \(Providing Information about Internet Security Aspects\)](#)
 - [La Commission de la Protection de la vie privée](#)
- Doctrine
 - ARNOU, L., « Het respecteren van het telefoongeheim in België na de afluisterwet van 30 juni 1994 », *Computerr.* 1995/4, 156
 - BENSOUSSAN, A., *Les télécommunications et le droit*, Paris, Hermès, 1992
 - DEBBASCH, CH., ISAR, H. en AGOSTINELLI, X., *Droit de la communication*, Paris, Dalloz, 2002
 - DE SCHUTTER, B., « Het Belgisch Bistel-syndroom », *Computerr.*, 1999/3, p.164
 - DUMORTIER, J., *Informatica –en telecommunicatierecht*, Leuven, ACCO, 2001
 - DUMORTIER, J., « Little Brother is watching you : mag de werkgever het internetgebruik van zijn werknemers controleren », in *Liber Amicorum Roger Blanpain*, Brugge, Die Keure, 1998
 - DUMORTIER, J. en LAMBERT, P., « De wet van 19 december 1997 tot uitvoering van de Europese liberaliseringsrichtlijnen in het Belgisch telecommunicatierecht : een overzicht », *Computerr.* 1998/2, 47-55
 - DUPONT, L. en VERSTRAETEN, R., *Handboek Belgisch strafrecht*, Leuven, Acco, 1990, nr. 692 jo 695
 - LAMBERT, P., *Bescherming van (privé-)telecommunicatie*, in *Recente ontwikkelingen in informatica- en telecommunicatierecht*, ICRI, Brugge, Die Keure, 1999, p.183

¹ On peut songer p.ex. à l’inviolabilité du domicile (la présente article 15 de la Constitution).

² Le présent article 29 de la Constitution

³ L’article 460 C.Pén.

⁴ Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.* 27 mars 1991, 6155.

⁵ Des régulations antérieures peuvent être retrouvées dans une circulaire ministérielle du 17 août 1923 qui permettait l’enregistrement de télécommunications à quelques conditions spécifiques.

⁶ Articles 17-20 de la loi du 13 octobre 1930 coordonnant les diverses dispositions légales sur la télégraphie et la téléphonie par fil, *M.B.* 20 octobre 1930.

⁷ Article 4c de la loi du 30 juillet 1979 relative aux radiocommunications, *M.B.* 30 août 1979.

⁸ 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, *M.B.* 24 janvier 1995, 1542.

⁹ Article 77 de la loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d’adapter le cadre réglementaire aux obligations en matière de libre concurrence et d’harmonisation sur le marché des télécommunications découlant des décisions de l’Union européenne, *M.B.*, 30 décembre 1997, 34986.

¹⁰ Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (Directive ISDN), *JOCE*. L 024, 30 janvier 1998, p.1-8.

¹¹ Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.* 3 février 2001, 2909.

¹² Cette attention pour les applications dans la société de l’information est également la raison pour laquelle nous ne commenterons pas l’article 109terC ici. Cet article a en effet trait à la réglementation des données dans les annuaires de téléphone. Bien que les intentions de cet article puissent certainement être utiles dans un contexte plus étendu, son champ d’application ne dépasse pas les annuaires.

¹³ 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, *M.B.* 24 janvier 1995, 1542.

¹⁴ *Doc. Parl. Chambre*, 1990-91, nr. 1287/1 – 89/90, p. 67.

¹⁵ Voyez Kindt, E. et Szafran, E. dans leur note sous [le jugement RedAttack](#). Corr. Gand, 11 décembre 2000, *Computerr.* 2001/2, p. 87.

¹⁶ Dans [le jugement RedAttack](#) la conclusion finale était pourtant différente. Dans ce cas fameux le juge estimait que le vol des noms de login ou des mots de passe constituait bel et bien une prise de connaissance frauduleuse de données en matière de télécommunications.

¹⁷ Pour de plus amples informations, nous renvoyons à [la loi relative au traitement de données à caractère personnel](#).

¹⁸ Pour être complet, il faut encore remarquer que l’ampleur de la sanction est disputée. En effet, l’article 114 §7 stipule :

« § 7. Est punie d’une amende de 100 à 5 000 francs et d’un emprisonnement de trois mois à un an ou d’une de ces peines seulement, la personne qui, personnellement ou par l’entremise d’une autre personne, sous réserve de l’application de l’article 109terE, viole des dispositions de l’article 109terC. »

Cependant, l’article 109terE a trait aux exceptions de l’article 109terD, et n’a rien à voir avec l’article 109terC, ce qui paraît pourtant être impliqué dans l’article 114 §7.

¹⁹ Conformément à l’adage latin : *lex specialis derogat legi generali*.

²⁰ Cet argument était notamment invoqué dans [le cas RedAttack](#), où un hacker se défendait entre autres par l’argument qu’il ne voulait que vérifier le bon fonctionnement du système.

²¹ *Doc.Parl.Chambre*, 1990-91, nr. 1287/1 – 89/90, p. 68

²² A la vérité, ceci n’est pas possible que dans un nombre de cas très limité, à cause du caractère fort discutable de la mesure. Les cas où l’enregistrement de télécommunications serait acceptable sont fixés dans les articles 88bis et 90ter à 90decies du Code Judiciaire pénal.

²³ On peut notamment songer à l'usage du protocole SSL (Secure Socket Layer).

²⁴ Les critiques remarquent que rien n'attire l'attention comme un message excessivement crypté, et que l'usage de tels algorithmes ne bénéficie pas la discrétion.

²⁵ Ceci est entre autres le cas dans les Etats-Unis, où la cryptographie est bien permise, mais où l'exportation des algorithmes de cryptographie est fort réglementée. Pour plus amples informations nous renvoyons à [la page d'information de la U.S. Department of Justice](#).

²⁶ Cette attitude flexible est une conséquence de la loi du 19 décembre 1997 qui libérait tout à fait la livraison et l'usage de cryptographie en Belgique (Loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, *M.B.*, 30 décembre 1997, 34986). Auparavant, le Ministre de Télécommunications pouvait interdire la distribution de certains équipements cryptographiques.