



LE DROIT DE L'INFORMATIQUE, DES
RESEAUX ET DES TECHNOLOGIES DE
L'INFORMATION ET DE LA
COMMUNICATION

JANVIER 2004

Sommaire

L'opposabilité des conditions générales d'utilisation d'un site Internet -22/01/2004	2
Le Wi-fi, enjeux juridiques -18/01/2004	4
La prospection par messagerie électronique : le projet de LCEN au 24 décembre 2003 -10/01/2004.....	7
La responsabilité du prestataire de services en matière de solutions de sécurité informatique -06/01/2004.....	13

Commerce électronique, Droit de la consommation, protection du consommateur

L'opposabilité des conditions générales d'utilisation d'un site Internet -22/01/2004

Par Webconseil, Société de conseil.

Les conditions générales d'utilisation (CGU) d'un site Internet revêtent une réelle importance, tant pour les responsables de sites Internet que pour les utilisateurs. Elles permettent, en effet, de porter à la connaissance de ces derniers les droits et obligations de chacune des parties concernant l'utilisation du site, des services qu'il offre, et des données qu'il contient.

► La valeur des CGU ne repose cependant pas seulement sur le niveau de clarté et de précision de leur rédaction, mais également sur leur opposabilité, ce dernier critère ressortant notamment de la visibilité des CGU sur le Site, et donc de la possibilité pour les utilisateurs d'en prendre connaissance.

Les CGU contribuent ainsi à la sécurisation de la relation avec les utilisateurs, ainsi qu'à la protection des éléments constitutifs du Site. Les CGU permettent ainsi de légitimer a priori toute action future du responsable du site contre un utilisateur qui agirait en violation de celles-ci.

La jurisprudence n'impose pas en effet une acceptation expresse en matière de CGU, contrairement au cas des Conditions Générales de Vente.

Elle exige toutefois que les Conditions Générales d'Utilisation soient largement visibles sur le site et facilement accessibles, à tout moment de la visite sur le site, étant précisé que ces conditions de visibilité et d'accessibilité peuvent être interprétées de façon plus ou moins rigoureuses.

Ainsi, un tribunal de Rotterdam, dans un jugement rendu en décembre 2002, a en effet jugé que les CGU d'un site, accessibles seulement depuis la page d'accueil sous un hyperlien « CONDITIONS », demeureraient opposables à un utilisateur professionnel, alors même que ce dernier ne les avait pas expressément

acceptées. Les juges ont considéré que ce professionnel devait savoir que, sous ce lien, figuraient les CGU. Dans cette affaire, il s'agissait d'une relation qualifiée de B to B (professionnel à professionnel), concernant au surplus la réutilisation à des fins commerciales de données personnelles, domaine particulièrement sensible.

Il est cependant probable que les juges n'auraient pas statué à l'identique si l'utilisateur en question avait été un consommateur. Il est donc essentiel pour les responsables de sites de faire figurer les CGU sur toutes les pages de leur site, et de faire une référence expresse à ces conditions sur les pages mettant à disposition des internautes des données ou services considérés comme « sensibles », au risque de voir leurs CGU inopposables.

Par Webconseil, Société de conseil .

Pour en savoir plus: contact@webconseil.fr

Droit de la communication et des télécommunications

Le Wi-fi, enjeux juridiques -18/01/2004

Par Melle Sophie Lalande, et M. Nicolas Lalande .



Le gouvernement est conscient du retard de la France dans le développement des nouvelles technologies, notamment du réseau Internet. Il a donc présenté, début septembre, un ensemble de mesures visant à déployer la téléphonie mobile et le Haut Débit.

Le gouvernement est conscient du retard de la France dans le développement des nouvelles technologies, notamment du réseau Internet. Il a donc présenté, début septembre, un ensemble de mesures visant à déployer la téléphonie mobile et le Haut Débit. Certaines mesures ont été prises afin de libéraliser les technologies hertziennes. Ainsi, la mise en place des réseaux locaux sans fil, le Wi-Fi (Wireless-Fidelity), est désormais simplifiée.

Le principal attrait du Wi-Fi est de supprimer le câblage et de réduire les coûts de déploiement. Cependant, les communications sans fils sont difficiles à sécuriser (1.).

De plus, on entend souvent parler des problèmes que peuvent engendrer les ondes radio pour le corps humain. Or, la technologie du Wi-Fi demande l'installation d'un émetteur radio dans les locaux où l'on désire utiliser le réseau sans fil... (2.)

1. Un problème de responsabilité juridique

Nous le disions précédemment, les réseaux Wi-Fi sont difficiles à sécuriser. En effet, les ondes que le système Wi-Fi utilise peuvent arroser un environnement plus large que celui désiré. Le mode « infrastructure » plus sûr que le mode « Ad Hoc » [1], n'est tout de même pas infallible. Ainsi, il est nécessaire d'installer un cryptage avancé [2]. Cette protection revêt d'autant plus d'importance que des utilisateurs frauduleux peuvent, à notre insu, utiliser la connexion Wi-Fi à des fins juridiquement répréhensibles.

Or, comme nous l'avons vu dans une précédente étude [3], le Conseil d'État [4]

avait précisé [5] qu'« [...] il importe de trouver un équilibre entre la préservation de l'anonymat des individus sur les réseaux et **la nécessité de pouvoir retrouver leur identité lorsqu'ils commettent des infractions**. Des obligations de conservation des données de connexion doivent dès lors être imposées aux intermédiaires techniques afin de faciliter les enquêtes judiciaires par une meilleure « traçabilité » des utilisateurs des réseaux ». En résumé, l'adresse IP d'un ordinateur peut être utilisée aux fins d'une enquête judiciaire.

Nous savons que lors de la navigation sur Internet, c'est l'adresse IP du serveur Proxy [6], ou du routeur, qui apparaît. Ainsi, le propriétaire du réseau local est responsable juridiquement en cas d'infraction. Cependant celui-ci pourra se retourner contre l'utilisateur ayant commis la faute. A cet égard il est nécessaire que le propriétaire du réseau soit équipé d'un système permettant de tracer l'activité des utilisateurs, et ce dans le respect des libertés individuelles. Ce dernier point rend d'autant plus difficile l'utilisation légale d'un traceur et montre l'importance de fixer des règles pour les personnes connectées connues et/ou l'acquisition d'un filtrage efficace.

2. Un devoir d'information pour l'installateur du réseau sans fil

La diffusion Wi-Fi, contrairement à Internet, ajoute des émissions radio supplémentaires à notre environnement. En effet, il est nécessaire d'installer un émetteur dans son environnement pour faire fonctionner le réseau. Des lois en limites cependant la puissance [7].

Il est reconnu que, même s'il est difficile de déterminer l'ampleur des risques sanitaires des ondes radios, ces dernières restent nocives pour le corps humain en particulier pour le cerveau.

De ce fait, l'idée d'avoir plusieurs heures par jour, une quantité de radiations électromagnétiques supplémentaires devrait susciter de sérieuses questions chez le consommateur.

Certes, les défenseurs du Wi-Fi rétorquent que les téléphones portables nous exposent plus aux ondes électromagnétiques en raison de leur plus grande puissance. Cependant, il faut réfléchir au fait que ce n'est pas une à deux heures par jour d'exposition aux ondes avec le Wi-Fi mais bien 24h/24. De plus, le Wi-Fi ne remplace pas le mobile. Il faut donc se poser la question quant à l'expansion galopante du nombre d'ondes électromagnétiques dans notre environnement.

Un second point, découlant du premier, concerne la pollution occasionnée par les ondes émises. En effet, tout comme la cigarette, le Wi-Fi contamine à leur insu, via ses ondes, les personnes alentour. Sur ce point, aucune loi n'existe si ce n'est sur la limitation de la puissance des antennes.

Un autre problème est le brouillage radio généré par un appareil électronique (micro-onde, cartes ou antennes...) dont une des harmoniques émises pourrait perturber l'émetteur sans fil. Le fonctionnement du réseau risquerait alors d'être brouillé.

Il est donc intéressant de souligner que les prestataires de service (vendeur du matériel et/ou installateur) sont soumis au **devoir de conseil et une obligation de renseignement de l'article 1147 du Code civil**. Un défaut d'information du client, concernant l'ensemble des spécificités précitées, pourrait bien mettre lesdits professionnels dans une situation délicate...

Ainsi, nous comprenons que le Wi-Fi présente de grands avantages en termes de facilité d'usage. Il est cependant important de prendre conscience des complications en terme de sécurité du réseau et de santé, ceci afin de prévenir les problèmes juridiques qu'elles pourraient dans l'avenir engendrer.

Par Melle Sophie Lalande, et M. Nicolas Lalande .

[1] « En mode infrastructure chaque ordinateur station se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé ensemble de services de base (en anglais basic service set, noté BSS) et constitue une cellule. En mode ad hoc les machines sans fil clientes se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès ». Définitions tirées du site Comment ça marche ? URL : <http://www.commentcamarche.net/wifi/wifimodes.php3#adhoc>, dernière visite le 29 décembre 2003.

[2] Le chiffrement n'est pas à la portée du commun des mortels; il est donc nécessaire de faire appel à un informaticien afin de sécuriser un réseau. Pour de plus amples informations techniques sur la sécurisation des communications Wi-Fi, se référer à l'article de Frédéric Combeau dans la revue MISC, Novembre – Décembre 2003, Sécurisation des communications Wi-Fi avec IPSec.

[3] Sophie Lalande, L'adresse IP de votre ordinateur : une donnée personnelle relevant du régime de protection communautaire ?, URL : <http://www.droit-ntic.com/news/afficher.php?id=191> , décembre 2003.

[4] Jean-François THERY, Isabelle FALQUE-PIERROTIN. Conseil d'État. Section du rapport et des études Paris. La Documentation française. 1998, (Les Etudes du Conseil d'État), URL : <http://www.internet.gouv.fr/francais/textesref/rapce98/sommaire.htm>, dernière consultation le 10 décembre 2003.

[5] Par une lettre du 22 septembre 1997, le Premier ministre avait demandé au Conseil d'État d'analyser les questions juridiques liées au développement d'Internet et de mettre en lumière les adaptations nécessaires de notre droit.

[6] Interface entre un réseau local et Internet.

[7] Pour plus d'information voir sur : <http://www.art-telecom.fr/>, dernière consultation le 8 janvier 2004.

Informatique et libertés, Pourriels

La prospection par messagerie électronique : le projet de LCEN au 24 décembre 2003 -10/01/2004

Par Me. Pascal ALIX, Avocat individuel (cabinet groupé) .



L'article 12 du projet de loi pour la confiance dans l'économie numérique (LCEN) contient les dispositions relatives à la prospection électronique, lesquelles sont destinées à transposer notamment les normes européennes.

► L'article 12 du projet de loi pour la confiance dans l'économie numérique (LCEN) contient les dispositions relatives à la **prospection électronique**, lesquelles sont destinées à **transposer notamment** :

- la **directive** européenne n° 2000/31 du 8 juin 2000 dite "**commerce électronique**",

- ainsi que la **directive** n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 dite "**vie privée et communications électroniques**".

L'article 7 de la directive européenne dite "commerce électronique", relatif aux ""communications commerciales non sollicitées" dispose, rappelons-le :

"1. Outre les autres exigences prévues par le droit communautaire, les États membres qui autorisent les communications commerciales non sollicitées par courrier électronique veillent à ce que ces communications commerciales effectuées par un prestataire établi sur leur territoire puissent être identifiées de manière claire et non équivoque dès leur réception par le destinataire.

2. Sans préjudice de la directive 97/7/CE et de la directive 97/66/CE, les États membres prennent des mesures visant à garantir que les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées consultent régulièrement les registres "opt-out" dans lesquels les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces dernières.",

tandis que l'article 13.1 de la directive "**vie privée et communications électroniques**" interdit le "spamming" publicitaire, de la manière suivante : "l'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs, de courrier électronique à des fins de prospection directe **ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable** " ("opt-in").

Cependant l'alinéa 2 contient une dérogation : la prospection est permise, par la personne, physique ou morale, qui a recueilli les données (adresse e-mail, nom, ...) lorsque celles-ci ont été obtenues auprès de clients **dans le cadre de la vente d'un produit ou de la fourniture d'un service**, mais seulement à des fins de prospection directe **pour des produits ou services analogues** par cette même personne. Dans cette hypothèse, le client/prospect doit être clairement et expressément informé, à chaque message électronique, de la faculté de s'opposer à cette exploitation ("opt-out").

Par ailleurs, aux termes de l'article 10 de la directive n° 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002, l'utilisation par un fournisseur des techniques de communication à distance (notamment automate d'appel et télécopieur) en matière de **services financiers** à distance nécessite le **consentement préalable du consommateur, sans distinction**.

Cette réglementation européenne a pour conséquence l'interdiction de tout courriel non sollicité émanant d'une personne avec laquelle le prospect n'a jamais eu aucune relation d'affaires,

La directive dite "**vie privée et communications électroniques**" laisse toutefois aux États membres le choix du régime pour la prospection des personnes morales.

En France, au mois de février 2003 l'Assemblée Nationale, en première lecture, a choisi de ne pas distinguer les personnes morales des personnes physiques. Le double régime du consentement préalable ("opt-in") et du droit d'opposition ("opt-out") devait donc s'appliquer à tout prospect, sans distinction.

Après examen du texte par le Sénat, la position du Parlement français était la suivante :

S'agissant des personnes morales, il était nécessaire de distinguer selon que la prospection est effectuée **au moyen d'automates d'appel et de télécopieurs** ou au moyen de **courriers électroniques** (courriels ou SMS).

Pour les "mailings" par automate d'appel ou par télécopie, la prospection directe d'une personne morale nécessitait son **consentement préalable dans tous les cas**.

Pour les courriers électroniques, le projet de loi tel qu'adopté par le Sénat **distinguait** selon que la personne morale était ou non **inscrite ou non au registre de commerce et des sociétés**. Si la personne morale n'était pas inscrite au registre de commerce et des sociétés (par exemple association régie par la loi de 1901 ou membre d'une profession libérale), la prospection directe était interdite en l'absence de consentement préalable de la personne morale. Si la **personne morale** était **inscrite au registre** de commerce et des sociétés (sociétés commerciales ou civiles), la prospection directe était autorisée, **sous réserve de réunir quatre conditions** cumulatives :

- les coordonnées du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi n° 78 17 du 6 janvier 1978 dite "Informatique et Libertés" (1),

- à l'occasion de la vente d'un produit ou de la fourniture d'un service (2),

- la prospection directe concerne des produits ou services fournis par la même personne physique ou morale que celle ayant fourni initialement des produits ou services au destinataire (3),

- le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé ("opt-out") (4).

Le Sénat a réussi le difficile exercice de se conformer à la directive dite "**vie privée et communications électroniques**" tout en ne négligeant pas les souhaits exprimés par les professionnels et notamment les professionnels du marketing direct.

Le prospecteur était tenu, bien entendu, de se conformer aux dispositions de la loi n° 78 17 du 6 janvier 1978 dite "Informatique et Libertés", en permettant au destinataire de se désinscrire facilement.

Il était, enfin, interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise, et de mentionner un objet de message sans rapport avec la prestation ou le service proposé.

Le projet de LCEN a été notablement modifié, le 10 décembre 2003, par l'Assemblée Nationale.

Tenant compte des souhaits exprimés par les professionnels du marketing direct, l'Assemblée nationale a exclu de la double protection ("opt-in" et "opt-out") l'ensemble des personnes morales, sans retenir le critère - délicat à appliquer - de l'inscription au registre du commerce et des sociétés.

Pour résumer, la situation, en matière de prospection électronique (par courriel ou SMS) la situation est, pour le moment, la suivante :

Prospection en direction des personnes physiques :

1. Principe du **consentement préalable** ("opt-in"), qui s'exprime (en principe de manière "libre et éclairée") **par la personne physique concernée**, lors de la constitution de fichiers "opt-in" (par exemple pour bénéficier de services gratuits). La faiblesse de cette protection réside dans la possibilité d'exploitation des fichiers par les partenaires du prestataire qui a collecté les données (nominatives) et recueilli le consentement à recevoir des offres promotionnelles.

2. Principe du **droit d'opposition préalable** ("prior opt-out") : le client d'un site marchand doit pouvoir s'opposer a priori (lors de la collecte des données) à la prospection par les partenaires du prestataire. Seul ce dernier peut adresser des courriels de nature publicitaire ou promotionnelle. Il s'agit, en théorie, d'une protection assez efficace des consommateurs.

Prospection en direction des personnes morales :

Actuellement, le projet de LCEN exclut la double protection s'agissant des personnes morales. De sorte que les sociétés commerciales et les personnes morales n'ayant pas un objet commercial pourraient être la cible d'un nombre encore plus grand d'envois non sollicités, jusqu'à un encombrement des comptes e-mail que de plus en plus de professionnels dénoncent.

Le dispositif ainsi défini demeure assez **critiquable** dès lors que

la distinction entre les personnes physiques et les personnes morales n'est pas opérante (il y a plusieurs millions d'entreprises individuelles et de personnes morales à but non lucratif),

il est souvent extrêmement difficile de s'assurer a priori qu'un fichier concerne un professionnel ou un non professionnel, tant l'utilisation des moyens professionnels à des fins privées et l'utilisation des moyens privés à des fins professionnelles sont aujourd'hui choses courantes.

Il est au demeurant inefficace, car les courriels réellement gênants, proviennent, pour l'essentiel, de l'étranger et notamment du continent nord-américain, pour lequel le spam automatisé est une véritable industrie. De sorte que les solutions sont d'abord techniques (filtrage du "spam").

Pour cette raison, les politiques de marketing direct par messagerie électronique, risquent d'être sérieusement limitées dans leurs effets dans les années à venir,

quel que soit le contenu de la LCEN, pour cause de filtrage systématique des courriels non expressément sollicités, ainsi que le proposent des prestataires de plus en plus nombreux (éditeurs de logiciels de sécurité, fournisseurs d'accès, etc...), compte tenu de l'exaspération des professionnels.

Trop de mailing tue le mailing...

Par Me. Pascal ALIX, Avocat individuel (cabinet groupé) .

Responsabilité

La responsabilité du prestataire de services en matière de solutions de sécurité informatique - 06/01/2004

Par Me. Murielle-Isabelle Cahen, Avocate .



La sécurité par voie électronique repose largement sur l'utilisation de moyens de chiffrement des échanges pour en assurer la confidentialité. Ces dernières années, le cadre juridique de la sécurité des services informatiques était mis en place, avec deux grands volets : la libéralisation de la cryptologie et la reconnaissance de la signature électronique.

► Le Conseil des ministres a adopté le 15 janvier 2003 un projet de loi "sur la confiance dans l'économie numérique", dans lequel la question de la responsabilité des "prestataires techniques" de l'Internet est un des points majeurs (chapitre 2 du projet de loi). Ce projet de loi fait suite au projet de loi sur la société de l'information ("LSI") et à l'avant-projet de loi sur l'économie numérique ("LEN"). Il a notamment vocation à transposer en droit français la directive européenne du 8 juin 2000 sur le commerce électronique.

Cette réglementation a mis en place le système d'une responsabilité limitée des prestataires techniques. L'article 2 du projet de loi redéfinit les obligations des prestataires intermédiaires des services de communication en ligne.

En matière de sécurité, et sans l'abroger formellement, le nouveau projet de loi modifie substantiellement la partie de la loi du 26 juillet 1996 consacrée à la cryptologie. La nouvelle loi libéralise sans réserve l'utilisation des moyens de cryptologie, définies comme "tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète".

En ce que concernent les prestataires qui assurent des prestations de cryptologie à des fins de confidentialité, le projet précise qu'ils sont présumés responsables, jusqu'à preuve contraire, et malgré toute disposition contractuelle contraire, du

"préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions". Cette présomption pourra être levée si le prestataire peut démontrer qu'il n'a commis aucune faute intentionnelle ou de négligence.

L'article 20 institue un régime de présomption de responsabilité à l'égard des fournisseurs de prestations de cryptologie. Les prestataires de cryptologie doivent pouvoir être reconnus responsables des dommages qui surviennent, lors de l'exécution de leurs prestations, aux personnes qui leur confient le soin d'assurer la confidentialité de certaines données. Lors de litiges mettant en cause la responsabilité civile de ces prestataires, le présent article renverse la charge de la preuve en établissant un régime de présomption de responsabilité des fournisseurs de prestations de cryptologie. Le champ d'application de ce régime se limite aux prestations de cryptologie à des fins de confidentialité.

Un régime spécifique de responsabilité est prévu à l'article 21 du présent projet de loi pour les personnes qui fournissent des prestations de cryptologie ayant seulement une fonction d'authentification ou de contrôle de l'intégrité de données. Le présent article institue, dans des hypothèses spécifiques, une véritable présomption de responsabilité. La présomption de responsabilité a un champ limité d'application : ce régime ne s'appliquerait qu'en présence de certificats dits « qualifiés » ou, tout au moins, présentés comme tels par le fournisseur.

La présomption de responsabilité ne jouerait qu'à l'égard des personnes ayant confié aux fournisseurs de prestations concernés la gestion de leurs conventions secrètes, lorsqu'un préjudice résulte d'une atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide desdites conventions. Dans le projet de loi sur la confiance dans l'économie numérique, l'Assemblée nationale a, en première lecture, précisé que les fournisseurs ne sauraient être responsables que dans le cadre des prestations qu'ils ont effectuées auprès des victimes de dommages.

Cet article vise à transposer l'article 6 de la directive 1999/93/CE du 13 décembre 1999 définissant un cadre communautaire pour les signatures électroniques :

- > les prestataires sont présumés responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés comme qualifiés qu'elles délivrent, lorsqu'il s'avère que ces certificats ne sont pas qualifiés;
- > ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité professionnelle.
- > Enfin, seuls certains faits générateurs du préjudice seraient couverts par ce

régime de responsabilité présumée. A ce titre, le présent article définit les hypothèses limitatives :

1°) lorsque les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes. Cette hypothèse d'engagement de responsabilité est prévue par le a) du point 1 de l'article 6 de la directive.

2°) lorsque les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes.

3°) lorsque le prestataire d'un service de certification électronique n'a pas vérifié que le signataire détenait bien, lorsque le certificat lui a été délivré, des données de création de signature qui correspondaient à celles, fournies ou identifiées dans le certificat, permettant de vérifier cette signature.

4°) lorsque le prestataire n'a pas assuré la complémentarité des données afférentes à la création de signature (clé privée) et de celles relatives à la vérification de cette signature (clé publique).

5°) lorsque le prestataire n'a pas enregistré la révocation du certificat et n'a pas tenu informé les tiers de ce fait.

Nonobstant le fait que ces conditions de mise en jeu de la présomption de responsabilité sont satisfaites, le présent article prévoit, conformément aux points 3 et 4 de l'article 6 de la directive 1999/31/CE, une éventuelle exclusion de responsabilité.

Les prestataires des services de sécurité informatique ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé à la condition que ces limites aient été clairement portées à la connaissance des utilisateurs dans le certificat.

Contractuellement, les prestataires et utilisateurs peuvent fixer des limites à l'utilisation des certificats fournis ainsi qu'à la valeur des transactions pour lesquelles ils peuvent être utilisés. Le projet de loi exige qu'en pareille circonstance ces limites doivent avoir été « clairement portées à la connaissance des utilisateurs dans le certificat ». Il faut en déduire que le défaut d'information des utilisateurs de certificats sur ce point rendra impossible l'exclusion contractuelle de la responsabilité du fournisseur de prestations de certification. Il reviendra à la jurisprudence de déterminer, au cas par cas, si le prestataire a bien « clairement » fait connaître à son cocontractant ces limitations de responsabilité. Dans ces conditions, l'utilisateur ne pourra bénéficier du régime de responsabilité défini par le présent article s'il a, de manière abusive, utilisé le certificat au-delà des limites fixées par le prestataire. Pour échapper à la mise en cause de sa responsabilité, le prestataire pourra toujours apporter la preuve qu'il n'a commis

aucune faute ou aucune négligence en fournissant ses services.

L'article 22 institue un mécanisme de sanction administrative à l'encontre du fournisseur de moyens de cryptologie qui n'aurait pas respecté les prescriptions de l'article 18 du projet de loi. L'autorité compétente pour prononcer des sanctions administratives à l'encontre des personnes qui n'auraient pas satisfait à leurs obligations est le Premier ministre. Les sanctions administratives s'appliquent aux personnes qui auraient omis de déclarer ou de solliciter une autorisation préalable, selon le cas et les modalités définies par l'article 18, pour la fourniture, l'importation, l'exportation, le transfert depuis ou vers un autre Etat membre de la Communauté européenne de moyens de cryptologie. Le non-respect de ces obligations est également sanctionné pénalement par les dispositions de l'article 23 du présent projet de loi.

La sanction qui peut être prononcée au titre du présent article est unique : une mesure d'interdiction de mise en circulation du moyen de cryptologie concerné.

Le projet de loi fait obligation aux personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité de remettre aux agents compétents les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Le fait de ne pas déférer à cette demande étant considéré comme une infraction (prévues à l'article 23). Un décret devra être adopté permettant de définir les modalités pratiques de mise en œuvre de cette obligation et sa prise en charge financière par l'Etat.

L'article 23 prévoit que sera désormais puni par la loi «le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçue ou spécialement adaptés», pour commettre des infractions dans des systèmes de traitement automatisé de données. Cet article donne un cadre juridique, non plus aux seules actions frauduleuses, mais également aux outils qui servent à les commettre.

Par Me. Murielle-Isabelle Cahen, Avocate .