# *Légiférer sur la sécurité informatique : la quadrature du cercle ?*

*Par Valérie Sédallian*
*Avocat au barreau de Paris*
*Membre du Comité scientifique de Juriscom.net*

*e-mail : sedallian@argia.fr*

**Introduction**

L'interconnexion croissante des réseaux et systèmes d'informations, la dépendance croissante des activités aux systèmes d'information induisent une vulnérabilité accrue de ces systèmes d'information vis-à-vis des atteintes à leur sécurité.

**Le monde électronique actuel est tout sauf sécurisé et fiable.** Régulièrement la presse se fait l'écho des attaques virales susceptibles d'affecter nos ordinateurs et de se propager à travers des applications aussi courantes que la messagerie, et ce sans compter les intrusions, piratages, malveillances en tout genre. De plus, elle révèle fréquemment de nouvelles failles affectant tel logiciel ou tel système d'exploitation avec en principe les moyens de corriger la faille. En pratique, on constate que les entreprises ne prennent pas toujours la peine de corriger les failles de sécurité qui sont signalées.

Les aléas techniques sont nombreux en matière informatique et la plupart des systèmes informatiques comportent des failles de sécurité.

A titre d'exemple, le FBI s'est associé au palmarès des 20 plus grandes failles de sécurité[1] publié par l'institut de recherche *SANS* (*Sysadmin, Audit, Networking and Security*). Des logiciels aussi courants que Internet Explorer, le navigateur par défaut fourni par *Microsoft*, ou Sendmail, le logiciel de gestion de la messagerie électronique des systèmes UNIX et GNU/LINUX sont concernés.

La sécurité informatique nécessite une véritable prise de conscience et la mise en place de mesures techniques et organisationnelles adéquates.

Ainsi, le 25 juillet 2002, l'*OCDE* mettait à jour ses Lignes directrices sur la sécurité des systèmes et réseaux d'information[2] et soulignait la nécessité de développer une culture de la sécurité, précisant que chacun, gouvernements, entreprises, organisations, utilisateurs individuels a un rôle à jouer pour assurer la sécurité.

La politique législative fait partie de cet arsenal de mesures destinées, non seulement à sanctionner, mais également à sensibiliser toutes les personnes concernées par la nécessité d'adopter et de mettre en œuvre les procédures disponibles pour faire face aux risques d'atteinte à la sécurité informatique.

Quel est justement l'arsenal législatif dont nous disposons ? On connaît bien les incriminations destinées à poursuivre et réprimer les pirates informatiques, mais à partir de quel moment devient-on un pirate ? Tant les juristes que les spécialistes de la sécurité informatique brandissent la menace du délit de manquement à l'obligation de sécurité des données personnelles prévu par l'article 226-17 du Code pénal, mais qu'en est-il sur le terrain judiciaire ? Les éditeurs de logiciels sont-ils soumis à des contraintes spécifiques ? Faut-il repenser l'arsenal législatif existant ?

[1] Voir : <http://www.sans.org/top20>.
[2] Lignes Directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information –Vers une culture de la sécurité – Recommandation du Conseil de l'OCDE du 25 juillet 2002, 1037ème session.

Trois acteurs interviennent dans ce débat sur la sécurité informatique : les organismes utilisateurs de systèmes d'information, les auteurs d'actes de fraude informatique et les éditeurs de logiciels.

Nous allons examiner la législation sur la sécurité informatique sous ces trois angles : celle des organismes utilisateurs de systèmes d'information, celle des pirates et celle des éditeurs de logiciels.

## 1. L'obligation de sécurité : une obligation méconnue ?

La législation sur les données personnelles soumet le responsable d'un traitement de données à l'obligation d'assurer la confidentialité et la sécurité des traitements de données, sous peine de sanctions pénales. En pratique, les poursuites sont exceptionnelles. Devrait-on envisager d'autres voies que la seule sanction pénale ?

### 1.1. La portée de l'obligation de sécurité

#### 1.1.1. Définition de l'obligation de sécurité

Le principe de l'obligation de sécurité est posé par l'article 29 de la loi du 6 janvier 1978 dite Informatique et Libertés :

« *Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* ».

Le non-respect de ces précautions est sanctionné par l'article 226-17 du Code pénal :

« *le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ».

La directive européenne 95/46 du 24 octobre 1995 relative au traitement de données à caractère personnel comporte des dispositions détaillées sur la confidentialité et la sécurité des traitements.

L'article 17.1 « Sécurité du traitement » de la directive précise :

« *Le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

Par ailleurs, la directive définit de manière précise les obligations incombant aux prestataires traitant des données pour le compte du responsable du traitement.

L'article 16 relatif à la confidentialité des traitements prévoit que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instructions du responsable du traitement, sauf en vertu d'obligations légales. Cette disposition vise les obligations incombant aux prestataires qui traitent des données pour le compte d'un organisme, par exemple un hébergeur.

L'article 17.2 relatif à la sécurité des traitements prévoit que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces principes.

L'article 17.3 précise que la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement et que les obligations de sécurité définies par l'article 17.1, incombent également à celui-ci.

Ces dispositions visent à formaliser les procédures (délégation de pouvoir, clauses adéquates dans les contrats, documents prouvant l'ordre de procéder à un traitement, possibilité d'audits afin de vérifier le respect des mesures de sécurité que le prestataire s'est engagé contractuellement à prendre par exemple), et à établir une chaîne de responsabilités, le responsable du traitement demeurant responsable de la confidentialité des données traitées pour son compte[3].

Les dispositions de la directive sont reprises aux articles 34 et 35 du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, portant transposition de la directive[4].

### 1.1.2. La portée de l'obligation de sécurité

L'article 226-17 du Code pénal ne précise pas la notion de « *précautions utiles pour préserver la sécurité de ces informations* ».

Classiquement, on considère qu'il s'agit d'une obligation de moyens, c'est-à-dire que l'on n'exige pas une sécurité absolue. L'obligation de sécurité a un caractère préventif et fait référence à une notion très générique : les « règles de l'art ».

Les besoins de sécurité des fonctions et informations sont notamment appréciés en fonction du triptyque DIC : Disponibilité, Intégrité, Confidentialité, bien connu des spécialistes de la sécurité informatique.

La mise en  d'une politique de sécurité nécessite de mettre en place des mesures variées, d'ordre logique (exemple : *firewalls*, cryptage, mots de passe, installation d'anti-virus), organisationnel (accès aux données en fonction des habilitations, sauvegardes, maintenance, mise à jour des logiciels pour installer les correctifs) et physique (contrôle d'accès aux locaux, protection contre les incendies, etc.).
Elle suppose également des actions de sensibilisations et de formation du personnel. Le tout consigné dans un document de référence et intégré aux procédures de l'organisme. Enfin, les mesures doivent être auditées et réexaminées périodiquement.

La mise en place de toutes ces mesures représente évidemment un poste de coût pour les organismes concernés.

L'article 17.3 de la directive précise que les mesures de sécurité : « *doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ».

En d'autres termes, les mesures adoptées doivent être adaptées à la nature des données à protéger : un simple fichier client de noms et adresses n'exige pas le même degré de sécurisation que des données médicales ou bancaires, couvertes par le secret professionnel. On raisonne en termes de gestion des risques, afin de trouver un compromis entre les besoins de circulation de l'information et de rapidité d'exécution et le niveau de sécurité exigé au regard des caractéristiques des données.

Dans le cadre des dossiers de déclaration (pour le secteur privé) ou de demande d'avis (pour le secteur public) des traitements de données nominatives, la CNIL demande que lui soient précisées les mesures relatives à la sécurité informatique prises par le responsable du traitement.
La CNIL joue à cet égard un rôle de sensibilisation des responsables de traitement[5].

---

[3] A. Lucas, Jean Devèze, Jean Frayssinet, *Droit de l'informatique et de l'Internet,* PUF, coll. Thémis, 2001, n°281.
[4] Projet de loi adopté en première lecture par l'Assemblée nationale (texte n° 780) le 30 janvier 2002 et par le Sénat (texte n°96) le 1er avril 2003, voir : <http://www.assemblee-nationale.fr/12/dossiers/cnil.asp>.
[5] *Lamy Droit de l'Informatique et des Réseaux,* 2003, n° 559.

Ainsi, la portée de l'obligation de sécurité, lourdement sanctionnée pénalement, apparaît très contraignante. Elle nécessite la mise en place de véritables politiques de sécurité au sein des organismes et de gérer avec rigueur les relations contractuelles avec les prestataires informatiques extérieurs. Dans la mesure où tout organisme est appelé à gérer des données personnelles, ne serait-ce que les données relatives aux clients ou usagers, et au personnel, le champ d'application de l'obligation de sécurité apparaît relativement large.

Certains auteurs soulignent ainsi que les risques de mise en cause de la responsabilité s'avèrent particulièrement élevés[6].

Voilà pour la théorie. Qu'en est-il sur le terrain ?

### 1.2. Le délit de manquement à l'obligation de sécurité

#### 1.2.1. Un délit ignoré ?

Les exemples de manquement à l'obligation de sécurité, et spécialement sur Internet, sont légion.

Par exemple, le site *Kitetoa.com* dénonce régulièrement les sites commerciaux qui sécurisent mal les données personnelles concernant leurs clients.

D'une manière générale, on invoque le manque de « culture sécurité » des entreprises. Pourtant, les poursuites pour manquement à l'obligation de sécurité informatique demeurent exceptionnelles en France.

On peut citer un arrêt de la Chambre criminelle du 30 octobre 2001 ayant condamné le Président d'un syndicat de médecins du travail pour défaut de prise des précautions utiles pour empêcher la communication d'informations médicales à du personnel administratif, tiers non autorisé, au motif notamment qu'il n'avait pas fait assurer une formation suffisante pour que chacun connaisse parfaitement le fonctionnement du système[7].

Dans le cas où un traitement ne permettait pas de gérer les homonymies, ce qui avait nuit à une personne victime d'une homonymie dans un fichier de mauvais payeurs, les juges ont estimé que le délit était constitué : ils ont considéré que l'obligation de sécurité concernait les troubles engendrés par la qualité de l'information et le processus de mise à jour et de correction des erreurs[8].

Le délit a été également considéré comme constitué dans le cas de la diffusion par un directeur de banque d'une liste de clients à des commerçants, la liste faisant apparaître des renseignements sur des tiers, l'attention des commerçants n'ayant pas été attirée sur la confidentialité des informations diffusées[9].

Ces affaires n'ont pas toujours trait *stricto sensu*, à la sécurité informatique.

Le fait de ne pas avoir adopté les mesures de sécurité informatique adéquates n'entraînerait donc pas un grand risque de poursuites pénales, c'est du moins sous cet angle que le ratio risques-coût d'une politique de sécurité pourrait être envisagé par les dirigeants des organismes concernés.

#### 1.2.2. Existe-t-il des explications à la faiblesse de ce contentieux ?

L'organisme dont les données sont divulguées suite à une mauvaise sécurisation de son système d'information est peut-être coupable du délit de manquement à l'obligation de sécurité, mais il peut

[6] Jean Frayssinet, « Internet et l'obligation de sécurité des données personnelles », *Expertise*, Août-septembre 2000, p. 253.
[7] Crim. 30 octobre 2001, Gaz. Pal. 12 octobre 2002.
[8] Ch. Crim. 19 décembre 1995, Expertises, janv. 97, 34, obs. Frayssinet.
[9] CA Rennes, 13 janvier 1992, Juris-data n° 42488.

être également victime du délit d'accès non autorisé à un système informatique, sanctionné par une peine d'un an d'emprisonnement et 15 000 euros d'amende (article 323-1 du Code pénal).

Bien que dans les textes, les peines encourues soient plus importantes pour le manquement à l'obligation de sécurité, la répression pénale préférera s'intéresser au pirate plutôt qu'à sa « proie ». Ainsi, nous verrons dans la deuxième partie de cette étude que l'exigence de protection du système ne fait pas partie des conditions de l'incrimination du délit d'intrusion frauduleuse.

L'affaire *Kitetoa c/ Tati* est une bonne illustration de cette problématique.

En 1999, l'animateur du site *kitetoa.com*, Antoine C., avait signalé à l'hébergeur du site des magasins *Tati* une faille de sécurité permettant d'accéder au contenu des bases de données clients du serveur grâce à un simple navigateur.

Constatant près d'un an après que les failles détectées et signalées existaient toujours, il publiait sur *Kitetoa.com* un article relatant la faille du site de *Tati*. L'information était reprise dans un magazine spécialisé, ce qui amenait la société *Tati* à porter plainte pour introduction non autorisée dans un système informatique.

L'animateur du site a été poursuivi par le parquet. En revanche, la société *Tati* n'a pas été poursuivie pour manquement à l'obligation de sécurité, alors que le simple fait que des données nominatives soient accessibles sur Internet sans protection, quelle qu'en soit la raison (faille non corrigée, mauvaise configuration) semblait caractériser un manquement à l'obligation de protéger les données personnelles.

Dans une décision en date du 13 février 2002, le Tribunal correctionnel de Paris a déclaré le webmestre du site *Kitetoa.com* coupable d'accès frauduleux dans un système de traitement automatisé de données, mais a rejeté la constitution de partie civile de la société *Tati*, au motif que : « *celle-ci ne saurait se prévaloir de ses propres carences et négligences pour arguer d'un prétendu préjudice en réalité subi par les personnes victimes éventuelles de violations de leur vie privée*[10] ».

Suite à un appel du Parquet général en vue de solliciter la relaxe du prévenu, démarche dont il convient de souligner au passage le caractère inhabituel, Antoine C. a été relaxé par décision en date du 30 octobre 2002 de la 12ème Chambre de la Cour d'appel de Paris[11].

Il existe pourtant une autre victime du délit d'intrusion dans un système informatique, celle dont les données auront été divulguées[12]. Cette victime-là peut porter plainte au titre du délit de manquement à l'obligation de sécurité sans risquer d'être elle-même poursuivie.

La faiblesse du contentieux relativement au manquement à l'obligation de sécurité s'expliquerait aussi par le faible nombre de victimes qui portent plainte.

Quelques tentatives d'explication peuvent être avancées :

- la victime peut, en premier lieu, ignorer totalement que ses données ont été divulguées. Si une entreprise a mal sécurisé ses données, peu importe les conditions dans lesquelles cette carence aura pu être constatée, il y a peu de chances qu'elle fasse de la publicité autour de l'incident ;
- en second lieu, le préjudice subi est d'ordre immatériel, difficile à quantifier en termes de gravité, et une plainte pénale peut sembler inappropriée, voire disproportionnée pour une victime individuelle, alors qu'il s'agit d'un préjudice collectif ;
- en troisième lieu, il ne semble pas exister de politique pénale clairement définie en la matière. Encore une fois, l'affaire *Tati* nous permet d'illustrer notre propos : après avoir déclenché des

[10] TGI Paris, 13 février 2002, *Revue Communication – Commerce Electronique*, mai 2002, p. 31 note Grynbaum.
[11] CA Paris, 12ème ch. 30 octobre 2002, *Revue Communication – Commerce Electronique*, janvier 2003, p. 30, note Grynbaum.
[12] Jean Frayssinet, « Internet et l'obligation de sécurité des données personnelles », *Expertise*, Août-septembre 2000, p. 253.

poursuites contre l'animateur du site *Kitetoa.com* suite à la plainte de la société *Tati*, le parquet fait appel de sa condamnation pour solliciter la relaxe, ce qui ne semble guère cohérent. La société *Tati* ne sera pas poursuivie mais verra sa demande de dommages et intérêts rejetée en raison de ses propres carences. Les contentieux sont rares parce que les poursuites du Ministère public dans ce domaine le sont également ;

- enfin, dernière raison qui peut être avancée, celle de la difficulté d'une instruction pénale dans un tel domaine. En matière pénale, on ne peut pas se contenter de présomptions. Il faut prouver que les mesures de sécurité nécessaires n'ont pas été mises en œuvre, ce qui peut nécessiter de constater l'état de la sécurité du système au jour de l'incident ou dans un laps de temps très proche. Si les failles sont corrigées après divulgation d'un incident (ex : article de presse relatant le piratage d'une base de données), comment pourra-t-on prouver avec certitude les manquements ? Comment en dehors du « flagrant délit » caractériser les éléments du délit ?

Mais si le contentieux est faible, n'est-ce pas également en raison de l'inadéquation entre les lourdes sanctions pénales prévues à l'encontre d'organismes qui ont à la fois la casquette de « délinquant » et de « victime » en cas de piratage ?

Pourrait-on envisager des sanctions et/ou obligations autres que le couperet de la loi pénale ?

### 1.3. La sanction pénale doit-elle être la seule envisagée ?

#### 1.3.1. Elargir l'éventail des sanctions

En novembre 2001, quelques personnes ont découvert une faille de sécurité sur un site Internet de l'éditeur américain *Ziff Davis Media*. Les autorités judiciaires de plusieurs états américains ont engagé des poursuites au nom de la défense des consommateurs.

Un accord a été passé avec lesdites autorités judiciaires, prévoyant le versement d'une amende de 125 000 dollars, un dédommagement de 500 dollars pour chacun des internautes victimes de la faille et le versement de 100 000 dollars aux états-plaignants. L'éditeur a dû également s'engager à faire établir un audit régulier de ses systèmes de sécurité[13].

De tels arrangements sont spécifiques au droit américain et difficilement transposables. Nous ignorons également le fondement légal des poursuites et les peines encourues, alors qu'il n'existe pas à notre connaissance de délit équivalent à notre manquement à l'obligation de sécurité en droit américain. Quelques idées suggérées par ces faits pourraient toutefois être explorées :

- le fondement des poursuites n'est pas un manquement à la sécurité informatique, mais le droit de la consommation. Or, les associations de consommateurs peuvent intenter des actions dites en cessation d'agissements illicites, sur le fondement de l'article L 421-6 du Code de la consommation ;
- des sanctions financières ;
- l'obligation d'établir un audit régulier de ses systèmes d'informations.

#### 1.3.2. Favoriser la prévention et l'information

Une politique de sécurité informatique devrait également favoriser la prévention et l'information.

Certains textes semblent d'ailleurs privilégier une approche préventive de la sécurité informatique.

On retrouve des dispositions relatives à l'obligation de sécurité dans la directive n° 2002/58 du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

---

[13] Thuan Huynh, « Ziff Davis se fait épingler sur sa sécurité internet », *Journal du Net*, 2 septembre 2002, <http://www.journaldunet.com/0209/020902ziff.shtml>.

L'article 4 « Sécurité » de cette directive prévoit :

«1. *Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.*

*2. Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable »*.

Si le premier paragraphe est un rappel de l'obligation de prendre les mesures de sécurité adéquates, déjà prévue dans la directive 95/46 sur le traitement des données à caractère personnel, le deuxième paragraphe est différent quant à sa portée.

Il s'agit de mettre à la charge des fournisseurs de services une obligation d'information des risques existant en matière de sécurité et des mesures que les utilisateurs et abonnés peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou des techniques de cryptage[14].

Or, curieusement, le projet de loi relatif aux communications électroniques et aux services de communication audiovisuelle, présenté en Conseil des Ministres le 23 juillet 2003[15] et visant à transposer différentes directives relatives au secteur des télécommunications, dont la directive « vie privée », ne contient aucune disposition reprenant l'article 4.2 de la directive.

L'article 84 du projet prévoit d'insérer un nouvel article L. 121-90 au Code de la consommation afin de définir précisément les clauses minimales qui devront figurer dans les contrats conclus entre les fournisseur de services de communications électroniques et les consommateurs. L'obligation d'information des risques existant en matière de sécurité ne fait pas partie de ces clauses contractuelles imposées aux fournisseurs de services.

En d'autres termes, il n'aurait pas semblé utile aux rédacteurs du projet de transposer en droit français cette obligation d'information. Peut-être cet oubli sera-t-il réparé par le Parlement.

En Californie, une loi datant du 12 février 2002 (*Security Breach Information Act* – SB 1386) entrée en vigueur le 1er juillet 2003[16] innove en matière de politique législative et en matière de sécurité informatique, en obligeant tout organisme traitant des données informatiques qui contiennent des données personnelles, en cas d'atteinte à la sécurité du système, à en informer (*disclose*) les résidents californiens dont les données personnelles contenues dans ses fichiers ont été divulguées ou sont présumées divulguées à des personnes non autorisées.

Les données concernées sont les prénom et nom associés à un numéro de sécurité sociale, de permis de conduire, de plaque d'immatriculation, ou de compte bancaire, de carte de paiement et de crédit couplé à un mot de passe.

Les organismes ayant crypté leurs fichiers ne sont pas soumis à cette obligation.

Il est également prévu que les forces de l'ordre puissent interdire cette notification, pour ne pas entraver le bon déroulement d'une enquête pénale en cours.

---

[14] Considérant n° 20 de la directive 2002/58/CE.
[15] Voir : <http://www.telecom.gouv.fr/telecom/index_ce.htm>.
[16] Le texte de la loi est disponible à l'URL : <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.

Cette loi vise notamment à enrayer les conséquences de l'explosion des usurpations d'identité, un phénomène en expansion outre-atlantique, alors que la protection des données personnelles est beaucoup moins encadrée aux Etats-Unis qu'en Europe [17].

En cas de manquement à cette obligation d'information, le client qui a subi un dommage du fait de ce manquement dispose d'une action civile en dommages et intérêts.

L'avenir nous dira si ce type de démarche s'avère efficace pour sensibiliser les entreprises et autres organismes à la nécessité de mieux sécuriser les données personnelles traitées.

Pour résumer, la législation française exige un bon niveau de sécurité des données personnelles traitées, adapté à la sensibilité des données en cause. Le manquement à l'obligation de sécurité est envisagé sur un terrain uniquement répressif.

Ce tout répressif des textes est contredit par un contentieux quasi-inexistant, ce qui affaiblit la portée du texte, l'angle préventif étant absent des textes en vigueur et en préparation.

Voyons maintenant comment le législateur envisage la répression de la fraude informatique.

## 2. L'incrimination de la fraude informatique : quelles limites ?

Les articles 323-1 à 323-7 du Code pénal instituent un certain nombre d'incriminations en matière de fraude informatique.

Est notamment réprimé et est puni de peines d'emprisonnement et d'amende :

- le fait de s'introduire frauduleusement dans un système informatique et/ou de se maintenir frauduleusement dans le système (article 323-1 du Code pénal) ;
- le fait d'entraver ou de fausser le fonctionnement d'un système informatique (article 323-2 du Code pénal) ;
- le fait d'introduire frauduleusement des données dans un système informatique ou de supprimer ou de modifier frauduleusement les données qu'il contient (article 323-3 du Code pénal).

Traditionnellement, on considère que l'exigence de protection du système ne fait pas partie des conditions de l'incrimination (2.1).

Un projet de loi relatif à la confiance dans l'économie numérique, en cours de discussion devant le Parlement[18], prévoit une augmentation des peines encourues en matière de fraude informatique et la création d'une nouvelle incrimination dite de fourniture de moyens, c'est-à-dire que l'on donnerait un cadre juridique pour les poursuites contre ceux qui fournissent les outils servant à commettre les attaques informatiques (2.2).

Ce sont à ces deux problématiques que nous allons nous intéresser.

### 2.1. La protection du système par un dispositif de sécurité

Peu importe qu'un système ait été mal sécurisé : la protection du système n'est pas une condition de l'incrimination et tester les failles de sécurité d'un système de sa propre initiative caractérise le délit d'accès frauduleux à un système informatique.

#### 2.1.1. La protection d'un système n'est pas une condition de l'incrimination

[17] Jean-Marc Manach, « La Californie impose que les failles de sécurité informatique soient rendues publiques », *Transfert.net,* 1er juillet 2003, <http://www.transfert.net/a9056>.
[18] Les travaux préparatoires sont disponibles à l'URL : <http://www.assemblee-nationale.fr/12/dossiers/economie_numerique.asp>.

La loi ne distingue pas selon les procédés d'accès. La jurisprudence en a déduit que les textes visent tous les modes de pénétration irréguliers d'un système de traitement automatisé de données[19].

L'accès tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'accéder au système ou n'a pas le droit d'y accéder de la façon dont elle y a accédé.

La Cour d'appel de Paris dans un arrêt rendu le 5 avril 1994 a posé le principe que :

« *Pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu'il n'est pas nécessaire pour que l'infraction existe, que l'accès soit limité par un dispositif de protection, mais il suffit que le « maître du système »*[20] *(au sens de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel signée à Strasbourg le 28 janvier 1981...) ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées ; que lorsque l'accès a été régulier, le maintien sur un système automatisé de données peut devenir frauduleux, lorsque, par une sorte d'intervention de titre, l'auteur du maintien se trouve privé de toute habilitation* »[21].

L'accès ou le maintien irrégulier suppose que l'accédant n'a pas respecté la « règle du jeu », que celle-ci procède de la loi, du contrat ou de la volonté du « maître du système », peu importe que le système ait bénéficié d'un dispositif de sécurité que l'agent aurait violé.

La barrière technique n'est pas indispensable au jeu de l'interdiction, et l'acte incriminé est indépendant de la difficulté d'exécution. L'élément moral de l'infraction, l'intention frauduleuse résultera de ce que l'auteur a conscience de l'irrégularité de son acte, de ce qu'il accède ou se maintient sans droit dans le système[22].

Certains auteurs considèrent ainsi que : « *il n'est pas licite de pénétrer chez autrui sans autorisation et que, notamment, l'infraction de violation de domicile peut être constituée sans qu'il faille avoir égard à la hauteur du mur d'enceinte ou à la résistance de la serrure*[23]. »

Dans le même ordre d'idée, dans une proposition de décision-cadre relative aux attaques visant les systèmes d'information24, la Commission européenne souligne que :

« *La Commission ne souhaite nullement mettre en cause l'importance qu'elle attache à l'utilisation de mesures techniques efficaces pour protéger les systèmes d'information. Le fait est néanmoins qu'une grande partie des utilisateurs s'exposent malheureusement à des attaques faute d'une protection technique adéquate (voire même de toute protection). En vue de prévenir les attaques contre ces utilisateurs, le droit pénal doit couvrir l'accès non autorisé à leurs systèmes, même si ces systèmes ne bénéficient pas d'une protection technique appropriée. C'est pour cela et à condition que soit établie soit une intention de porter préjudice soit une intention d'obtenir un avantage économique qu'il n'est pas nécessaire que des mesures de sécurité aient dû être déjouées* ».

---

[19] *Juris-classeur Pénal*, « Atteintes aux systèmes de traitement automatisé de données », art. 323-1 à 323-7, n°25 et suivants ; *Lamy Informatique et Réseaux*, 2003, n°3494 et suivants.

[20] Au sens de la législation sur les données personnelles, le « maître du système » est la personne ayant le pouvoir de décider de la mise en œuvre d'un traitement informatique. La Convention internationale pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981 donne la définition suivante du « maître du fichier » : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.* »

[21] CA Paris, 5 avril 1994, Petites Affiches 1995, n° 80, p. 13, note Alvarez.

[22] Jérôme Dupré, « Pour un droit de la sécurité économique de l'entreprise », Thèse 2000, *Université de Nice-Sophia Antipolis*, n° 342 et s ; Voir aussi du même auteur : « Renseignement et entreprises – Intelligence économique, espionnage industriel et sécurité juridique, *Lavauzelle*, 2002.

[23] Christian Le Stanc, « Du Hacking considéré comme un des beaux arts et de l'opportun renforcement de sa répression », *Revue Communication, Commerce Electronique*, avril 2002, p. 9.

[24] Com/2002/0173 final, JOCE C 203 E du 27 août 2002, p. 0109.

Lors des travaux préparatoires à la loi dite Godfrain, le Sénat avait souligné qu'une exigence de protection du système pour que l'infraction soit constituée lui paraissait raisonnable, le droit pénal ne devant pas compenser l'insuffisance ou la défaillance des mesures de sécurité.
L'assemblée nationale a jugé excessive cette exigence du Sénat[25].

Il y a ainsi une contradiction entre les objectifs poursuivis par la législation sur les données personnelles, qui visent à obliger l'organisme responsable de la mise en œuvre d'un traitement à sécuriser son système d'information, et les nécessités de la répression à l'égard des atteintes frauduleuses aux systèmes informatiques. Or, dans ce cadre, l'infraction ne doit pas être fonction de la difficulté matérielle liée à son exécution, de l'état de la technique, mais du caractère dolosif de l'intrusion.

Il est possible que l'exigence de protection raisonnable du système créerait des marges d'interprétation trop larges. Pourtant, et pour reprendre l'analogie faite par certains auteurs avec la violation de domicile, même si le délit de violation de domicile ou de vol ne nécessite pas que le domicile objet de l'effraction ait été fermé à clé, aucune loi n'oblige les personnes à fermer à clé leur domicile sous peine de sanction pénale. **Ce serait finalement face à un constat de carence sur le faible niveau des mesures de sécurité prises par les utilisateurs que la protection du système par un dispositif de sécurité n'est pas érigée en condition de l'incrimination d'accès frauduleux dans un système informatique.**

Cependant, nous avons vu à propos de l'affaire *Kitetoa / Tati*, que le fait pour un organisme victime d'un piratage de ne pas avoir respecté l'obligation de sécurité peut priver ce dernier de tout recours contre l'auteur de la fraude informatique[26], et pourrait, le cas échéant, comme en matière de vol, le priver de son droit à indemnisation par son assurance.

De même, le mobile est indifférent : peu importe que l'auteur du délit d'accès non autorisé ait voulu dénoncer les failles de sécurité d'un système.

### 2.1.2. Tester les failles de sécurité d'un système

Forcer un accès, quand bien même il s'agirait de tester la sécurité d'un système ou démontrer que des règles élémentaires de sécurité n'ont pas été respectées rentre dans le cadre de l'incrimination d'accès frauduleux.

Ainsi, le journal d'informations en ligne *Transfert.net* relatait dans un article du 2 octobre 2003 que le dirigeant d'une société de sécurité informatique américaine, après avoir révélé l'existence de failles dans les systèmes informatiques de l'armée américaine, a été incarcéré[27].

L'article indique que les mots de passe par défaut de certaines machines (*administrator* ou *password*) n'avaient pas été changés.

En droit français, un accès non autorisé au système en cause, constituerait également le délit d'introduction frauduleuse dans un système informatique, peu importe que les mots de passe par défaut n'aient pas été changés.

Une démarche de recherche scientifique n'est pas davantage une excuse autorisant à démontrer, en fabriquant des fausses cartes bancaires, l'existence d'une faille dans le système des cartes de paiement[28].

---

[25] Jérome Dupré, préc. n° 346.
[26] Voir supra § 1.2.2.
[27] Jean-Philippe Gaulier, « Le patron d'une startup américaine arrêté pour avoir révélé des failles de sécurité », *Transfert.net*, <http://www.transfert.net/a9371>.
[28] Aff. Serge H. / GIE Cartes bancaires, TGI Paris, 13ème chambre, 25 février 2000, *Revue Communication, Commerce Electronique*, mars 2001, comm. n° 28.

Sur le terrain du contentieux du travail, un salarié qui avait voulu critiquer les choix de sa direction informatique en matière de sécurité informatique, a vu le bien-fondé de son licenciement pour faute grave confirmé par la Cour de cassation[29]. A l'appui de ses critiques sur la sécurité informatique mise en place, ledit salarié avait en effet procédé à des tests d'intrusion sans autorisation de sa hiérarchie et accédé à des données auxquelles il n'était pas habilité à accéder avec son propre mot de passe.

Ainsi, tester de sa propre initiative, les faiblesses de la sécurité informatique d'un système, sans être mandaté, par exemple au titre d'un audit de sécurité, ledit système serait-il celui de votre hôpital, celui de votre banque ou celui de votre employeur, est un délit pénal. De manière classique, la motivation ne supprime pas l'intention frauduleuse.

En d'autres termes, la carence d'un organisme à sécuriser les données personnelles qu'il traite n'est pas une excuse ou une circonstance atténuant la responsabilité pénale de ceux qui chercheraient, par des moyens frauduleux, à accéder au système.

Pour l'avoir oublié, dix personnes qui voulaient démontrer devant la presse la vulnérabilité de sites bancaires ont vu leur conférence de presse annulée par l'intervention de la police[30].

La vulnérabilité reposait selon eux sur une « *faille élémentaire… facilement exploitable sans connaissance informatique complexe ni matériel sophistiqué* ».

Mais qu'en est-il lorsqu'un système n'est pas seulement mal sécurisé, mais pas sécurisé du tout, de telle sorte qu'il devient possible d'y accéder par des « moyens informatiques réguliers » ?

Dans l'affaire *Tati* que nous avons évoquée ci-dessus[31], c'est suite à un appel du Parquet, que l'animateur du site *Kitetoa* sera finalement relaxé par une décision en date du 30 octobre 2002 de la 12ème Chambre de la Cour d'appel de Paris[32].

La Cour considère qu'on ne peut pas reprocher à un internaute d'accéder ou de se maintenir dans les parties d'un site accessible par la simple utilisation d'un logiciel de navigation, et que « *ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès (…). La détermination du caractère confidentiel et des mesures nécessaires à l'indication et à la protection de cette confidentialité relevant de l'initiative de l'exploitant du site ou de son mandataire* ».

Cette motivation paraît directement en contradiction avec la jurisprudence qui considère que l'exigence de protection d'un système est indifférente pour caractériser l'élément matériel du délit d'intrusion frauduleuse.

Ainsi, pour solliciter la relaxe du webmestre du site *Kitetoa*, le Parquet avait plutôt insisté sur l'absence d'élément intentionnel et de volonté de nuire.

La décision vise en définitive exclusivement l'accès à des données via une simple URL sur Internet, sans mot de passe ni restriction.

On ne peut toutefois pas généraliser au regard des particularités de cette affaire et considérer que la jurisprudence considère désormais que l'absence de sécurité suffisante d'un système empêche la caractérisation du délit d'accès frauduleux.

---

[29] Soc. 1er octobre 2002, *Gaz. pal*. 20 avril 2003, p. 33, note Tessalonikos.
[30] Dépêche AFP du 27 septembre 2002.
[31] Voir supra § 1.2.2.
[32] CA Paris, 12ème ch. 30 octobre 2002, *Revue Communication – Commerce Electronique*, janvier 2003, p. 30, note Grynbaum.

### 2.2. L'incrimination autonome de la fourniture de moyens : jusqu'où peut-on aller ?

Plusieurs textes, déjà en vigueur ou en cours d'adoption, dans l'objectif de renforcer notre arsenal répressif contre la fraude informatique, prévoient l'incrimination autonome de la fourniture de moyens. L'objectif est de permettre une répression efficace de la mise à disposition des outils qui permettent la réalisation d'actes de fraude informatique.

#### 2.2.1. Les textes incriminant la fourniture de moyens

Ces textes concernent :

- **la contrefaçon des cartes de paiement**[33]

L'article L 163-4-1 du Code monétaire et financier[34] dispose que :

« *Est puni de sept ans d'emprisonnement et de 750 000 Euros d'amende le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions prévues au 1° de l'article L. 163-3 et au 1° de l'article L. 163-4* ».

Il s'agit, notamment, de réprimer le recours à des logiciels de fabrication de faux numéros de cartes de paiement ou de piratage de ceux-ci à l'occasion d'une transaction sur Internet, qui sont ensuite exploités frauduleusement ou mis à la disposition du public sur des sites spécialisés dits de « *carding* ».

- **la fraude informatique proprement dite**

Le projet de loi pour la confiance dans l'économie numérique[35], tel qu'adopté en première lecture par le Sénat, prévoit la création d'un nouveau délit, en insérant un nouvel article 323-3-1 dans le code pénal à la suite des articles prévoyant l'incrimination des divers cas de fraude informatique :

« *Art. 323-3-1. - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

L'objectif du législateur est de pouvoir incriminer détenteurs ou fabricants de virus informatiques.

- **le contournement des mesures techniques de protection des œuvres**

L'article 13 du projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information portant transposition de la directive 2001/29 du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[36] prévoit qu'est assimilé à un délit de contrefaçon :

« *1° Le fait pour une personne de porter atteinte, en connaissance de cause, à une mesure technique mentionnée à l'article L. 331-5 afin d'altérer la protection, assurée par cette mesure, portant sur une œuvre ;*
*2° Le fait, en connaissance de cause, de fabriquer ou d'importer une application technologique, un dispositif ou un composant ou de fournir un service, destinés à faciliter ou à permettre la réalisation, en tout ou en partie, du fait mentionné au 1° ci-dessus ;*

[33] La contrefaçon des cartes de paiement est réprimée par l'article L 163-3 et l'article L 163-4 1°du Code pénal.
[34] Inséré par Loi nº 2001-1062 du 15 novembre 2001 art. 40 Journal Officiel du 16 novembre 2001.
[35] Les travaux préparatoires sont disponibles à l'URL : <http://www.assemblee-nationale.fr/12/dossiers/economie_numerique.asp>.
[36] Voir : <http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/auteursi.htm>.

*3° Le fait, en connaissance de cause, de détenir en vue de la vente, du prêt ou de la location, d'offrir à la vente, au prêt ou à la location, de mettre à disposition sous quelque forme que ce soit une application technologique, un dispositif ou un composant ou de fournir un service destinés à faciliter ou à permettre la réalisation, en tout ou en partie, du fait mentionné au 1° ci-dessus ;*
*4° Le fait, en connaissance de cause, de commander, de concevoir, d'organiser, de reproduire, de distribuer ou de diffuser une publicité, de faire connaître, directement ou indirectement, une application technologique, un dispositif, un composant ou un service destinés à faciliter ou à permettre la réalisation, en tout ou en partie, de l'un des faits mentionnés au 1° ou au 2° ci-dessus* ».

Ce projet a été présenté en Conseil des Ministres le 12 novembre 2003.

Partant du constat que le piratage est facilité dans un environnement numérique, les titulaires de droit d'auteur craignent de ne plus percevoir la rémunération qui leur est due. D'où l'idée de mettre en place des dispositifs techniques de protection des œuvres (systèmes anti-copie, systèmes de contrôle d'accès, certification et marquage des œuvres, recours à la cryptographie etc.).

Ces mesures techniques de protection des œuvres font elles-mêmes l'objet d'une protection par le droit[37].

L'article 6.1 de la directive dite DAVSI du 22 mai 2001[38] dispose que les Etats membres doivent prévoir une protection juridique appropriée contre le contournement de toute mesure technique efficace.

Ces dispositions découlent de l'article 11 du traité OMPI en date du 20 décembre 1996 sur le droit d'auteur.

Aux Etats-Unis, la loi dite " *Digital Millenium Copyright Act* " a été définitivement adoptée le 28 octobre 199839. Cette loi contient également des dispositions spécifiques sur la protection des mesures techniques : la neutralisation des mesures techniques qui contrôlent l'accès à une œuvre est sanctionnée, de même que la commercialisation de dispositifs permettant la neutralisation et les actes et activités préparatoires.

L'objectif de ces différentes dispositions est de sanctionner les divers fournisseurs de moyens qui peuvent faciliter à des tiers l'accès non autorisé ou le maintien indu dans des systèmes informatiques, entendus au sens large. Pour ce faire, on réprime de façon très vaste le fait *« d'offrir, de céder ou de mettre à disposition* », des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions de contrefaçon de cartes bancaires, de fraude informatique, de contournement des mesures techniques de protection des œuvres.

Certains auteurs saluent cette volonté du législateur de prévenir ainsi les actes d'accès indus en réprimant de façon autonome la complicité par fourniture de moyens[40].

En soi, cet objectif est parfaitement légitime.

Cependant, on peut s'interroger sur la question de savoir s'il y a proportionnalité entre les objectifs poursuivis et les actes incriminés dans les projets de loi en cours d'adoption.

### 2.2.2. Les revers de l'incrimination autonome de la fourniture de moyens

---

[37] Guillaume Gomis, « Réflexions sur l'impact des mesures techniques de protection des oeuvres », *Bulletin Lamy droit de l'informatique et des réseaux*, oct. 2003, n° 162 et *Juriscom.net* : <http://www.juriscom.net/pro/visu.php?ID=78>.
[38] Directive n° 2001/29/CE du 22 mai 2001, JOCE 22 juin n° L 167/10 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[39] Le texte complet du DMCA peut être consulté depuis le site web du Copyright Office américain à l'adresse : <http://lcweb.loc.gov/copyright/>.
[40] Christian Le Stanc, préc.

Nous allons examiner les interrogations soulevées par les dispositions du projet de loi sur l'économie numérique et du projet de loi sur le droit d'auteur, au regard des objectifs de sécurité des systèmes d'information.

**a) L'élargissement des incriminations en matière de fraude informatique**

En matière de sécurité informatique, les mêmes outils peuvent être utilisés à des fins malveillantes ou à des fins légitimes, en vue de tester la sécurité des systèmes d'information. Les outils d'analyse de la sécurité sont parfois les mêmes que les outils servant à commettre une attaque.

La création d'une nouvelle incrimination en droit pénal de l'informatique, vise selon le rapporteur pour avis devant la Commission des lois de l'Assemblée Nationale, à pouvoir incriminer les détenteurs ou les fabricants de virus informatiques[41].

Le projet de loi du gouvernement prévoyait que les sanctions pénales ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition sont « *justifiés par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communication électronique et des systèmes d'information* ».

Cette exclusion du champ d'application de la sanction pénale a pour objectifs de permettre aux laboratoires scientifiques en informatique, de poursuivre leurs travaux en ce domaine et pour les sociétés chargées de concevoir des programmes informatiques de veille, de sécurisation ou de défense des systèmes informatiques, de concevoir des virus afin de tester la fiabilité de leur propre programme anti-virus.

Comme le souligne le rapporteur : « *il est quelque peu curieux de prévoir une irresponsabilité pénale absolue pour des organismes ou des personnes physiques qui ont détenu ou conçu des programmes « spécialement adaptés » pour commettre une infraction* »

Le champ de l'exclusion pénale proposée lui paraissait également trop large.

En effet, les notions de « *besoins de la recherche scientifique et technique* » ou de « *protection et de la sécurité des réseaux de communication* » sont particulièrement imprécises.

C'est pourquoi, afin de renforcer les garanties juridiques quant au bon usage des virus informatiques, il semblait préférable au rapporteur de prévoir que les organismes, publics et privés, qui sont habilités à mettre en œuvre de tels programmes informatiques, procèdent préalablement à une déclaration auprès des services du Premier ministre.

Le texte adopté en première lecture par l'Assemblée Nationale prévoyait dès lors :

« *Art. 323-3-1. - Le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre les faits prévus par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée*.
« *Les dispositions du présent article ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition de l'instrument, du programme informatique ou de toute donnée sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information et lorsqu'elles sont mises en œuvre par des organismes publics ou privés ayant procédé à une déclaration préalable auprès du Premier ministre selon les modalités prévues par les dispositions du III de l'article 18 de la loi n° du pour la confiance dans l'économie numérique*. »

Autant pour le volet diminution de la bureaucratie et simplification des mesures administratives.

[41] Rapport pour avis de Madame Tabarot, député, pour la Commission des lois, en ligne à l'URL : <http://www.assemblee-nationale.fr/12/rapports/r0608.asp>.

Toutefois, la nouvelle incrimination ainsi créée ne s'applique pas, contrairement à ce que semble croire le législateur, à la seule fabrication de virus informatiques, mais à tout programme informatique conçu ou spécialement adapté pour commettre une infraction dite de fraude informatique[42].

Ainsi, l'utilisation de tout logiciel destiné à réaliser un test d'intrusion risquerait de tomber dans le champ de l'incrimination.

Les spécialistes de la sécurité des systèmes d'information s'en sont émus, soulignant que leurs activités risquaient d'être mises en péril[43].
D'autres craignent au contraire que le simple fait d'invoquer un objectif de recherche scientifique soit une « excuse en or » pour les pirates.

Pour le Sénat[44], la solution proposée par l'Assemblée nationale pourrait susciter de sérieuses difficultés d'application. Le texte proposé par l'Assemblée nationale pourrait en effet exposer des organismes détenant des virus à des fins de recherche à des poursuites si elles omettaient de procéder à la déclaration tout en utilisant les virus à des fins légitimes.

Le Sénat a donc introduit l'exception de « motif légitime », qu'il reviendrait au juge d'apprécier.

Cette exception permettrait davantage que la solution proposée en première lecture par l'Assemblée nationale de préserver les activités de recherches et de prestations de service en matière de sécurité des systèmes d'information.

Cependant, il peut paraître tout aussi curieux de prévoir que des dispositifs destinés à commettre une infraction pénale puissent être détenus à des fins légitimes.

Nous ignorons encore la rédaction définitive de ce texte qui sera adoptée par les parlementaires, le projet devant revenir en seconde lecture avant son adoption définitive.

Il reste que ces débats parlementaires soulignent bien que légiférer sur la sécurité informatique peut s'avérer un art délicat : en voulant élargir l'efficacité de la sanction pénale contre les fraudeurs, on risque dans le même temps d'incriminer des actes destinés à la prévention de la fraude informatique et à l'amélioration de la sécurité des systèmes d'information.

**b) Le projet de loi sur le droit d'auteur : la création d'un nouveau délit d'aide au contournement des mesures techniques de protection des œuvres**

La directive sur le droit d'auteur et les travaux de transposition font l'objet de nombreux débats. Nous nous limiterons aux questions susceptibles d'avoir un impact sur les activités liées à la sécurité des systèmes d'information.

La question de savoir comment élargir la sanction pénale aux actes de fourniture de moyens sans faire tomber sous le coup de l'incrimination des activités légitimes liées à la sécurité des systèmes d'information n'a pas été prise en compte par les rédacteurs du projet de loi de transposition de la directive sur le droit d'auteur.

Le projet incrimine non seulement la fabrication ou la mise à disposition de moyens destinés à contourner une mesure technique de protection, mais également, d'une manière plus générale « *le fait de faire connaître, directement ou indirectement, une application technologique, un dispositif, un composant ou un service destinés à faciliter ou à permettre la réalisation, en tout ou partie, de l'un des faits mentionnés au 1° ou au 2° ci-dessus* », à savoir le fait de contourner une mesure technique de

[42] Force est de constater que le législateur semble avoir une conception très étroite de la sécurité informatique.
[43] Christophe Guillemin, « Des experts en sécurité critiquent un article du projet de loi pour la confiance dans l'économie numérique », 17 janvier 2002, *Zdnet.fr :*
<http://www.zdnet.fr/actualites/technologie/0,39020809,2128896,00.htm>.
[44] Avis de Monsieur Alex Türk, au nom de la commission des lois, n° 351, 11 juin 2003, en ligne à l'URL :
<http://www.senat.fr/rap/a02-351/a02-351.html>.

protection ou le fait de fabriquer une application, un dispositif, un composant destinés à permettre le contournement d'une mesure technique.

Quel est le rapport entre ces dispositions et la sécurité informatique ?

Le contournement d'une mesure technique de protection d'une œuvre s'analyse également en un accès frauduleux à un système de données automatisé[45], compte tenu de l'acceptation très large de la notion de système automatisé de données. Dès lors, l'impact de ces dispositions concerne tout le secteur de la sécurité de l'information au sens large.

Or, le fait d'assimiler à un délit de contrefaçon le fait de faire connaître, directement ou indirectement, toute application, dispositif, composant, qui pourrait faciliter, en tout ou partie, la réalisation de dispositifs de contournement, fait planer une incertitude juridique sur la seule publication d'informations sur des failles de sécurité, pour peu que le dispositif de sécurité critiqué soit utilisé comme moyen de protection d'une œuvre.

Ainsi, sur le fondement des dispositions anticontournement du *Digital Millennium Copyright Act* de 1998[46], un professeur de l'Université de Priceton, M. Felten, a été menacé de procès par le *SMDI, Secure Digital Music Intiative*, un consortium d'industriels, et la *RIAA (Recording Industry Association of Americ*a), s'il dévoilait dans une conférence scientifique les vulnérabilités techniques d'un système de protection des œuvres par marquage (*watermarketing*) dont le *SMDI* avait voulu faire tester la fiabilité en lançant un concours.

Après avoir été portée devant les tribunaux, l'affaire a fait l'objet d'un désistement, après que le gouvernement a indiqué que les dispositions du *DMCA* n'avaient pas vocation à s'appliquer aux chercheurs[47].

Comme le souligne le Professeur Pamela Samuelson : « *the DMCA is a cloud on the horizon for all computer security and encryption researchers, whether they operate in an academic or commercial setting, if their work has any potential appplication to protecting digital content* »[48].

Des propos parfaitement transposables au projet de loi de transposition de la directive.

Selon l'*Electronic Frontier Fondation*, une association américaine de défense des libertés, par crainte de poursuites judiciaires, des chercheurs auraient cessé de publier les détails de leurs travaux sur des protocoles de sécurité. Elle cite dans un rapport « *Unintended consequences : four years under the DMCA* » différentes affaires mettant en cause la recherche scientifique et la liberté d'expression sur le fondement des dispositions anti-contournement du *DMCA*[49]. Il ne semble pas toutefois qu'à ce jour les tribunaux américains aient jugé inconstitutionnelles les dispositions critiquées du *DMCA*.

Ces exemples venus d'outre-atlantique nous permettent de nous interroger : fait-on avancer la sécurité informatique en prohibant la publication des informations relatives aux vulnérabilités de certains dispositifs ?

La publication d'informations sur les failles de sécurité n'est pas une activité illicite pratiquée par les seuls pirates en tout genre, mais une démarche destinée à avertir les organismes utilisateurs et éditeurs de programmes informatiques des vulnérabilités susceptibles de mettre en cause la sécurité des systèmes informatiques. La publication de ces failles est généralement accompagnée des

---

[45] Voir : Isabelle Vaillant, « Le contournement des mesures techniques de protection, contrefaçon ou criminalité informatique », juin 2003, rapport rédigé pour l'initiative EUCD.INFO, <http://eucd.info/pr-2003-06-21.fr.php>.
[46] Voir : <http://www.loc.gov/copyright/legislation/dmca.pdf>.
[47] Aff. Felten / RIAA. Voir sur cette affaire le dossier de l'EFF, à l'URL : <http://www.eff.org/IP/DMCA/Felten_v_RIAA/>.
[48] Pamela Samuelson, « Anticircumvention rules : threat to science », *Computers and Science*, vol. 293 Science p. 2028, 14 septembre 2001, voir : <http://www.law.upenn.edu/law619/f2001/week09/samuelson_dmca.pdf>.
[49] Voir : <http://www.eff.org/IP/DRM/DMCA/20031003_unintended_cons.php>.

moyens d'y remédier. A titre d'exemple, en France, le *CERTA*, Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques, une structure dépendant de la *DCSSI*, Direction Centrale de la Sécurité des Systèmes d'Information, et chargée d'une mission de veille et de réponse aux attaques informatiques, publie régulièrement des alertes de sécurité, la dernière en date du 6 octobre 2003 concernant une vulnérabilité d'Internet Explorer[50].

Il faut également souligner que le projet de loi sur le droit d'auteur va beaucoup plus loin que la directive, rédigée en des termes beaucoup plus restrictifs quant aux actes à incriminer.

L'article 6.2 de la directive indique :

« *Les États membres prévoient une protection juridique appropriée contre la fabrication, l'importation, la distribution, la vente, la location, la publicité en vue de la vente ou de la location, ou la possession à des fins commerciales de dispositifs, produits ou composants ou la prestation de services qui :*
*a) font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de contourner la protection, ou*
*b) n'ont qu'un but commercial limité ou une utilisation limitée autre que de contourner la protection, ou*
*c) sont principalement conçus, produits, adaptés ou réalisés dans le but de permettre ou de faciliter le contournement de la protection de toute mesure technique efficace* ».

Les dispositions de la directive soulèvent également des interrogations, notamment sur la portée de la notion de « *principalement conçus* ». A titre d'exemple, certains outils sont utilisés en matière d'audit de sécurité pour détecter les erreurs de programmation (« *debuggers* »). Ces outils, qui peuvent permettre de passer outre les mesures de protection, peuvent-ils être considérés comme « *principalement adaptés* » pour détourner les protections [51]?

En tout état de cause, le projet de loi de transposition ne s'embarrasse même pas de ces nuances, puisqu'il est prévu qu'il suffit que le moyen permette en partie de contourner une mesure de protection pour que l'élément matériel du délit soit constitué (nouvel article L 335-3-1 du Code de la propriété intellectuelle, 1°, 2° et 3°).

Ne devrait-on pas incriminer les seules personnes qui créent des logiciels dans le seul but de contourner une protection, sans faire planer l'incertitude juridique sur d'autres types de développement ou d'actions (sécurité, interopérabilité, intégration de logiciels) dont les objectifs sont légitimes ?

Le texte en son état n'envisage aucune exception pour les activités de recherche scientifique ou de protection de la sécurité des systèmes d'information, à la différence du projet de loi pour l'économie numérique. Il ne vise pas uniquement, comme en matière de contrefaçon de cartes de paiement ou de fraude informatique, la mise à disposition de données, équipements, programmes informatiques « *conçus ou spécialement adaptés* » pour commettre les infractions visées, mais le seul fait de « *faciliter* » ou de permettre la réalisation, « *en tout ou partie* », d'un acte de contournement d'un dispositif de protection, par des moyens aussi vagues que « *la mise à disposition sous quelque forme que ce soit* », ou encore le fait de faire « *connaître, directement ou indirectement* ».

Le fait d'avoir précisé dans le projet que ces actes doivent être réalisés « *en connaissance de cause* » ne suffit pas à lever l'incertitude juridique quant à l'étendue des actes incriminés.

On peut se demander si le projet ne porte pas atteinte au principe constitutionnel de légalité des peines et délits, dont il résulte la nécessité pour le législateur de définir les infractions en termes suffisamment clairs et précis pour exclure l'arbitraire, et le principe selon lequel la loi ne doit établir que des peines strictement et évidemment nécessaires[52]. Un texte pénal ne doit pas être imprécis et

[50] Voir : <http://www.certa.ssi.gouv.fr/>.
[51] Magali Julin, « Les extensions au droit d'auteur : une menace pour les logiciels libres ? », rapport de stage du DESS de droit public des nouvelles technologies et systèmes d'information, Paris X, mai 2002, p. 32 et s., en ligne à l'URL : <http://www.vilya.org/dcssi/>.
[52] Conseil constitutionnel, Décision n° 80-127 DC des 19 et 20 janvier 1981.

ambigu, conditions que ne semble pas remplir l'incrimination du « *fait de faire connaître directement ou indirectement* ».

Il nous paraît essentiel que les travaux parlementaires de transposition de la directive prennent en compte la nécessité de trouver un juste équilibre entre la lutte anti-piratage et la protection des intérêts légitimes de recherche scientifique et technique ou de protection de la sécurité des systèmes d'information, équilibre que ne concilie pas le projet de loi en son état. Pourtant, nos parlementaires sont à la recherche d'un tel équilibre dans le projet de loi sur l'économie numérique.

Dans ce débat sur la politique législative de lutte contre la fraude informatique, tout le monde est de près ou de loin concerné, du *hacker*[53], au spécialiste de la sécurité informatique, en passant par l'organisme utilisateur coupable d'avoir insuffisamment sécurisé ses données. Tout le monde, enfin presque. Nous allions oublier l'éditeur de programmes informatiques.

## 3. Failles de sécurité : faut-il blâmer les éditeurs de logiciel ?

### 3.1. Un constat : l'absence de responsabilité en matière de programmes informatiques

Un mouvement commence à dénoncer le fait que **l'industrie de l'informatique ne prend pas suffisamment en compte la qualité de ses produits, et que le modèle de qualité de cette industrie est différent de celui des autres industries**[54]. Les fournisseurs informatiques ne semblent encourir aucune responsabilité lorsque leurs produits sont défectueux. On ironise sur le fait que les programmes « tombent en marche », et on regrette que les éditeurs lancent sur le marché des logiciels qui n'ont pas été suffisamment testés. On considère aujourd'hui comme une fatalité que les systèmes informatiques comportent une part irréductible d'erreurs, des « *bugs* », qui peuvent engendrer des anomalies dans les traitements effectués[55].

Prenons l'exemple de la signature électronique consacrée par la loi n° 2000-230 du 13 mars 2000.

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, laquelle doit remplir deux conditions :

- Etre établie grâce à un *dispositif sécurisé de création de signature électronique* ;
- La vérification de cette signature doit reposer sur l'utilisation d'un *certificat électronique qualifié*[56].

Or, si la directive et le projet de loi de transposition de cette directive[57] ont bien traité le cas de la responsabilité du prestataire de services de certification électronique, la responsabilité du fournisseur du dispositif de création de la signature électronique n'a été envisagée ni par le législateur français, ni par le législateur européen. Cette responsabilité ressortira entièrement du domaine contractuel.

Nous avions expliqué dans un précédent article que les clauses limitatives ou exclusives de responsabilité sont des clauses standard des licences de logiciel et qu'il est difficile d'engager la responsabilité d'un éditeur en raison du défaut de qualité de ses logiciels, même si le droit commun de la responsabilité civile a vocation à s'appliquer[58].

---

[53] Employé ici au sens de personne qui aime disséquer, comprendre un système d'information, et non au sens de « *cracker* », qui est une personne animée uniquement par l'intention de découvrir des données confidentielles. Voir The Jargon Dictionary : <http://info.astrian.net/jargon/terms/h.html#hacker>.

[54] Bruce Schneier, « Secrets et mensonges – Sécurité numérique dans un monde en réseau », éditions *Vuibert Informatique*, p. 374 ; Jean-Pierre Corniou, « La complexité créée par les éditeurs détruit de la valeur », *Le Monde Informatique* n° 927, 22 février 2002 ;

[55] Valérie Sédallian, « Les engagements des prestataires informatiques », *Cahiers Lamy droit de l'informatique et des réseaux*, octobre 2001, n° 140, p. 11 ; *Juriscom.net* : <http://www.juriscom.net/pro/2/cta20011002.htm>.

[56] Article 1316-4 du Code civil ; décret n° 2001-272 du 30 mars 2001, article 2.

[57] Article 21 du projet de loi pour la confiance dans l'économie numérique, voir : <http://www.assemblee-nationale.fr/12/dossiers/economie_numerique.asp>.

[58] Valérie Sédallian, « Garanties et Responsabilités dans les logiciels libres », septembre 2002, *Juriscom.net* : <http://www.juriscom.net/pro/2/da20020901.htm> et *Cahiers Lamy droit de l'informatique et des réseaux,* novembre 2002, n° 152.

Il est vrai que le logiciel n'est pas un produit comme les autres en raison de sa nature immatérielle et compte tenu du fait qu'il est destiné à interagir avec d'autres logiciels et matériels.

Si l'on part de l'équation :

> obligation de moyens + clauses limitatives ou exclusives de responsabilité + constat de la complexité des logiciels

on aboutit au résultat suivant : les éditeurs de logiciels ne sont pas responsables des failles de sécurité.

Comme le souligne Cyril Voisin, chef de programme sécurité de *Microsoft France* :

« *Les logiciels sont créés par des hommes et des femmes. L'erreur étant humaine, les logiciels comportent des erreurs, appelés "bogues" dont certains touchent à la sécurité* »[59].

A cet égard, lorsqu'une vulnérabilité est découverte, la seule obligation des éditeurs semble se limiter à la publication d'un correctif ou d'un « patch », qu'il appartient à l'utilisateur de se procurer et d'appliquer. Ledit utilisateur pouvant être un organisme possédant un système informatique en réseau composé de centaines, voire de milliers d'ordinateurs.

Ainsi, si un utilisateur est victime d'un virus, il peut s'en prendre à lui-même (manquement à l'obligation de sécurité si ledit virus a endommagé des données personnelles) ou au pirate qui a fabriqué ou diffusé le virus.

En revanche, son recours contre l'éditeur reste en l'état de la législation et de la jurisprudence, très aléatoire, voire une fiction juridique.

Fin de la démonstration et fin du débat ?

### 3.2. Une lacune qui commence à être dénoncée

Pourtant, la malveillance tire parti des défauts des programmes informatiques[60].

Comme le souligne le Professeur Lawrence Lessig :

« W*ere contract law not so eager to allow liability in economic transactions to be waived, the licences that absolved the code writers of any potential liability from bad code would not have induced an even greater laxity in what these code writers were producing*[61]. »

Ainsi, suite à la vague de virus qui se sont propagés pendant l'été 2003, il a été reconnu que le virus Blaster était dû à une erreur de programmation lors de son implémentation dans les produits *Microsoft* qui n'avait pas été détectée[62].

Les spécialistes de la sécurité informatique commencent à souligner que les éditeurs de logiciels devraient être soumis aux mêmes responsabilités du fait du défaut de leurs produits que les autres industries[63].

---

[59] Jean-Philippe Gaulier, « Les logiciels sont créés par les hommes et l'erreur est humaine... », 6 octobre 2003, *Transfert.net* : <http://www.transfert.net/a9390>.
[60] Jim Landers, « As Threat of Cyber Attacks Grows, Security Specialists blame faulty software », *Newsfactor.com*, 21 août 2002, <http://www.newsfactor.com/perl/story/19104.html>.
[61] Lawrence Lessig, « Code and other laws of cyberspace », *Basic Books*, 1999, p. 232.
[62] Jean-Philippe Gaulier, préc.
[63] Elinor Mills Abreu, « Le logiciel est-il un produit ou un service ? », *Reuters*, 16 juin 2002.

Pour Russ Cooper, l'éditeur de la liste de diffusion NTBugtraq, dédiée aux discussions sur les problèmes de sécurité dans les systèmes d'exploitation Windows[64], « *les éditeurs devraient davantage assumer la responsabilité de leurs failles*[65] ».

Allant plus loin, Bruce Schneier, auteur de « Secrets et mensonges – Sécurité numérique dans un monde en réseau »[66], considère que les éditeurs ne prendront pas la peine de concevoir des produits sûrs en l'absence de contrainte légale : « *security is poor because vendors are not held responsible* [67]». Pour lui, le seul moyen d'inciter les vendeurs de logiciels à s'intéresser davantage à la qualité de leurs produits est de les tenir pour responsables des vulnérabilités de sécurité de leurs produits.

Dans un rapport publié en janvier 2002 intitulé : « *Cybersecurity Today et Tomorrow* », l'Académie Nationale des Sciences, un organisme consultatif du gouvernement américain, invite le législateur à réfléchir à une réglementation visant à augmenter la responsabilité des vendeurs de logiciels et de systèmes pour les défauts de sécurité, entre autres mesures destinées à améliorer la sécurité informatique [68].

### 3.3. Un débat prématuré ?

On s'en serait douté, l'industrie américaine des nouvelles technologies est d'un tout autre avis. Pour Harris Miller, Président de l'*Information Technology Association of America*, cette vision est réductrice : le développement de logiciels est un processus complexe opéré dans un environnement technique et commercial en constante évolution. Faire peser une telle responsabilité sur les éditeurs porterait atteinte à l'innovation et entraverait la compétitivité des entreprises américaines. Il faut laisser faire le marché et ne pas se tromper de cible : les fautifs sont les auteurs des délits de fraude informatique. On ne peut pas légiférer sur la qualité, la productivité ou l'innovation[69].

Pour l'heure, aucun projet de nature à inquiéter les éditeurs de logiciel n'est à l'ordre du jour[70].

Il est vrai que légiférer sur un tel sujet, indépendamment des aspects économiques, risquerait d'être un vrai casse-tête.

Cependant, en octobre 2003, un recours collectif (*class action suit*) était déposé dans l'Etat de Californie à l'encontre de la société *Microsoft*, à la demande d'une résidente californienne à la suite du vol sur son ordinateur de ses données personnelles par un pirate ayant exploité les failles de sécurité des logiciels de *Microsoft*. Cette plainte vise la vulnérabilité du système d'exploitation Windows aux attaques virales[71]. Il est encore beaucoup trop tôt pour savoir si ce recours collectif sera jugé recevable et bien fondé. Il relance en tout état de cause le débat sur la responsabilité des éditeurs sur la sécurité informatique.

En France, une question pourrait éventuellement être soumise un jour aux tribunaux, celle de savoir si la responsabilité du fait des produits défectueux est applicable à un logiciel à l'origine d'une atteinte à la sécurité des personnes.

---

[64] Voir : <http://www.ntbugtraq.com/>.
[65] Russ Cooper, « Les éditeurs devraient davantage assumer la responsabilité de leurs failles », propos recueillis par François Morel, *JDNet*, 16 novembre 2001, <http://solutions.journaldunet.com/itws/011116_it_ntbugtraq_cooper.shtml>.
[66] Editions *Vuibert Informatique, 2000.*
[67] Bruce Schneier, « Security is poor because vendors are not held responsable », 22 avril 2002, *NetworkWorldFusion* : <http://www.nwfusion.com/columnists/2002/0422faceoffyes.html>.
[68] Voir : <http://books.nap.edu/html/cybersecurity/>.
[69] Harris Miller, « Penalizing vendors brings consequences », 22 avril 2002, *NetworkWorldFusion* : <http://www.nwfusion.com/columnists/2002/0422faceoffno.html>.
[70] Robert Lemos, « le plan Bush sur la cybersécurité n'emballe pas les spécialistes », 20 septembre 2002, *Zdnet.fr,* http://www.zdnet.fr/actualites/technologie/0,39020809,2122626,00.htm>.
[71] Kevin Krolicki et Reed Stevenson, « Microsoft attaqué sur la vulnérabilité de Windows aux virus », Reuters, 3 octobre 2003 : <http://fr.biz.yahoo.com/031003/85/3fcr4.html>.

Une directive du 25 juillet 1985 sur la responsabilité du fait des produits défectueux prévoit une protection du consommateur contre les produits défectueux. Elle prévoit le principe d'un régime de responsabilité sans faute des fabricants et distributeurs dès lors qu'un produit fini cause des dommages corporels ou matériels du fait d'un défaut. Cette directive a été transposée par une loi du 19 mai 1998 dans les articles 1386-1 à 1386-18 du Code civil. Un produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre. Dans ce régime, les clauses limitatives de responsabilité sont réputées non écrites, sauf si elles sont stipulées entre professionnels et ne concernent que des dommages causés aux biens qui ne sont pas utilisés principalement pour la consommation privée.

La Commission européenne a déclaré que la directive s'appliquait au logiciel[72].

On considère aujourd'hui que les cas d'application à des logiciels devraient être exceptionnels.
Ainsi, en réponse à une question parlementaire, la Ministre de la Justice a répondu que « *les seuls dommages dont ladite loi assure la réparation sont les atteintes physiques à la personne et les dommages matériels causés aux biens. L'application de ce texte aux logiciels ne vise donc que les situations où ceux-ci seraient à l'origine directe d'une atteinte à la sécurité des personnes ou des biens, hypothèses pour le moins résiduelles*[73]».

Il est également possible d'invoquer l'article 1386-11 dernier alinéa qui prévoit que « *le producteur de la partie composante n'est pas non plus responsable s'il établit que le défaut est imputable à la conception du produit dans lequel cette partie a été incorporée ou aux instructions données par le producteur de ce produit*».

Pourtant, il est des situations où un logiciel s'intègre dans un système qui concerne directement la sécurité des personnes : pilotage d'une centrale nucléaire, d'un appareil médical, d'un avion…

A l'heure où l'informatique est omniprésente, est-il certain que les hypothèses où le défaut d'un logiciel met en danger la sécurité des personnes resteront résiduelles ?

Il est vrai que nous quittons là le terrain de la sécurité informatique pour aborder celui de la sécurité des personnes.

En conclusion, il est beaucoup plus facile d'augmenter les peines encourues par les auteurs d'actes de fraude informatique que d'obliger les entreprises à garantir la sécurité de leur système informatique, ou même imaginer faire peser un début de responsabilité sur les fournisseurs de logiciels.

Une citation de Bruce Schneier semble bien résumer la situation actuelle en matière de politique législative :
« *Les lois n'augmentent pas la sécurité des systèmes, ou évitent que les attaquants trouvent des trous. Leur rôle est de permettre à des fabricants de produits de se dissimuler derrière une sécurité imprécise, blâmant les autres pour leur propre inaptitude. Il est certainement plus simple d'implémenter de la mauvaise sécurité et de rendre hors la loi tous ceux qui le font remarquer que d'implémenter de la bonne sécurité*[74] ».

On rétorquera avec justesse qu'on ne peut pas mettre sur le même plan d'une part, les responsabilités pénales encourues par les auteurs d'actes répréhensibles, et d'autre part, les responsabilités qu'il conviendrait de faire peser sur les utilisateurs et les fournisseurs.

Force est de constater toutefois que si la sécurité est l'affaire de tous, la législation traite dans ce domaine avec plus de rigueur l'utilisateur que son fournisseur.

---

[72] Rép. Min. 15 novembre 1988, JOCE 8 mai 1989, C 144 p. 42.
[73] Rép. Min. n° 15677, JOANQ 24 août 1998, <http://www.questions.assemblee-nationale.fr/>.
[74] Bruce Schneier, « Secrets et mensonges, Sécurité numérique dans un monde en réseau », *Vuibert Informatique*, 2001, p. 355.

Les textes applicables peuvent paraître incohérents entre eux : le manquement à l'obligation de sécurité est lourdement sanctionné, mais démontrer qu'un système est mal sécurisé est un délit pénal. Quant au législateur, en voulant permettre une répression plus efficace de la mise à disposition des outils qui permettent la fabrication de virus ou le piratage d'œuvres protégées par des mesures techniques, il prend le risque de faire planer l'incertitude juridique sur des actes parfaitement dénués de toute intention frauduleuse et visant à améliorer la sécurité des systèmes informatiques.

L'action législative doit prendre plus de recul et avoir une vision d'ensemble cohérente.

V.S.