Le droit des obligations de sécurité informatique

Amory, Bernard

Published in:
Securicom 87

Publication date:
1987

Document Version
le PDF de l'éditeur

LE DROIT DES OBLIGATIONS DE SECURITE INFORMATIQUE

LIABILITIES IN RESPECT OF COMPUTER SECURITY

Bernard E. Amory*

Abstract: Since companies are becoming more and more dependent upon their computer systems, any malfunctioning or failure of the latter can result in a disaster for the company's business. Numerous types of means of security are available to minimize the risks of failure and, when it happens, the consequences. From a legal standpoint, these means of security are imposed on the various parties involved by virtue of general principles of law, specific statutes and contracts. This paper will examine (i) what are the legal obligations in respect of computer security; (ii) who is responsible for them and (iii) what are the civil, criminal and administratative sanctions in the event of non-compliance.

* Assistant à la Faculté de Droit de Namur
Membre du Cabinet juridique Dechert Price & Rhoads,
Avenue Louise 250 Bte 114
1050 Bruxelles
Belgique

Introduction

Les entreprises deviennent de plus en plus dépendantes de l'informatique. Ceci est d'autant plus vrai que les applications informatiques, autrefois réduites à quelques fonctions autour d'un seul ordinateur, se sont étendues grâce à la télématique, à des systèmes d'information répartie et sont fondés sur une utilisation beaucoup plus massive de l'information à tous les niveaux (1). Un problème dans le fonctionnement des systèmes informatiques peut résulter en une véritable catastrophe pour l'entreprise. Une compagnie d'assurances américaine a affirmé que 80% des grandes entreprises ne pouvaient survivrent à une catastrophe informatique (2).

Heureusement, il existe de nombreux moyens d'assurer la sécurité informatique. D'un point de vue juridique, il importe de déterminer quelles sont les obligations en matière de sécurité et de savoir sur qui elles reposent, tâche compliquée en raison du grand nombre de personnes impliquées dans l'installation et le fonctionnement des systèmes informatiques; enfin, il est intéressant de connaître quelles sont les sanctions éventuelles, de nature civile, pénale ou administrative, qui seraient appliquées en cas de violation desdites obligations.

Le présent exposé tentera d'abord de définir ce qu'est une obligation de sécurité. Ensuite seront successivement examinées les obligations résultant de dispositions juridiques générales, celles résultant de lois particulières et enfin les obligations de nature contractuelle.

---

(1) Cf. Yves Poullet, Droit et sécurité informatique: le management juridique de la sécurité du système informatique, Texte d'une conférence donnée pour l'Institut des Reviseurs d'Entreprises le 13 décembre 1985.

(2) Cf. Proceedings of the AEAI/RIMS International Risk Management Conference, October 6-9, 1985, Monte Carlo.

1. Qu'est-ce qu'une obligation de sécurité ?

Par sécurité d'un système informatique, au sens large, on entend diverses qualités qu'il importe de distinguer (1):

- la fiabilité: un système est réputé fiable dans la mesure où les résultats qu'il génère sont identiques aux résultats attendus sur base des spécifications. Ceci suppose, d'une part, l'intégrité des données, leur non-déformation lors de l'introduction, pendant leur stockage et lors de leur utilisation, et d'autre part la fiabilité des opérations , c'est-à-dire que la qualité des résultats effectifs suite au traitement soit précisément celle attendue du traitement.

- la confidentialité du traitement et des informations. Il s'agit ici de protéger le système contre toute fuite ou sortie indésirée de programme ou d'informations.

- la continuité permet de maintenir le système à tout moment de sa vie conforme aux nécessités de l'utilisateur; ceci implique non seulement des activités de prévention et d'intervention en cas d'incidents, mais également des activités d'adaptation du système à des besoins nouveaux (par exemple des adaptations d'un logiciel comptable nécessitées par une modification de la réglementation comptable).

- la conformité du système avec les réglementations relatives à la sécurité des tiers, notamment les réglementations en matière de sécurité électrique et de connection aux réseaux publics de télécommunications.

L'obligation n'est pas entendue ici dans son sens strict du droit civil comme découlant soit d'un contrat, soit des règles régissant la responsabilité civile. La notion est entendue dans un sens plus large comprenant toutes les exigences nécesaires à assurer la sécurité informatique telle que définie ci-avant et découlant non seulement des dispositions générales du Code Civil, mais aussi des lois et réglementations particulières, voire des codes de bonne conduite professionnelle.

---

(1) Cf. Yves Poullet, op. cit. et Anne Finet, Data Center Protection - Definition of Risk and Technical Parade, AEIA/RIMS Conference, cit. supra.

Le titulaire de l'obligation est déterminé par le texte qui est à la source de celle-ci. On soulignera qu'en matière informatique, la multiplicité des parties impliquées dans la mise en place et le fonctionnement d'un système peut compliquer cette détermination. On recommandera dès lors d'user à ce sujet de la liberté contractuelle prévue par l'article 1134 du Code Civil sans toutefois empiéter sur les dispositions d'ordre public ou impératives. Ainsi, en tant que "professionnel", le fournisseur d'un système de sécurité ne pourra se dégager de la garantie des vices cachés en la reportant sur une autre partie.

2. Les obligations résultant de dispositions générales

Allant du général au particulier, il convient d'abord d'examiner les obligations résultant des principes généraux du droit. Parmi celles-ci, les obligations découlant des règles relatives à la responsabilité civile contenues dans les articles 1382 et. seq. du Code Civil retiendront d'abord notre attention, étant donné leur importance au regard de la sécurité informatique au moment de l'acquisition d'un système et au cours de la vie de celui-ci. Si on se place dans un contexte "télématique" (usage combiné de l'informatique et des télécommunications) permettant la réalisation de certaines opérations à distance comme les transferts électroniques de fonds se pose alors la question de la preuve de ces opérations au regard des dispositions du Code Civil (article 1341) qui sera examinée dans un deuxième paragraphe.

2.1 La responsabilité civile

2.1.1 Lors de l'acquisition d'un système informatique

Rappelons que la responsabilité prévue par les dispositions précitées est de nature purement extra-contractuelle: les obligations qui en résultent ne découlent donc pas du contrat mais de la loi. Lors de l'acquisition d'un système, ces dispositions couvriront toute la phase pré-contractuelle. Pour que cette responsabilité soit mise en oeuvre trois conditions doivent être remplies: une faute, un dommage et un lien causal entre les deux. Dans le chef d'un fournisseur d'un système informatique, la faute pourra être le défaut de renseignement, de conseil ou de mise en garde de l'utilisateur. Il y aurait alors violation d'une obligation de bonne foi contenue dans l'article 1134 du Code Civil. Reste à établir que cette faute a causé un préjudice. Ce préjudice se manifestera dans un défaut de sécurité et les éventuelles conséquences dommageables de celui-ci (par exemple perte de clientèle, coût d'heures supplémentaires prestées par le personnel de l'entreprise).

L'acquéreur supporte lui aussi une obligation de renseignement: celle de formuler ses besoins adéquatement. Une violation de cette obligation par l'acquéreur d'un système informatique entraîne soit une exonération totale de la responsabilité du fournisseur discutée dans le paragraphe précédant, soit un partage de responsabilité (1).

2.1.2 En cours de vie du système

Les détenteurs d'un système informatique peuvent être tenus pour responsables, en vertu de l'article 1384 du Code Civil de tout dommage que ce système pourrait causer à un tiers (par exemple le personnel de l'entreprise, les clients, etc.). L'article 1384 s'applique à celui qui a la "garde de la chose", c'est-à-dire selon la Cour de Cassation belge, celui qui a l'usage, la direction et le contrôle de la chose (2). L'utilisateur locataire ou preneur en leasing d'un système informatique sera donc en principe considéré comme "gardien de la chose" et pourra être tenu pour responsable d'un dommage causé à un tiers (par exemple, un employé, un client, un technicien assurant la maintenance du système, ...) pour autant que celui-ci puisse établir que le dommage dont il est la victime est dû à un vice du système informatique.

2.2 Le droit de la preuve

Si une opération est réalisée par voie télématique et que celle-ci entre dans la catégorie des "actes juridiques" (par exemple un contrat) par opposition aux "faits juridiques" (par exemple un accident), les parties à cette opération ne pourront, en principe, en rapporter la preuve qu'au moyen d'un écrit signé en vertu de l'exigence posée par l'article 1341 du Code Civil. Il est donc de l'intérêt de chacune des parties de respecter l'article 1341. La jurisprudence ne reconnaît pas jusqu'à présent la validité de la "signature électronique" (codes secrets, cryptographie, ...). L'exigence contenue dans l'article 1341 du Code Civil constitue en principe un sérieux obstacle au développement de la télématique utilisée pour la conclusion de contrats, étant

---

(1) Pour plus de détails sur ces questions, on se réfèrera utilement à Michel Coipel et Yves Poullet in "Le droit des contrats informatiques - Principes - Applications" (oeuvre collective), Larcier, 1983, p. 29 et suivantes.

(2) Cour de Cassation, 6 février 1958, Pas. 1958, I, 616.

donné l'insécurité en matière de preuve de l'opération qui affecte les deux parties en cas de non respect de l'exigence de l'écrit signé. Ce risque peut cependant être considérablement réduit en convenant par contrat écrit préalable de la validité de la signature électronique (1). Il est en effet admis que l'article 1341 du Code Civil est une disposition qui n'est ni d'ordre public ni impérative.

3. Les obligations résultant de lois particulières

Les spécificités de l'informatique créent certaines difficultés quant au respect de certaines obligations légales et règlementaires qui avaient été conçues dans un contexte non-informatique. Tel est le cas des différentes exigences légales et règlementaires en matière de conservation de documents à des fins comptable, fiscale ou sociale. Dans un premier paragrpahe, nous examinerons comment ces obligations peuvent être remplies en cas d'usage de l'informatique. L'utilisation généralisée de l'informatique a aussi suscité l'adoption de réglementations dont il convient d'examiner les dispositions spécifiques relatives à la sécurité. Tel est le cas des lois dites "Informatique et Libertés" et de réglementations sur la sécurité des équipements et leur connection aux réseaux publics de télécommunications. Celles-ci seront examinées dans un deuxième paragraphe.

3.1 Les obligations relatives à la conservation des documents

Il existe en matière comptable, fiscale et sociale des exigences particulières quant à la tenue et la conservation de certains documents. L'utilisation de l'informatique permet-elle de répondre à ces exigences? Ce type de réglementation peut varier considérablement d'un pays à l'autre. Le présent examen se limitera à un examen de la situation en France et en Belgique.

3.1.1 L'exemple du droit belge

Du point de vue du droit comptable, la législation belge n'empêche pas la tenue des livres comptables sous la forme de documents d'origine informatique, pour autant que

---

(1) Pour plus de détails voir Benard Amory et Yves Poullet, Le droit de la preuve face à l'informatique et à la télématique, Revue Internationale de Droit Comparé, No. 2, 1985, p. 331 et. seq.

ceux-ci répondent aux exigences de la loi comptable, notamment celles de l'intelligibité directe et de l'inaltérabilité. La première sera respectée si ces documents d'origine informatique sont imprimés sous forme directement lisible par l'homme (par exemple les listings), la seconde en apposant une signature qui chevauche la page du livre servant de support et le document de sortie d'ordinateur collé sur celui-ci. Les pièces justificatives de la comptabilité qui doivent en principe être conservées pendant dix ans peuvent l'être en original ou en copie, notamment sous forme de microfilm ou tout autre support analogue.

En droit fiscal, l'obligation de conservation des pièces justificatives pendant cinq ans porte, en principe, sur les documents originaux, bien qu'une tolérance administrative permette sous certaines conditions une conservation sous forme de microfilms, y compris microfilms de sortie d'ordinateur.

Enfin, sur le plan du droit social, il a été précisé à l'occasion d'une réponse à une question parlementaire que l'employeur peut conserver les documents sociaux sous une autre forme que l'original pour autant qu'ils soient bien lisibles et que la forme de reproduction utilisée permette un contrôle efficace. Moyennant respect de ces conditions, la tenue de ces documents sous forme informatique est donc possible en Belgique.

3.1.2 L'exemple du droit français

Le nouveau droit comptable français a aboli le concept de livres et parle de "documents d'enregistrements comptables", et du coup valide "tous supports de l'information fiables" (1).

Les "Dispositions Générales relatives à l'utilisation des traitements automatisés du Nouveau Plan Comptable" précisent d'ailleurs que le "système de traitement doit établir sur papier ou éventuellement sur tout support offrant des conditions de garantie et de conservation définies en matière de preuve, des états périodiques, ..." En ce qui concerne les pièces justificatives de la comptabilité, leurs modalités de conservation n'ont pas été précisées. Il convient donc de se rapporter aux dispositions du droit commun figurant aux articles 1334 et 1348 du Code Civil requérant la conservation soit en original, soit sous forme de copie "fidèle et durable" c'est-à-dire une reproduction indélébile de l'original qui entraîne une modification irréversible du support".

---

(1) Cf. A. Bensoussan, Droit et comptabilité informatique, 01 Informatique, No. 168 avril 1983, p. 110 et 111, no. 169 mai 1983, p. 102 et 103 et No. 170 juin-juillet 1983, p. 140 et 141.

Sur le plan fiscal, il n'existe à notre connaissance aucune règle quant à la présentation et à la tenue de la comptabilité. Toutefois, une comptabilité ne respectant pas les normes de la loi comptable risquerait d'être rejetée par les autorités fiscales. Quant à la conservation des pièces justificatives, n'importe quelle forme de copie, y compris électronique ou magnétique, est permise en ce qui concerne les documents émis par l'entreprise. A l'inverse, la conservation doit se faire sous forme originale pour les pièces reçues.

Enfin, la réglementation sociale permet l'usage de microfilms pour la conservation des renseignements relatifs aux bulletins de paie, moyennant certaines conditions permettant notamment de faciliter leur consultation par les services de contrôle.

L'ensemble des obligations énumérées ci-avant relatives à l'utilisation de l'informatique en matière comptable, fiscale et sociale repose évidemment sur le titulaire de l'obligation principale, c'est-à-dire l'utilisateur final du système informatique. Il lui appartiendra donc de s'assurer que le système qu'il utilise réponde aux exigences précitées au risque de se voir infliger des sanctions administratives ou pénales prévues par les réglementations en ces matières.

3.2 Les obligations résultant des lois sur la protection de la vie privée

Plusieurs pays européens ont adopté des lois relatives à la protection de la vie privée, particulièrement contre les abus qui pourraient résulter des possibilités offertes par l'informatique. Ci-après, à titre illustratif, figure un relevé des principales obligations prévues par la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).

La personne physique et morale qui a le pouvoir de décider la mise en oeuvre d'un traitement automatisé d'informations nominatives est tenue a une déclaration préalable à effectuer auprès de la Commission Nationale de l'Informatique et des Libertés. Il importe de souligner qu'en cas de sous-traitance de l'exploitation des informations, l'entreprise principale reste tenue à la déclaration. Par contre, en cas de cession de fichier, on considère qu'il y a nouvelle constitution de fichier et il devra donc y avoir deux déclarations (2).

---

(1) Loi No. 78-17, Journal Officiel du 8 janvier 1978, page 227. Pour un excellent résumé et commentaire de la loi sur lequel s'appuie le présent texte, voir X. Linant de Bellefonds et A. Hollande, Droit de l'informatique, J. Delmas & Cie., Paris, 1984, p. 80 et. seq.

(2) X. Linant de Bellefonds et A. Hollande, op. cit.

Corrélatif du droit d'accès (lequel permet à toute personne pensant figurer dans un fichier d'obtenir communication des informations nominatives le concernant) il existe une obligation de communication à charge du maître du fichier. En vertu de cette obligation, ce dernier est tenu de communiquer au titulaire du droit d'accès l'information en langage clair et ce dans les plus brefs délais, compte-tenu, néanmoins, d'éventuels obstacles techniques.

3.3 Les obligations résultant des normes en matière de sécurité des appareils électriques

Les équipements informatiques sont en principe soumis aux normes de sécurité pour les appareils électriques généralement établies au niveau national et international par des organismes professionnels reconnus. Ces normes peuvent obtenir une force juridique obligatoire généralisée suite à leur intégration dans la réglementation par la voie de lois, arrêtés, décrets ou, au niveau européen, directives et règlements.

Ces normes visent à assurer la sécurité au sens strict, c'est-à-dire essentiellement la sécurité physique des utilisateurs et la compatibilité avec d'autres équipements.

C'est normalement le fabricant d'un équipement informatique ou le vendeur de cet équipement qui sont tenus à assurer le respect de ces règles. Il appartient donc au fabricant ou au vendeur de suivre la procédure de l'homologation, appelée aussi agréation, afin d'assurer le respect de l'obligation. Ces pocédures sont organisées différemment d'un pays à l'autre. Des efforts d'harmonisation européenne de ces procédures sont actuellement mis en oeuvre avec le concours notamment du Comité européen de normalisation electrotechnique. La violation de ces réglementations donne lieu à des peines variables selon les pays. A titre d'exemple, en Belgique, un Arrêté Royal du 11 juillet 1961 prévoit des amendes pénales et un emprisonnement pouvant aller jusqu'à six mois en cas de violation des normes de sécurité. Si ces sanctions visent au premier chef le fabricant et le fournisseur d'un équipement informatique, on rapellera que l'utilisateur d'un appareil non conforme peut, par le biais de l'article 1384 du Code Civil, être tenu pour responsable en cas de dommage causé à un tiers par cet équipement (voir ci-dessous).

3.4 Les obligations résultant de la réglementation des télécommunications

Etant donné que les équipements informatiques sont de plus en plus souvent connectés aux réseaux publics de télécommunications, il y a lieu d'attirer l'attention sur les obligations qui trouvent leurs sources dans la réglementation sur les télécommunications.

Dans la plupart des pays européens, il existe des dispositions législatives ou règlementaires qui soumettent la connection des appareils en général (en ce compris les logiciels et matériels informatiques) à certaines obligations préalables. Ces obligations ont pour objectif d'assurer l'intégrité des réseaux de télécommunications et la sécurité des usagers et du personnel affecté à l'entretien des réseaux. Contrairement aux obligations de sécurité électrique étudiées au paragraphe prédédent, celles-ci s'imposent généralement en ordre principal aux utilisateurs. Ainsi en Belgique, le Décret Ministériel du 20 septembre 1978 interdit à tout usager du réseau téléphonique d'y connecter par quelque moyen que ce soit un appareil quelconque sans l'autorisation préalable écrite de la Régie de Télégraphes et Téléphones. L'agréation doit être obtenue par le fabricant ou le vendeur de l'équipement, suite à une procédure de nature administrative et technique.

La violation de l'interdiction édictée par l'Arrêté Ministériel du 20 septembre 1978 ne donne actuellement lieu qu'à des sanctions administratives consistant en la déconnection des appareils connectés au frais de l'utilisateur. Toutefois, dans d'autres pays européens, il existe des interdictions semblables qui sont sanctionnées pénalement.

4. Les obligations d'origine contractuelle

Les contrats font la loi des parties. Il en résulte de multiples obligations variables dans chaque cas d'espèce. Nous voulons simplement attirer ici l'attention sur certaines obligations particulières en matière de sécurité dans différents types de contrats.

4.1 Les contrats de fourniture de matériel et/ou logiciel

En raison des contacts préliminaires qu'il a avec un acquéreur potentiel (dès l'analyse d'opportunité pour la préparation de son offre) et, le cas échéant, tout au long de la phase de développement, le fournisseur aura probablement accès à des informations considérées comme confidentielles par l'acquéreur. Dès ce moment, il est conseillé d'exiger d'un fournisseur un engagement de confidentialité dans lequel il garantira de ne pas divulguer cette information, l'utiliser à d'autres fins ni la conserver plus longtemps que nécessaire. En toute hyposthèse, le fournisseur respectera une obligation de discrétion au risque, même en l'absence de clause contractuelle à cet effet, de se voir accusé de mauvaise foi dans l'exécution du contrat (violation de l'article 1134 du Code Civil).

En ce qui concerne l'acquisition de logiciels, les questions de sécurité se posent:

- à propos de la qualité du logiciel. Celle-ci dépendra largement des exigences formulées par l'acquéreur. L'acquéreur ne pourra se contenter du libellé des garanties techniques mais exigera des garanties de résultats fonctionnels. Une fois le logiciel installé, des tests de validation seront effectués.

- à propos de la continuité du logiciel, les parties ont intérêt à ce qu'une copie du logiciel en code source soit déposée auprès d'un tiers auprès duquel il y aura toujours moyen de se le procurer en vertu des dispositions d'un contrat ad hoc en cas de perte, vol ou destruction auprès d'une des parties.

En ce qui concerne la fourniture de matériel, c'est surtout sur la garantie de l'existence d'un stock de pièces de rechange durant toute la vie du système qu'on insistera.

4.2 Les contrats de maintenance

La sécurité d'un système dépend aussi d'une maintenance adéquate de celui-ci. Si la maintenance est effectuée par un tiers, on accordera une attention particulière aux points suivants lors de la signature d'un contrat de maintenance:

- Quelles sont les parties exclues de la maintenance?
- Le moment, la durée et la fréquence des visites.
- Le temps d'intervention en cas de panne.
- La possibilité éventuelle pour la firme de maintenance d'assurer un système de back-up.
- La correction des erreurs contenues dans le logiciel et l'adaptation éventuelle de celui-ci à de nouvelles normes.

Aux clauses visant ces situations correspondent les obligations contractuelles.

4.3 Les contrats de back-up

Lorsque l'entreprise ne dispose pas de son propre système de back-up, elle peut conclure un contrat de back-up avec une autre firme, en vue d'avoir à sa disposition un système de rechange en cas de catastrophe. Un tel contrat peut être conclu sur une base de réciprocité avec une autre entreprise qui ressent le même besoin ou avec une firme spécialisée dans la fourniture de service de back-up. De tels contrats doivent être rédigés avec une attention particulière de sorte que si un accident se produit, les parties sachent exactement et immédiatement quels sont leurs droits et devoirs respectifs en ce qui concerne l'utilisation et l'assistance. Les clauses suivantes sont particulièrement importantes:

- une clause définissant avec précision les situations dans lesquelles la partie qui rencontre une difficulté peut avoir recours au service de back-up. Seule une description précise de ces circonstances garantira en cas de besoin urgent de back-up que l'autre partie ne conteste pas le droit au back-up.
- une clause prévoyant la procédure suivant laquelle la demande de back-up du service sera notifiée.
- un clause décrivant l'étendue du service offert et notamment s'il comprend l'assistance technique du personnel de la firme de back-up.
- une clause précisant quelles modifications peuvent être apportées par les parties à leurs systèmes respectifs, leur procédure de notification et d'acceptation. Cela évitera que les systèmes ne deviennent incompatibles.
- enfin, il importe que le fournisseur du back-up s'engage personnellement et au nom de son personnel et de ses sous-contractants à respecter la confidentialité de l'information à laquelle il aurait accès en cas d'utilisation du service de back-up.

4.4 Les contrats d'emploi

La sécurité informatique requiert aussi l'insertion de certaines clauses particulières dans les contrats conclus avec le personnel. Cela s'applique, spécialement, au personnel employé dans le département informatique de l'entreprise ou en contact avec celui-ci. On sait en effet qu'une grande majorité (1) des cas de fraude informatique trouve son origine parmi le personnel de l'entreprise. L'employeur doit être conscient qu'en copiant un logiciel concédé à l'entreprise et en le vendant à un tiers, l'employé peut rendre l'employeur responsable vis-à-vis du concédant.

Les obligations particulières qu'il est recommandé d'imposer au personnel dans les contrats d'emploi sont reprises ci-après. Premièrement, une interdiction de communiquer à des tiers ou d'utiliser à des fins personnelles les informations confidentielles acquises au sein de l'entreprise. Bien qu'une telle clause apparaisse dans la plupart des contrats d'emploi, en ce qui concerne le personnel informatique, il est utile d'établir dans le contrat d'emploi une liste des types d'informations ou de données que l'employeur considère comme particulièrement sensibles et confidentielles. Cela pourra éventuellement faciliter soit un licenciement pour faute grave si l'employé a violé cette obligation de confidentialité en cours de contrat, soit l'obtention de dommages et intérêts si l'information a été communiquée après qu'il ait été mis fin au contrat d'emploi. Il est aussi utile de

(1) 78% selon une étude de l'American Bar Association
75% selon une étude de Data Processing Management Association.

prévoir une clause de non-concurrence en conformité avec les éventuelles dispositions d'ordre public réglementant ce genre de clause (au risque de la voir déclarée non-écrite). Si l'employé est amené à développer un logiciel, le contrat d'emploi déterminera à l'avance qui, de l'employeur ou de l'employé, en est propriétaire (1).

4.5 Les contrats "télématiques"

Nous avons vu que la combinaison de l'informatique et des télécommunications (connue sous le nom de "télématique") permet aux entreprises de relier leurs ordinateurs respectifs. Cette technique permet d'échanger des informations et même de conclure des transactions.

La télématique soulève des nouvelles questions de sécurité relatives à l'identification des parties, l'authenticité et l'intégrité du contenu des messages (c'est-à-dire l'absence de fraudes et d'erreurs) et à la détermination des responsabilités en cas de dommage survenant durant la transmission du message.

Ces nouveaux risques requièrent que de nouvelles obligations soient imposées dans les contrats ayant pour objet des services télématiques. Ainsi, comme il n'est pas possible de signer, au sens juridique du terme, une opération télématique, on conviendra dans le contrat de base de la validité de la signature électronique (voir ci-dessus). Le contrat de base prévoira aussi que les documents informatiques conservés par les parties constituent une preuve valable de leur contenu. Le contrat de base déterminera aussi les responsabilités respectives des parties impliquées dans l'opération télématique étant donné la difficulté de localiser un mauvais fonctionnement dans un réseau télématique.

En matière de télématique financière, on n'oubliera pas un principe développé en droit bancaire(2) selon lequel le banquier est responsable de la technique qu'il met à la disposition de son client. Une application de ce principe en matière de transferts électroniques de fonds est la décision rendue par la Civil Court of the City of New York dans l'affaire Ognibene v. Citibank N.A.(3) dans laquelle la banque a été tenue responsable d'une fraude effectuée auprès d'un distributeur automatique de billets étant donné le défaut de sécurité que présentait le système en place. Le tribunal a déclaré:

---

(1) En France, en vertu de la loi du 3 juillet 1985, à défaut d'une telle clause, l'employeur est considéré comme titulaire des droits d'auteurs sur un tel logiciel.

(2) Voir notamment Cass. fr. Com. 20 juin 1977 (Bull. Civ. 1977, IV p. 149).

(3) N.Y. City Civ. Ct., 446 N.Y. S 2d 845.

"Since the bank established the electronic fund transfer service and has the ability to tighten its security characteristics, the responsibility for the fact that plaintiff's code, one of the two necessary components of the access device or means of access to his account, was observed and utilized as it was must rest with the bank".

Conclusions

La plupart des mesures nécessaires à l'obtention d'un degré de sécurité informatique maximum sont de nature purement technique. Certaines d'entre elles dont le présent exposé a établi un relevé qui n'a pas la prétention d'être exhaustif sont coulées en forme d'obligations de nature juridique, d'origine légale, règlementaire ou contractuelle. Etant donné la multitude de ces obligations, on ne peut que recommander aux utilisateurs et aux fournisseurs de systèmes informatiques de s'assurer à tout moment qu'ils remplissent valablement les obligations qui leurs sont imposées. En ce qui concerne les obligations d'origine légale ou réglementaire cela suppose de se tenir au courant des changements opérés par le législateur particulièrement fréquent dans un secteur en évolution constante comme celui de l'informatique et de la télématique. Etant donné le principe de la liberté contractuelle, ce sont bien entendu les obligations d'origine contractuelle qui sont les plus nombreuses et les plus variées. Chaque cas est particulier et nécessite une étude individuelle des exigences de sécurité à imposer contractuellement aux parties en présence en raison des circonstances.

* * *