# Le management juridique de la sécurité du système d'information

Poullet, Yves

*Published in:*
Informatique et contrôle

*Publication date:*
1986

*Document Version*
le PDF de l'éditeur

# DROIT ET SECURITE INFORMATIQUE

## LE MANAGEMENT JURIDIQUE DE LA SECURITE DU SYSTEME D'INFORMATION

Texte d'une conférence donnée pour
l'Institut des Reviseurs d'Entreprises
le 13 décembre 1985.

Y. POULLET
Chargé de cours aux F.N.D.P.
Directeur du Centre de Recherches
Informatique et Droit (Namur)

## INTRODUCTION

### COMPUTERS : THE CHANGING RISK

Les applications informatiques autrefois réduites à quelques fonctions autour d'un seul ordinateur central, se sont étendues à des systèmes d'information réparties, systèmes fondés sur une utilisation beaucoup plus massive de l'information à tous les niveaux.

En outre, les utilisateurs ont besoin entre eux de communications directes par réseaux de terminaux dispersés dans le pays, voire dans le monde.
La dépendance des entreprises par rapport à ces systèmes est telle, qu'elles ne peuvent survivre plus de quelques jours, voire plus de quelques heures à un désastre informatique.

Aux Etats-Unis, une compagnie d'assurances a affirmé que 80% des grandes entreprises ne pouvaient survivre à un désastre informatique.

Le fait que l'informatisation soit présente à tous les niveaux d'activité d'une entreprise et qu'elle soit accessible même à des non-informaticiens, voire à des tiers, entraîne l'existence de nouveaux risques, ainsi ceux de fraude informatique ou d'espionnage informatique.

Quant aux données elles-mêmes, même reproduites à divers endroits, elles se retrouvent concentrées sur un petit nombre de disques, et dès lors, sont totalement vulnérables à une erreur d'opération, au disfonctionnement d'une

machine, à la mauvaise programmation d'un logiciel, voire enfin, à leur détournement. Le nombre d'informations reprises par unité spatiale est de plus en plus élevé et ce mouvement est exponentiel. Bref, on ne peut plus parler de risques de l'informatique, mais de risques de l'informatisation.

Notre propos est, ayant analysé brièvement le concept de sécurité informatique, d'éclaircir le rôle que le droit peut jouer, conscient du fait que la solution certes est d'abord technique.



## CHAPITRE I : DE LA SECURITE

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

- La "**fiabilité**" : Un système est dit fiable dans la mesure où les résultats qu'il génère sont identiques aux résultats attendus sur base des spécifications" (I. HOORENS). 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 non désirée de programme ou d'information.

La "**continuité**" : permet de maintenir le système à tout moment de sa vie conforme aux nécessités de l'utilisateur; ceci implique non seulement les activités de prévention et d'intervention en cas d'incidents, mais également les activités d'adaptation du système à des besoins nouveaux, ainsi, en cas de modification d'une législation comptable nécessitant des adaptations du logiciel comptable.

## CHAPITRE II : DU DROIT

Traditionnellement, le rôle du droit est de trois ordres : prévenir, réparer et sanctionner.

Face aux problèmes posés par la sécurité du système d'information, ce triple rôle du droit peut s'analyser comme suit :

1. Le rôle peut aider à prévenir les risques informatiques c'est-à-dire proposer des solutions contractuelles qui permettent à l'utilisateur de diminuer voire d'évacuer certains risques.

2. En cas de survenance du risque, le droit peut prévoir des solutions de remplacement, solutions financières bien souvent.

3. Enfin, la faute humaine à la base du sinistre mérite parfois d'être sanctionnée.

Le rôle préventif du droit est assuré essentiellement par le droit des contrats. L'intégrité des données, la fiabilité des traitements et la confidentialité des résultats feront l'objet de clauses particulières dans les contrats portant sur la fourniture du hardware, du logiciel mais également dans les contrats d'emploi et dans les contrats "télématiques". Ils peuvent faire l'objet de contrats ou prestations particulières auprès de tiers, chargés de valider les programmes. Le maintien des différentes qualités du logiciel tout au long de la vie du système sera assuré par des clauses particulières du contrat de maintenance.

Le rôle curatif du droit est l'objet de contrats spéciaux : contrats de back-up d'une part, contrat d'assurance, d'autre part. Il est également garanti par les multiples clauses de réparation des dommages proposés dans les différents contrats conclus avec les fournisseurs.

Enfin, une lourde sanction pénale est parfois le meilleur moyen pour dissuader les personnes susceptibles d'être les auteurs d'un sinistre. A cet égard, le droit pénal a certes à s'adapter aux nouvelles infractions permises par les nouvelles technologies de l'information.

Ainsi, nous étudierons successivement :

1. dans les contrats de fourniture de matériel et de logiciel, les clauses relatives à la sécurité et à la réparation en cas de sinistre;

2. les contrats particuliers conclus avec des tiers et destinés à assurer la sécurité du système informatique;

3. les clauses particulières dans les contrats d'emploi;

4. les clauses particulières dans les contrats de maintenance;

5. les clauses particulières dans les contrats "télématiques";

6. les contrats de back-up;

7. les divers types de contrats d'assurances;

8. les solutions pénales aux sinistres informatiques.

### I. Dans les contrats de fournitures de matériel et de logiciel, les clauses relatives à la sécurité et à la réparation en cas de sinistre

L'acquisition de matériels et/ou de logiciels constituant une partie ou l'entièreté du système d'information fait l'objet de divers contrats conclus avec l'un ou plusieurs contractants.

En effet, à côté des contrats portant sur un ou des éléments spécifiques : matériel, terminaux, modems, logiciels de base, logiciel d'application, on connaît des contrats globaux dits "clés en mains". Il est clair qu'en cas de multiplicité de contrats et de contractants, le principe de l'indépendance de chaque contrat et celui de la relativité des contrats risquent d'entraîner des conséquences graves pour l'utilisateur : ainsi, la commande non honorée d'un software ou la livraison d'un software non adéquat aux besoins de l'entreprise n'entraîne pas la nullité ni la résolution d'un autre contrat portant lui sur le hardware, encore qu'une jurisprudence récente tende à consacrer l'interdépendance des contrats lorsque les prestations, objets de ces contrats, sont le fait d'un même fournisseur.

En toute hypothèse, l'utilisateur a tout intérêt à créer une certaine interdépendance des contrats, par des clauses appropriées.

Autre problème : bien souvent, le fournisseur lui proposera en dernière minute des clauses types auxquelles doit adhérer, sans pouvoir les adapter à ses besoins sépcifiques. Il est donc utile, et en matière de sécurité comme en d'autres (par exemple délais de livraison, conditions de paiement, performances du système), d'introduire, dès le départ, les aspects juridiques dans la négociation.

Ces remarques générales proposées, que dire des aspects "Sécurité" entendue au sens le plus large ?

Nous distinguerons à cet égard trois étapes :

- les clauses relatives à la sécurité et plus particulièrement à la confidentialité dans la phase préparatoire et tout au long de l'opération d'informatisation.

- les clauses ad-hoc présentes dans les contrats relatifs au matériel.

- les clauses ad-hoc susceptibles d'être insérées dans les contrats de logiciels, en particulier de logiciel sur mesure.

A. Les clauses de confidentialité valables tout au long de l'opération et dès la phase préparatoire.

Sur base de ces contrats préliminaires avec l'entreprise (dès l'analyse d'opportunité, pour la préparation de son offre) et, le cas échéant, tout au long de la phase de développement (analyse fonctionnelle, étude d'opportunité), le fournisseur aura probablement accès à de l'information jugée confidentielle par l'entreprise (méthode de gestion, nombre et importance des clients, etc.)

Il est donc indispensable dès le départ de prévoir une clause de confidentialité relative aux données dont le fournisseur aurait pris connaissance au cours de ses relations avec le fournisseur.

Ces clauses de "non disclosure" de l'information doivent lier tous les membres du personnel du fournisseur affectés au marché qui ne pourront, par ailleurs se servir de l'information que dans le cadre de ce marché. Elle doit interdire toute communication directe ou indirecte à des tiers et leur efficacité ne doit pas être limitée à la durée de l'opération. Il est utile de prévoir en cas de violation, des dommages et intérêts forfaitaires minimaux, sous réserve de prouver des dommages plus grands. En outre, l'utilisateur, par une clause appropriée, imposera au personnel du fournisseur affecté au projet, l'obligation de suivre les règles de sécurité édictées pour le personnel de l'entreprise (identification à l'entrée et à la sortie des bâtiments, port de badge). Ces règles seront communiquées au fournisseur.

B. Les clauses relatives à la sécurité dans les contrats "matériel".

C'est principalement la clause relative à la garantie de réparation ou de remplacement des pièces ou éléments défectueux qui retiendra l'attention de l'utilisateur. La sécurité de l'ensemble du système est mise en cause si un des éléments importants (un disque dur, un lecteur de disques, etc...) ne peut être réparé ou remplacé et oblige à modifier l'ensemble ou une partie de la configuration devenue inutilisable.

Outre les garanties de réparation ou de remplacement incluses dans le contrat lui-même, valables pendant une période généralement courte, mais prolongées par la signature d'un contrat de maintenance (cfr IV), outre l'existence d'un contrat de back-up (cfr VI), l'utilisateur doit obtenir qu'en toute hypothèse, le fournisseur garantisse l'existence d'un stock de pièces de rechange pendant toute la durée de la vie normale du matériel. Certes, bien souvent, le fournisseur lie cet engagement au droit exclusif de fournir les pièces de rechange. Même dans ce cas, on peut imaginer que le fournisseur doive nécessairement avertir l'utilisateur, en cas d'incapacité de fournir certains composants (par exemple, le producteur a cessé sa production ou ses exportations), de sorte que l'utilisateur puisse se fournir ailleurs.



On évoque également les clauses portant sur les spécifications relatives à l'environnement de matériel et nécessaires à son bon fonctionnement. Le fournisseur a un devoir d'information à ce sujet, nonobstant l'absence de clauses.

C. Les clauses relatives à la sécurité dans les contrats "logiciels".

Les programmes sont l'âme du système informatique. C'est eux qui permettent de réaliser les besoins spécifiques de l'utilisateur. A propos de leur acquisition, (contrats de progiciels) ou de leur développement (contrats de développement de logiciel sur mesure), des questions de sécurité se posent :

1. à propos de la qualité du logiciel : la fiabilité du logiciel implique qu'il réponde à un certain nombre d'exigences variées, en fonction du besoin de l'utilisateur.

   Ainsi on peut souhaiter qu'il contrôle automatiquement la vraisemblance des données entrées; qu'il vérifie les mots de passe et stocke en mémoire les interrogations faites à partir de l'utilisation d'un mot de passe; qu'il identifie les corrections apportées à posteriori à une inscription comptable, la donnée originaire restant lisible qu'il permette le calcul automatique d'un certain nombre de ratios comptables; qu'il imprime selon telle structure et avec telles mentions légales, les factures.

   Comment s'assurer que le logiciel acquis ou à développer réponde à ces exigences ? Il est certain qu'en la matière, l'utilisateur ne peut se contenter du libellé des garanties techniques (langage de programmation, système de gestion des bases de données, structure des fichiers), mais doit exiger des garanties de résultats fonctionnels, compte tenu de l'environnement dans lequel le programme doit tourner. Ainsi, ce qui importe à l'utilisateur, c'est, étant donné l'activité de 80 terminaux connectés en ligne à tel ordinateur central, que telle opération voulue (ex. calcul de ratios comptables, identification des mots de passe) puisse s'opérer dans un délai X, sans erreur et sans être connue d'un autre utilisateur, situé à un autre terminal. L'utilisateur peut être plus vague encore : le fournisseur devra fournir un logiciel comptable de telle sorte que les sorties satisfassent aux conditions prévues par la loi ou par une norme comptable bien particulière.

2. à propos de la vérification des qualités du logiciel : la vérification des qualités du logiciel ne peut se faire que celui-ci une fois implanté. Il s'agit alors de contrôler dans quelle mesure le logiciel développé ou acquis dispose des qualités attendues. Un certain nombre de tests sont permis. Ces tests permettent la validation du programme. Ils peuvent porter sur le volume, les performances, le stockage, la configuration, ils peuvent être de différentes qualités,

vérifier l'exécution d'une instruction, de toutes les alternatives pour chaque instruction, de toutes les alternatives pour toutes les instructions, etc.

La réalisation de ces tests peut être le fait du fournisseur lui-même, de l'utilisateur ou d'un tiers (cfr II).

La réussite de ces tests permet la réception du sytème, constatée par un procès-verbal signé par les deux parties. Cette réception peut n'être que provisoire, la réception définitive pouvant être différée après quelques mois d'utilisation du programme en charge réelle.

On note qu'à ces réceptions, est généralement attaché le paiement d'une tranche du prix, l'utilisateur pouvant bloquer la suite des paiements, en cas d'incapacité du fournisseur à réaliser les tests.

3. à propos de la continuité du logiciel : le troisième aspect de la sécurité du logiciel, sa continuité, c'est-à-dire la possibilité d'adapter le logiciel par la suite, est résolu partiellement par des clauses reprises dans le contrat de logiciel (cfr en outre le point IV, relatif au contrat de maintenance).

   A cet égard, on note :

   a) Les clauses relatives à la documentation.
      Plus la documentation est importante et de qualité, plus l'utilisateur sera à même de faire lui-même les modifications qu'il souhaite, et dès lors, sera autonome par rapport au fournisseur. L'utilisateur exigera donc une documentation la plus complète possible, y compris des manuels d'utilisation détaillés.

   b) Le plus souvent, sauf lorsque l'utilisateur devient propriétaire du programme, le fournisseur met une limite à la fourniture de la documentation : il garde le code source empêchant ainsi l'utilisateur de modifier le programme du fournisseur mais non d'y apporter des programmes propres.

      Le fait que le fournisseur garde le logiciel source peut présenter un risque pour l'utilisateur lorsque le fournisseur n'est plus à même ou ne veut plus maintenir le logiciel.
      C'est pourquoi des contrats prévoient le dépôt du logiciel et de ses versions dès sa réalisation et par la suite à des échéances déterminées, dépôt dans les mains d'un tiers (notaire ou autres). Ce tiers pourra, le cas échéant, remettre à l'utilisateur, la copie déposée à charge pour ce dernier de s'en servir aux seules fins de maintenance.



## II. Les contrats particuliers conclus avec des tiers et destinés à assurer la sécurité du système informatique

De nombreux utilisateurs s'avèrent insuffisamment compétents pour discuter à égalité avec les sociétés fournisseurs. En particulier, ils peuvent craindre que la solution informatique qui leur est proposée et telle qu'elle est progressivement implémentée ne corresponde pas à l'ensemble des moyens de sécurité souhaités ou souhaitables.

En d'autres termes, les utilisateurs peuvent souhaiter dissocier, d'une part les fonctions de conception et de programmation du système informatique de celle, d'autre part d'audit ou de validation. Le problème de la validation, c'est-à-dire du contrôle externe d'évaluation dans son ensemble et pour chaque élément du système de conception et de programmation, couvre bien d'autres questions que celles de la sécurité, mais c'est peut-être en cette matière plus technique, plus spécialisée et aux conséquences plus importantes pour l'entreprise que la validation s'avère la plus nécessaire.

On peut songer confier la validation à la société qui conçoit et fournit le système. Certaines sociétés prévoient même en leur sein une équipe chargée de valider le travail d'une autre chargée elle de programmer. Elle sont conscientes qu'une équipe de programmation, psychologiquement et fonctionnellement, ne peut tester ses propres programmes ni l'adéquation de la configuration proposée aux besoins de l'utilisateur.

Ce dernier peut cependant souhaiter l'intervention d'un conseiller ou d'une société d'audit, neutre et indépendante du fournisseur. Il peut lui confier différentes tâches, allant de l'examen des propositions des fournisseurs à la rédaction et à l'implémentation de tests validant les différentes phases d'implantation du système. Cette activité d'audit, en particulier en matière de sécurité, pourrait être le fait de sociétés de reviseurs comptables et, à mon avis, entre parfaitement dans leur mission légale.

Pour l'utilisateur, il importera dans le contrat qu'il concluera à cet effet :

de s'assurer par des clauses appropriées de l'indépendance de la société d'audit, de la qualité des employés qu'elle affectera à ce travail et de leur devoir de confidentialité (cfr. supra point I).

de déterminer la qualité minimale de la validation (par exemple, les tests devront être rédigés de façon telle que toutes les valeurs possibles pour toutes conditions dans chaque décision du programme auront été testées (Mult Condition Average)) et prévoir la structure du rapport qui lui sera adressé.

- de souscrire un contrat dans toute la mesure du possible modulaire, c'est-à-dire distinguant les différentes prestations de la société d'audit (par exemple, examen de la configuration proposée, validation de l'analyse organique, rédaction de tests, exécution de ceux-ci, etc...) et résiliable après chaque phase;

- de prévoir des devis pour chaque prestation, devis qui ne pourront être dépassés sauf motivation par la société d'audit;

- de prévoir la livraison des jeux de tests de telle sorte que ceux-ci ne doivent pas être recrées lors de la modification ultérieure des programmes (cas de releases).

L'utilisateur aura soin de notifier à ces fournisseurs l'intervention de cette société externe, et obtiendra des premiers qu'ils répondent aux demandes d'information voire de travail complémentaires exigées des seconds.

## III. Les clauses dans les contrats d'emploi

Selon D. PARKER, les risques les plus importants encourus par les responsables d'un système d'information viennent du personnel. L'accès au système est généralement facile, étant donné la répartition des terminaux. En copiant des programmes sous licence et en les revendant à des tiers, les employés peuvent rendre leurs employeurs responsables vis-à-vis du donneur de licence. Le personnel peut également communiquer à des tiers des informations confidentielles traitées par le système (par exemple, une liste des clients).

Afin de prévenir de tels risques, les entreprises prennent généralement des mesures organisationnelles pour contrôler l'accès de leur propre personnel aux Centres de traitement (par exemple, utilisation de codes secrets et d'identification; engagement d'un responsable de la sécurité, mesures d'ordre interne à respecter en cas d'accès au Centre, rotation de personnel).

Quelques clauses spécifiques dans les contrats d'emploi aideront à garantir cette sécurité. A notre avis, de telles clauses doivent être présentes dans les contrats conclus avec les informaticiens ou programmeurs du Centre mais également dans ceux conclus avec le personnel susceptible d'entrer en contact avec le système d'information.

En ce qui concerne le contenu de ces clauses, premièrement, de tels contrats doivent prévoir une clause prohibant toute communication à des tiers ou toute utilisation à des fins propres d'informations confidentielles détenues par l'entreprise. On conçoit qu'il soit préférable de donner une liste d'exemples de données jugées particulièrement sensibles et confidentielles, et d'affirmer que cette obligation perdure au-delà de la durée du contrat d'emploi.



Deuxièmement, on prévoiera les sanctions attachées à la divulgation de données ou de programmes, sanctions disciplinaires d'ordre divers allant jusqu'au licenciement.

Troisièmement, dans le cadre des conventions avec les représentants des travailleurs, on cherchera à limiter les conséquences désastreuses qu'une grève avec occupation du centre de traitement pourrait avoir sur la vie de l'entreprise.

Enfin, dans les limites légales, on introduira une clause de non concurrence à propos des contrats conclus avec le personnel chargé de développer des programmes. Il est peut-être utile vis-à-vis de ce personnel de préciser que tout logiciel ou produit développé par l'employé pendant les heures de bureau ou même en dehors, du moment que l'employé a bénéficié de l'assistance directe ou indirecte de l'entreprise soit la propriété de l'employeur. En effet, le droit belge n'a pas encore suivi l'exemple de la loi française du 3 juillet 1985, laquelle affirme qu'à partir du 1er janvier 1986, la propriété des droits sur les softwares développés par les employés sont acquis par l'employeur, sauf convention contraire explicite.

## IV. Les clauses particulières dans les contrats de maintenance

La continuité d'un système d'information exige sa maintenance. Les prestations de maintenance sont souvent le fait des fournisseurs eux-mêmes, parfois de société spécialisées. La maintenance d'un système d'information est rarement l'objet d'un contrat global, mais se décompose le plus souvent en de multiples contrats sur chaque élément du système.

Le caractère indispensable de la maintenance est reconnu par tous les utilisateurs. Ainsi, aucun logiciel n'est exempt d'erreurs et les modifications de son environnement tant technique que fonctionnel, exigeront des adaptations. Il est donc rappelé aux utilisateurs que, dès la commande, et non après la signature du contrat de vente d'un élément du système, la maintenance de celui-ci doit être garantie même si le paiement des redevances de maintenance est logiquement différé à l'expiration des périodes de garantie prévues dans le contrat de fournitures. En effet, il n'est pas certain que les juges condamneraient le fournisseur qui n'ayant signé qu'un contrat de fournitures refuserait de prester des services de maintenance.

En ce qui concerne le contenu du contrat de maintenance "hardware", portant sur les "mainframe" que sur les différents éléments "terminaux" (micro-ordinateurs - stations de travail - terminaux au sens strict), on aura soin de relever :

- les éléments exclus de la maintenance (par exemple, ceux d'origine étrangère, ceux non utilisés en conformité avec les spécifications techniques);

- le temps, la durée et la fréquence des visites de maintenance (et le droit de modifier ces conditions);

- les conditions de résiliation de la maintenance éventuellement non similaires dans le chef des deux parties;

- en cas de panne, les conditions d'intervention du prestataire (temps d'intervention, qualité des intervenants, délai de réparation, sanctions en cas de non réparation,...)

La maintenance logiciel exige des clauses plus concrètes encore. Un contrat de logiciel doit clairement distinguer les prestations de maintenance correction et celles de maintenance adaptation. La maintenance correction vise toutes les activités liées à la détection et à la correction des erreurs. La maintenance adaptation vise toutes les activités d'adaptation du logiciel à des besoins nouveaux et différents de ceux couverts par l'analyse fonctionnelle initiale.

En ce qui concerne la maintenance correction, outre les points déjà relevés à propos du hardware, on mentionnera :

- la nécessité de définir ce que l'on entend par erreur, c'est-à-dire par divergence par rapport aux spécifications du système (fonctionnelles ou techniques).

- les considérations de prise en considération de l'erreur (le signalement au fournisseur, la reproductibilité, la non-modification du logiciel par le client, etc)

- l'utilité et les modalités de la tenue d'un logbook, c'est-à-dire d'un journal reprenant un résumé succinct des défaillances constatées et des interventions du fournisseur.

- la nécessité d'une définition d'un taux minimal de disponibilité du système (par exemple calcul d'un Mean Time Between Failure). L'indisponibilité du logiciel sera partielle ou total, elle entraînera directement ou indirectement l'indisponiblité d'autres éléments du système. On prévoira également les sanctions attachées à tout dépassement de ce taux.

- l'obligation absolue ou conditionnelle d'intégration des releases (l'implémentation d'une release peut entraîner des perturbations dans le fonctionnement d'autres programmes).

La maintenance adaptation soulève essentiellement les questions suivantes :

- le droit de l'utilisateur à exiger une adaptation à certaines modifications de l'environnement (exemple ; adaptation à une nouvelle législation, calcul de nouveaux ratios);

- le coût de ces modifications (travail en régie ou sur devis)



Enfin, il est bien certain que de façon générale, la qualité du prestataire de ces services de maintenance logiciel est un élément important et que l'utilisateur cherchera, par des clauses de non-cession ou de cession avec agrément de l'utilisateur, à se prémunir contre un changement de partenaire. On rappelle que la clause de dépôt chez un tiers des programmes maintenus, le protègera contre une cessation des activités du prestataire des services de maintenance.

## V. Les clauses particulières dans les contrats télématiques

L'utilisation combinée de l'informatique et des télécommunications, la télé-informatique, autorise les entreprises à mettre à la disposition de tiers, leurs ressources informatiques et ceci, tant pour échanger de l'information qu'éventuellement conclure des contrats.

Les applications bancaires sont certes les plus connues; des services télématiques bancaires offerts à des clients professionnels ou non, ou interbancaires existent : ils permettent la consultation des comptes, des transactions bancaires et l'accès à des bases de données financières. En dehors du monde bancaire, se développent également des services de "Time Sharing", de courrier électronique et d'accès à des bases de données.

De tels services font naître de nouveaux problèmes de sécurité, l'identification des parties, l'authentification et l'intégrité des messages (absence de fraude et d'erreurs), la détermination des responsabilités en cas de mauvais fonctionnement du service, la protection des biens informationnels constitués par les entreprises et mis à la disposition de tiers par ces services.

Chacun de ces points est l'objet de brefs développements.

1. en ce qui concerne l'identification des parties, des solutions techniques ont été proposées (codes secrets, cryptographie des messages. En l'état actuel de notre législation, il est utile pour l'entreprise qui met à disposition des services télématiques, de prévoir que l'utilisation de tels codes équivaut à une signature et est sous la responsabilité exclusive de l'utilisateur, le concept signature ne permettant pas encore d'englober de telles méthodes de signature électronique.

   en ce qui concerne l'authentification des messages et la responsabilité en cas de fraude ou d'erreur ou, plus généralement, de mauvais fonctionnement du service, vu l'absence d'une législation sur la preuve adaptée aux nouvelles technologies de communication de l'information, la plupart des entreprises qui offrent des services télématiques prévoient dans leurs contrats que les documents informatiques tenus par elles (sur disquettes, bandes magnétiques ou microfilms) constitueront une preuve valable des transactions conclues et de leur contenu. Certaines entreprises (en particulier les banques) excluent toute responsabilité en cas de réception de messages non normalisés.

Enfin, étant donné la multiplicité des intervenants, (le transporteur, les intermédiaires), se développent des règles a priori de partage de responsabilités auxquelles les utilisateurs doivent adhérer (ex : les règles SWIFT à propos des messages bancaires internationaux). De telles règles s'avèrent nécessaires étant donné la difficulté de localiser le mauvais fonctionnement dans un réseau de télécommunication, incluant parfois des transmissions par satellites.

On note également les clauses prévoyant une évaluation forfaitaire des dommages subis par l'utilisateur; ces clauses s'expliquent étant donné la difficulté d'évaluer les dommages, conséquence directe ou indirecte du non ou mauvais fonctionnement d'un service télématique (ex : un retard de paiement peut entraîner la faillite d'une entreprise).

3. enfin, l'entreprise qui met à disposition de tiers des services télématiques, entend protéger le travail de création intellectuelle que peut constituer la base de données. Des clauses prévoient que l'utilisateur non seulement ne peut vider la base de données, mais également ne peut commercialiser les informations acquises dans le cadre du contrat.

## VI. Les contrats de back-up

On connaît les conséquences désastreuses des pannes affectant un élément ou l'ensemble du système informatique d'une entreprise. C'est pourquoi, certaines entreprises fortement dépendantes de l'activité du système de traitement de l'information, prévoient un système de back-up complet, parfois dans des locaux séparés de ceux du Centre de Traitement de l'Information. Des connexions permettent à ce système de back-up de prendre le relais immédiat du système central, des copies de sécurité des programmes, la duplication partielle ou totale des informations traitées, permettent une redémarrage des opérations de traitement de l'information dans des conditions optimales.

L'entreprise peut estimer que le coût de la création et de la maintenance d'un système de back-up est dirimant, et se tourner alors vers une autre entreprise pour conclure un contrat de back-up.

Tantôt de tels contrat sont conclus sur une base de réciprocité, deux entreprises ayant des systèmes compatibles et le même besoin de système de sécurité; tantôt ils sont offerts par des entreprises spécialisées, en particulier des fournisseurs.

Quel est le contenu de tels contrats ? Il est en effet important que les parties soient parfaitement conscientes de leurs droits en cas d'incidents :

- une clause définira avec précision les situations dans lesquelles une partie, dont le Centre de Traitement de l'Information rencontre des difficultés, peut avoir recours au système de back-up.



La précision en la matière est obligatoire pour éviter des controverses avec le contractant, lorsque l'accès au système de back-up est demandé. Souvent on prévoit que ce droit n'existera pas lorsque le non fonctionnement du Centre est dû à une faute du responsable du Centre et avant une durée de panne minimale.

une clause établira la modalité d'appel au système de back-up; la procédure de notification spécifiera le moment exact de l'appel au secours et l'ordre de priorité en cas d'appels concommittants de diverses entreprises au Centre de back-up.

- une clause décrira le service de back-up offert et indiquera quel type d'assistance le personnel du Centre de back-up peut prêter.

- une clause définira les modifications à faire par les entreprises pour que leurs deux systèmes restent à tout moment compatibles. A défaut pour une entreprise d'exécuter de telles modifications, le contrat sera révoqué à ses torts.

en ce qui concerne le paiement, les parties détermineront qui supportera les coûts de la télécommunication.

enfin, il est indispensable que l'entreprise qui offre un service de back-up, garantisse, au nom de ses employés et de ses propres contractants, à l'entreprise qui demande un tel service, la parfaite confidentialité des données auxquelles il aura accès en cas de recours au système de back-up.

## VII. Les contrats d'assurances

S'il convient de rendre les utilisateurs attentifs à la nécessité qu'il y a d'assurer eux-mêmes la protection de leurs systèmes tant par des clauses appropriées dans les relations avec les tiers que par des mesures techniques, il n'en reste pas moins vrai que ces protections ne sont jamais absolues et qu'en dernier recours, les entreprises auront recours aux assureurs.

On notera d'ailleurs que ceux-ci exigeront avant de proposer leur couverture, que l'entreprise dispose d'un système adéquat de protection. Certaines compagnies imposent même un audit préalable.

Quels types de contrats d'assurances sont proposés en matière informatique ? En cette matière, le marché est en pleine expansion et chaque mois amène de nouvelles polices. Ainsi, une compagnie a proposé récemment une "Assurance de bonne fin de projets informatiques". Cette police permet de garantir qu'un projet d'informatisation soit mené jusqu'à son terme et implique que la compagnie d'assurance soit mêlée dès le départ au projet et aux relations entre l'entreprise et le fournisseur et qu'en cas de défaillance de ce dernier, elle puisse substituer un tiers pour l'achèvement de l'opération.

D'autres polices d'assurance informatique sont plus classiques. On se contentera ici d'épingler quelques caractéristiques de ces polices.

- Les assurances de choses sont celles qui ont pour but d'indemnisation des pertes patrimoniales pouvant résulter de la destruction, de la disparition ou de la perte de valeur d'une chose corporelle ou incorporelle, par suite de la réalisation du risque.
  Elles peuvent couvrir le système informatique ou un élément de ce système.

  Si une bonne assurance de choses dans le secteur informatique devra couvrir à la fois le matériel, les logiciels, les périphéries et les interfaces, généralement les polices restreignent leur couverture au seul matériel. Des compagnies proposent autant d'assurances que de type d'éléments. L'utilisateur veillera alors à ce que le même élément ne soit pas l'objet de deux assurances.

  On note enfin que la couverture des risques liés au développement et à l'exploitation des logiciels d'application sur mesure est généralement exclue des assurances de choses et couverte par une assurance en responsabilité civile.

  Les risques couverts varient suivant le type d'assurance. Les contrats mis sur le marché sont du type "multirisques" et revêtent la forme de police "tous risques ordinateurs" ou "tous risques électroniques". Ces polices sont conçues selon un schéma traditionnel, définition des risques couverts et des risques exclus. Les compagnies américaines ont introduit la particularité des polices "tous risques sauf" qui ne définissent que les risques exclus.

  On s'attachera plus particulièrement à cette catégorie des "risques exclus". Parmi les risques exclus, certains risques le sont du fait de la loi (risques de guerre, risques résultant de la faute grave, de l'armée, etc..., risque du profit espéré (encore que cela soit contesté)); d'autres sont propres à l'informatique, parmi ces derniers, on relève notamment les incidents dus à des utilisations non conformes aux spécifications du fournisseur, les risques déjà couverts par les garanties du fournisseur et surtout la perte de données qu'elle soit due à une erreur de programmation, un effacement par erreur où l'action de champs magnétiques étrangers.

  Les indemnités accordées en cas de sinistre couvert par la police d'assurance sont calculées sur la base de la valeur à neuf des objets assurés.

  En cas de sous-assurance, la règle proportionnelle joue.
  La somme assurée sera fonction idéalement : des conditions d'exploitation habituelles dans l'entreprise : nature, volume, importance de chaque catégorie de médias, existence de doubles de programmes ou de générations antérieures de fichiers et des modalités de reconstitution envisagées en cas de sinistre.



On se couvrira en outre par des polices particulières :

1. contre les frais supplémentaires d'exploitation, à savoir les frais de dépannage, recours à des procédures de back-up, engagement de personnel intérimaire, etc...

2. contre les pertes d'exploitation dues à la panne ou la défaillance du système informatique.

3. contre la fraude informatique, c'est-à-dire le fait pour une personne de falsifier ou de copier un programme ou des données pour s'en servir contre le gré de celui ou de ceux qui ont un titre légitime pour le faire.

   Une bonne assurance "fraude Informatique" doit couvrir non seulement les risques propres de l'entreprise, mais également la responsabilité de cette dernière vis-à-vis de tiers (retard dans l'exécution de prestations vis-à-vis de clients, divulgation de données confidentielles, etc...). On note que certaines polices ne couvrent pas la fraude d'employés de l'entreprise (ceci peut être grave car bien souvent la fraude sera le fait du personnel de l'entreprise) comme il a été dit au point III), ni les dommages indirects comme la perte de know how et le dommage commercial résultant de la perte de la clientèle.

2. Les assurances en responsabilité sont destinées à réparer le dommage que subit le patrimoine de l'assuré lorsque ce dernier, auteur responsable d'un préjudice fait l'objet d'un recours exercé contre lui par un tiers.

   Cette fois, c'est bien souvent l'entreprise qui exigera de ses fournisseurs, en particulier de sociétés de Conseil en Informatique, la prise de telles polices, afin de prévenir toute défaillance ou toute mauvaise exécution par ces derniers, des prestations, objet du contrat. Non seulement, elle exigera la prise d'une police d'assurance spécifique au marché avec stipulation du paiement des indemnités à son profit, mais demandera communication du contrat d'assurance. L'entreprise sera attentive aux risques exclus. En effet, certaines polices excluent les dommages résultant à la fois du retard dans l'accomplissement des prestations et du mauvais choix du système par rapport aux besoins du client.

   Il est clair que l'entreprise se couvrira de même par une assurance en responsabilité lorsque l'ordinateur qu'elle a acquis lui sert pour l'accomplissement de prestations vis-à-vis de tiers, c'est le cas en particulier pour les contrats télématiques dont nous avons parlé au point V.

## VIII. Droit pénal et sécurité informatique

Au contraire d'autres pays, la Belgique ne dispose pas encore de législation spécifique relative à la fraude ou au crime informatique, c'est-à-dire aux délits où l'ordinateur est l'instrument ou l'objectif de l'acte délinquant.

Cette législation spécifique ne peut être nécessaire,; étant donné la difficulté d'application de nos textes pénaux soumis au principe de l'interprétation restrictive.
A la suite de Melle ERKELENS, on distinguera les types de délits suivants :

- la manipulation de données, c'est-à-dire soit la falsification par introduction de données fausses ou par modification de données stockées, soit par détérioration de données. La manipulation des données ne pourra que dans des cas exceptionnels être poursuivie. Elle pourra l'être sur base de l'escroquerie si la manipulation produit une remise effective d'une chose et s'est faite grâce à un faux nom ou de fausses qualités;

- l'espionnage informatique, c'est-à-dire l'acquisition et/ou l'utilisation illicite de données, ne sera sanctionné que si les données secrètes acquises sont par la suite utilisées vis-à-vis de tiers pour servir au titulaire de ces données.
  La sanction sera alors la violation du secret professionnel ou de fabrique, voire l'acte contraire aux usages honnêtes;

- le sabotage informatique entraîne condamnation dans la seule mesure où il y a détérioration du matériel. La détérioration ou destruction du software n'est pas en elle-même sanctionnée;

- l'accès non autorisé aux données et aux transmissions de ces données n'est pas en soi répréhensible pénalement, le piratage de programmes a été considéré comme un vol par une décision récente du tribunal correctionnel d'Anvers le 13 décembre 1984, nonobstant le fait qu'en l'occurence il n'y avait point de soustraction du support.

Ainsi, la peur du gendarme ou plutôt de la répression pénale est un bien faible argument à l'heure actuelle pour dissuader les éventuels délinquants et garantir ainsi la sécurité informatique.



## CONCLUSION

1. Le droit a quelque chose à dire en matière de sécurité informatique.

2. A chaque type de risque, la technique juridique propose une couverture directe ou indirecte. Couverture indirecte lorsqu'il s'agit de conforter une sécurité technique, logique ou managériale : ainsi lorsque par une clause décrite ci-dessus, je puis obtenir la garantie qu'un logiciel possèdera un programme automatique de vérification de cohérence des données introduites ou que mes employés ne divulgueront pas certaines données de mon entreprise.

   Couverture directe, lorsque le droit intervient pour couvrir un risque qui n'a pu être couvert par les sécurités technique, logique ou managériale, ainsi, les divers contrats d'assurance qui interviennent en cas de défaillance des autres types de sécurité.

3. Diverses branches du droit concourrent à assumer cette sécurité informatique : droit des contrats, droit du travail, droit pénal, droit des assurances.

4. Il serait utile pour toute entreprise ayant identifié les divers risques encourus par la mise sur pied d'un système d'information de réfléchir plus systématiquement aux solutions juridiques qui peuvent être apportées à chacun de ces risques, en renfort ou en substitut d'autres solutions.

5. Enfin, ces diverses solutions juridiques doivent être étudiées dans leur complémentarité. Il est certain que l'exigence contractuelle de certaines qualités du logiciel entraîne logiquement la réclamation d'une couverture du fournisseur par un contrat d'assurance et des clauses de maintenance permettant de garantir la continuité de ces qualités tout au long de la vie du système.