Université de Montréal

LA CONVERGENCE DE LA SÉCURITÉ INFORMATIQUE ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL :

VERS UNE NOUVELLE APPROCHE JURIDIQUE

par

Ana I. Vicente

Faculté de droit

Maîtrise (LL.M.), option Nouvelles technologies de l'information

Table des matières

«Code is Law.»
- Lawrence Lessig

«Tout grand ordre contient un petit désordre.»
- Goethe

Introduction[♣]

L'émergence d'une structure d'information globale a eu un impact inattendu sur l'économie et la société en général. L'un de ces impacts est sans doute le fait que l'information soit devenue une ressource cruciale, sinon la source la plus importante de notre économie. Ce culte de l'information est fondé sur la croyance que plus on dispose de grandes quantités d'information, meilleure sera la compréhension d'une situation et les décisions qui en découlent[1]. La collecte des renseignements personnels n'échappe sûrement pas à cette vision. Ce type d'information a acquis une « valeur marchande, est devenu un bien commercial menant à la compétitivité commerciale dans un environnement où la concurrence est de plus en plus vive »[2]. Certes, le phénomène n'est pas nouveau. Mais, les performances des ordinateurs dans le traitement de l'information rendent techniquement réalisables des choses jusqu'ici hors de portée et ont accéléré le développement d'activités lucratives connexes répondant aux besoins de personnalisation des services comme dans le domaine du crédit à la consommation et du marketing direct. Dans ces domaines, des données personnelles sont collectées et accumulées, bien souvent sans la connaissance de la personne concernée, et utilisées dans un but autre que celui énoncé lors de la collecte d'origine.

À la lumière de cette réalité, il s'est développé un intérêt commun de la société pour la « protection adéquate »[3] des données à caractère personnel et plusieurs efforts législatifs ont été mis en oeuvre. Cependant, entre le progrès technologique de la capacité de traitement des systèmes d'information, progrès qui nous ferait croire que la tendance serait à la centralisation des bases de données, les renseignements personnels continuent à être accumulés et utilisés de manière décentralisée. Ces renseignements ne sont pas seulement manipulés en volume et traités par de larges systèmes informatiques, mais aussi par les divers ordinateurs moins puissants des entreprises, surtout les petites et moyennes entreprises, où la sécurité est moins bien gérée.

Cette diversification de traitement a augmenté le risque de maniement, de modification et d'accès de l'information personnelle par ceux qui non pas l'autorisation ou qui manque de formation, mettant en péril les principes de protection établis par les textes de loi. Et l'anxiété engendrée par la sensation de « perte de contrôle » s'accroît avec la diffusion des renseignements sur les réseaux de communication. Une fois « en ligne », les données

---

[♣] Mise en garde : plusieurs documents ont été consultés sur des sites électroniques, mais tous les liens hypertexte ont été vérifiés et étaient à jour au moment de dépôt de ce mémoire (juillet 2003).

[1] Theodore ROSZAK, The Cult of Information, The Folklore of Computers and the True Art of Thinking, Phanteon Books, New York, 1986.

[2] Commissaire à la protection de la vie privée, Rapport Annuel 1992-1993, p. 4 et 9.

[3] Voir, par exemple, l'article 25, par. 1 de la Directive 95/46/CE sur la vie privée prévoyant qu'un transfert de données à caractère personnel « ne peut avoir lieu que si […] le pays tiers en question assure un niveau de protection adéquat. »

personnelles peuvent être instantanément distribuées à un grand nombre de tiers, souvent hors frontières, ce qui explique le besoin croissant de l'harmonisation des mesures de protection, tant juridiques que techniques, des données personnelles.

Jusqu'à récemment, plusieurs étaient ceux, à l'exception des milieux spécialisés comme le milieu bancaire, l'aérospatiale et militaire (qui dépendent grandement des systèmes informatiques stables et sécuritaires), qui ne connaissaient rien à la sécurité informatique ou qui la considéraient négligeable. Pourtant, de plus en plus, les consommateurs, les compagnies et les gouvernements réalisent l'importance de la sécurité, surtout dans la sauvegarde de leurs droits fondamentaux. Donner une protection adéquate à cette information est devenu un enjeu important, particulièrement si l'on considère l'exposition croissante à divers types de risques et menaces, notamment l'accès non autorisé, les modifications ou destruction de l'information, refus de services, virus et même les attaques psychologiques[4] au sein de l'entreprise.

D'où vient donc ce changement de mentalité ? La raison la plus probable est sans doute expliquée par le changement culturel à long terme que nous traversons. La sécurité informationnelle a pris de l'importance au cours des dernières années dans plusieurs aspects commerciaux et personnels de notre quotidien ; nous sommes de plus en plus dépendants de la technologie informatique.

> « Computing, in short, is in the midst of a transition from an optional tool to a ubiquitous utility. And people expect utilities to be reliable. One definition of a utility, indeed, is a service that is so reliable that people notice it only when it does not work. Telephone service (on fixed lines, at least), electricity; gas and water supplies all meet this definition. Computing clearly does not, at least not yet. »[5]

Or, malgré les obligations de confidentialité imposées par les diverses lois[6] en la matière, les fichiers de renseignements personnels demeurent encore des paniers percés et ces failles de sécurité se produisent tant au sein des entités gouvernementales que dans les entreprises privées. Le problème provient du fait que leur sécurité soit mal assurée, les responsables sont négligents, de nombreuses personnes non autorisées ont accès aux informations et quelques-unes participent au marché noir des renseignements personnels[7].

Par exemple, le 11 mars dernier, le ministre des Ressources humaines de la Colombie-britannique a avisé 568 personnes sur la nécessité de garder l'œil ouvert sur leurs comptes bancaires et cartes de crédit, après avoir découvert que des informations personnelles et confidentielles avaient été volées durant un accès illicite au système informatique du ministère. Cette faille de sécurité survient quelques semaines après qu'une situation similaire se soit produite dans la ville de Regina. Là, un disque dur d'un ordinateur de la compagnie ISM Canada, inc. comprenant des renseignements personnels relatifs à plus d'un million de personnes a été volé. Richard Chambers, le porte-parole du ministère avoue que « there's a

---

[4] L'attaque psychologique se traduit par le recueil d'informations auprès de ceux qui les utilisent mettant en œuvre des procédés basés sur la tromperie et l'obscurcissement. Pour un exemple, voir Donald PIPKIN, Sécurité des Systèmes d'Information, Campus Press, 2000, p.227.

[5] Tom STANDAGE, « Securing the Cloud: a Survey of Digital Security », The Economist, 24 octobre 2002, en ligne: The Economist <http://www.economist.com>.

[6] Pour les lois étudiées dans ce travail de recherche voir Partie I, Chapitre 2.

[7] Rappelons-nous, par exemple, des fuites de renseignements personnels à la Société de l'assurance automobile du Québec en 2001.

concerns the information, which was contained on the computer equipment stolen from the office, could be used illegally. Social Insurance numbers, birth dates and addresses of clients and staff were stored on the stolen computers. »[8]

Ceci n'est qu'une illustration parmi tant d'autres. Toutefois, l'alarme doit être donnée, puisque ce type d'incident ayant tendance à survenir fréquemment. Ce mémoire essaie justement de répondre à cette nouvelle menace pour les droits fondamentaux des individus et peut servir de guide juridico-technique à tous ceux concernés par la mise au point de la sécurité des systèmes d'information. Il se veut, d'abord, une initiative tangible vers une meilleure prise en charge des mesures de protection des renseignements personnels dans le contexte de l'imputabilité de la responsabilité des gestionnaires des systèmes d'information. Ensuite, il tente d'offrir également une réponse aux membres de la communauté juridique qui souhaitent mieux connaître la teneur des éléments d'un programme global de sécurisation des systèmes informatiques et les implications pour les entreprises. Mais surtout, ce mémoire met le doigt sur la réalité du droit des nouvelles technologies, celle d'une culture de coopération et de co-existence grandissante entre le droit et la technique.

Les deux parties de ce mémoire visent essentiellement à mettre en évidence cette culture de coopération qui doit exister entre le droit et la technologie. La première partie explore les divers textes de loi et principes internationaux applicables aux renseignements personnels et à l'obligation d'assurer la sécurité de ceux-ci ainsi qu'à l'étude du caractère plus théorique du programme de sécurisation des informations personnelles de l'entreprise (politique de sécurité et analyse des risques). La deuxième traite de la manière d'atteindre un niveau adéquat de sécurité exigé par la loi, plus spécifiquement des mesures à adopter pour assurer la sécurité des actifs informationnels de l'entreprise et la protection des renseignements personnels. Nous parlerons alors des mesures organisationnelles, techniques et logiques qu'il importe de mettre en place.

ꕥ

Partie 1. Les fondements juridiques de la sécurité des données à caractère personnel

Normalement, un droit se traduit par une obligation. Dans notre cas, le droit d'une personne à la protection des renseignements personnels qui la concernent se traduit par l'obligation imposée aux entités qui collectent des données personnelles de respecter et de mettre en application chacun des principes et des règles de protection énoncées par la loi, dès le moment où le renseignement est recueilli, jusqu'à sa destruction. C'est justement à cette relation droit-obligation que la première partie de ce mémoire est consacrée.

[8] Allison LAWLOR, « Hundreds warned as data disappears », The Globe and Mail, 11 mars 2003, édition électronique en ligne: <http://www.globeandmail.com/>.

Chapitre 1. Exposé sur les concepts et les principes fondamentaux en matière de protection des renseignements personnels

Section 1. La définition des concepts de vie privée, protection des renseignements personnels et sécurité informationnelle

1.1. Qu'est-ce que le droit à la vie privée ?

Nous pouvons dire que la notion de vie privée, concept qui diffère de celui de renseignement personnel, paraît être un concept si bien compris que personne ne peut le définir. Les composantes de la vie privée n'ont pas fait l'objet d'une définition ou d'une énumération limitative afin d'éviter de limiter la protection aux seules prévisions légales. D'une manière générale, les tribunaux ont appliqué le principe de cette protection au droit à la vie sentimentale, à la vie familiale, au secret relatif à la santé, au secret de la résidence et du domicile et au droit à l'image.

Il a déjà été reconnu en droit civil québécois que le droit à la vie privée protège la personne contre une intrusion qui aurait pour effet de la gêner[9]. Le juge Baudoin de la Cour d'appel du Québec a défini la vie privée dans l'affaire Godbout[10]: « le concept de vie privée me paraît beaucoup plus, comme le Tribunal des droits de la personne le mentionne dans Dufour c. Centre Hospitalier St-Joseph de la Malbaie, [1992] R.J.Q. 825, destiné à protéger ce qui fait partie de la vie intime de la personne, bref ce qui constitue un cercle personnel irréductible, à l'abri des indiscrétions. »

Bien que la vie privée soit une notion difficile à définir avec précision, les catégories de vie privée ont été identifiées par la Cour Suprême du Canada, dans l'arrêt Dyment[11], catégories qui s'articulent respectivement sur les notions de protection de l'espace entourant la personne (protection classique par les garanties relatives aux perquisitions, aux fouilles et saisies), de protection de la personne elle-même (qui se fonde sur la dignité et de protection de l'information.

Cette protection est cruciale, car l'information ainsi dévoilée est liée à un ensemble d'autres droits et valeurs fondamentales tels que la liberté, la liberté d'expression et la liberté d'association. Si l'on ne peut adéquatement exercer un contrôle sur la circulation de ces informations, on risque de voir ses droits brimés. Dans l'arrêt Dyment, la cour, sous la plume du Juge La Forest, s'exprime à ce sujet que :

> « Selon ce que nous dit Westin, la société a fini par ce rendre compte que la notion de vie privée est au cœur de celle de la liberté dans un État moderne […] Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle méritait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. »[12].

---

[9] H. Patrick GLENN, « Le droit au respect de la vie privée », (1979) 39 R. du B. 879, 881.
[10] Godbout c. Longueuil (Ville de), J.E. 95-1848 (C.A.), p.17.
[11] R. c. Dyment, [1998] 2 R.C.S. 417.
[12] R. c. Dyment, [1998] 2 R.C.S. 417, 441, dans Patrick GINGRAS, Analyse juridique des méthodes de protection des renseignements personnels sur Internet, Mémoire de Maîtrise (LL.M.), Faculté des études supérieures, Université de Montréal, août 2000, p. 10.

Donc, nous pouvons dire que le droit à la vie privée est vu comme le droit au respect de la vie privée, permettant à une personne de choisir, dans quelles circonstances et dans quelle mesure elle accepte de s'exposer elle-même aux autres . La détermination de l'atteinte au droit dépendra du contexte et de l'environnement dans lequel elle se produit[13].

Mais dans tous les cas, lorsque la personne décide de donner des données personnelles à un tiers, elle s'attend à ce que ces données ne soient pas divulguées à n'importe qui, créant ainsi une expectative de confidentialité et de sécurité. Ainsi, si l'individu est répertorié, peu importe que la banque de données soit, gouvernementale ou privée, il doit s'attendre à ce que le caractère confidentiel des renseignements qu'il transmet soit protégé, notamment, que l'accès aux renseignements soit accordé uniquement aux personnes qu'en ont véritablement l'autorisation.

1.2. La protection des renseignements personnels

La protection des renseignements personnels est un droit de la personne que l'on désigne souvent comme le droit à son intimité ou le droit à l'anonymat. C'est un « sous-ensemble de la protection de la vie privée, [dont] l'objectif […] est de donner la possibilité à chacun de décider quand, comment et dans quelle mesure il souhaite partager avec des tiers des renseignements qui le concernent » . Nous pouvons aussi parler d'autodétermination informationnelle ou d'un droit de regard sur ses données personnelles. Ce droit comprend la capacité de contrôler les renseignements recueillis à son propre sujet (âge, numéro d'assurance sociale, orientation sexuelle, dossier médical, évaluation du rendement, droit aux avantages sociaux et autres) et la façon dont ces renseignements sont utilisés, accessibles, conservés, divulgués ou détruits. Comme dans tout autre domaine de la sécurité informatique, les renseignements personnels doivent être protégés durant tous les moments de leur cycle de vie.

Afin de bien cerner la question, il est important de définir les diverses expressions entourant la protection des renseignements personnels et de comprendre ce qui est exclu de celle-ci, permettant ainsi de faciliter la gestion de la sécurité de l'entreprise et centrer les efforts de sécurisation des données favorisant ainsi le respect des obligations légales qui lui sont imposées.

D'après le Grand dictionnaire terminologique[15], le terme « renseignement personnel » est défini comme étant une « information de caractère non public concernant une personne physique et permettant de l'identifier, directement ou indirectement. » Les mêmes expressions ont été retenues dans la Directive 95/46/CE[16] du Conseil européen. Son deuxième article dispose que les « données à caractère personnel » peuvent être « toute information concernant une personne physique identifiée ou identifiable […] » et « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, culturelle ou sociale […]».

---

[13] Pierre TRUDEL (dir.) et *Al.*, Droit du cyberespace, Éditions Thémis, 1997, p. 11-26 et ss.
[15] Le Grand dictionnaire terminologique, en ligne : <http://www.granddictionnaire.com/>.
[16] Directive 95/46/CE du Parlement européen et du Conseil de l'Europe du 24 août 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E., 23 novembre 1995, n°. L.282, p.31, en ligne : <http://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html> [ci-après Directive 95/46/CE].

Au Québec, ce n'est pas le Code Civil[17] qui nous fournit la définition de renseignement personnel, mais bien la Loi sur la protection des renseignements privés dans le secteur privé[18]. Le Code se limite à énumérer, aux articles 35 à 41, les droits et obligations, notamment le droit d'accès et de rectification, relatifs au respect de la réputation et de la vie privée. La Loi sur le secteur privé, à article 2, dicte une définition identique à celle contenue dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[19]: « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. » Cette définition est aussi très proche de ce qui se dit dans la Loi fédérale.

Dans la jurisprudence du secteur privé, la Commission d'accès à l'information a défini la notion de renseignement personnel dans l'affaire Claude Stébenne c. Assurances générales des Caisses Desjardins[20]. La commission prévoit que la définition de « renseignement personnel » dans la Loi sur le secteur privé concorde avec celle retenue par le législateur au moment de l'adoption de la Loi sur l'accès de 1982 :

> « Il n'y a là ni hasard, ni redondance. C'est l'expression d'une évidence qui correspond au sens commun. Il ne peut y avoir deux, encore moins plusieurs, notions de renseignements personnels. Un tel renseignement ne change pas de nature selon qu'il est traité par un agent de la fonction publique ou par le préposé d'une entreprise. »

Dans le secteur public, dans l'affaire Ségal c. Centre de services sociaux de Québec[21], la Commission d'accès à l'information a identifié trois éléments importants dans la définition de l'article 54 de la Loi sur l'accès. Il s'agit des mots « renseignements », « concerne » et « identifier ». Faisant référence au dictionnaire, la Commission a précisé les éléments suivants :

> « À l'aide de ces définitions des dictionnaires, on peut affirmer qu'un renseignement nominatif […] doit non seulement faire connaître quelque chose à quelqu'un et avoir rapport avec une personne physique, mais il doit aussi être susceptible (permettre) de distinguer cette personne par rapport à quelqu'un d'autre ou de reconnaître sa nature. »

Un renseignement doit faire connaître quelque chose à quelqu'un. Il s'agit d'une donnée objective que l'on porte à la connaissance de quelqu'un et doit avoir un rapport avec une personne physique. Les renseignements concernant les personnes morales, c'est-à-dire les entreprises, les organismes, les syndicats, etc., ne sont pas personnels. Le renseignement doit permettre de reconnaître la nature d'un individu, de le distinguer par rapport à quelqu'un d'autre, par rapport aux différentes classes ou catégories d'individus (caractéristiques de cet individu).[22]

---

[17] Code Civil du Québec, L.Q. 1991, c. 64 [ci-après C.c.Q.].
[18] L.R.Q., c. P-39.1. [ci-après Loi sur le secteur privé].
[19] Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels, L.R.Q., c. A-2.1. [ci-après Loi sur l'accès des organismes publics].
[20] Claude Stébenne c. Assurances générales des Caisses Desjardins, [1994] C.A.I. (94 03 66).
[21] Myriam Ségal c. Centre de services sociaux de Québec, [1988] C.A.I. 315 (88 01 92); voir aussi Antonio Sergi c. Ville de Mont Royal, [1997] C.A.I. 198 (97 01 67).
[22] Diane POITRAS et Lina DESBIENS, Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, textes annotés , S.O.Q.U.I.J., 1996, p. 269 dernier paragraphe.

Ainsi, un renseignement, indépendamment de son support et de sa forme, deviendra personnel s'il permet à une personne raisonnablement informée d'identifier la personne concernée, c'est-à-dire, « si la divulgation d'un renseignement peut permettre une identification en fonction du critère objectif de la personne raisonnablement informée en général, donc sans tenir compte des connaissances particulières de la personne »[23]. Ce sont les circonstances, au cas par cas, qui déterminent la possibilité d'identifier la personne concernée par le renseignement. Il se peut que plusieurs données qui en soi ne sont pas considérées comme personnelles le deviennent si à la lecture même du document, le lecteur peut déduire de qui il s'agit. Par exemple, un groupe de renseignements pourra permettre l'identification, sans que le nom de la personne concernée n'apparaisse.

Dès lors que l'information conservée par une entreprise permet « d'isoler » un individu, on peut la considérer comme un renseignement personnel, peu importe sa forme : objective ou mathématique[24] et suffit simplement que l'information concerne une personne physique et permette de l'identifier. L'entreprise devra donc se concentrer sur ces données puisque, ce sont ces dernières qui doivent être protégées par des *mesures de sécurité suffisantes*. Vous trouverez à l'annexe I, un tableau illustrant les renseignements considérés par la Commission d'accès à l'information comme personnels ou non.

Diverses lois et autres textes à portée juridique en matière de protection des renseignements personnels traitent souvent des termes « fichiers » ou « dossiers » de renseignements personnels. Il s'agit essentiellement d'un ensemble d'informations concernant une personne. Ces données, centralisées ou réparties sur plusieurs sites, font normalement l'objet d'un traitement automatisé ou sont structurées selon des critères déterminés, de manière à faciliter leur utilisation, leur mise en relation ou la prise de décision. Le dossier doit avoir un objet, par exemple, les dossiers médicaux ou les dossiers académiques.[25] De plus, lorsqu'on parle de « flux de renseignements personnels », on se réfère à l'ensemble des processus comprenant la collecte d'informations nominatives, leur transmission, leur entreposage, leur traitement, leur communication ainsi que leur utilisation dans divers processus de décision[26]. Nous verrons, dans la deuxième partie du mémoire, qu'un programme de sécurité informatique devra forcément envisager des mesures de protection pour chacune de ces étapes (cycle de vie des données personnelles) afin de garantir un niveau de protection adéquat à ceux-ci.

Au fédéral, la Loi sur la protection des renseignements personnels et les documents électroniques[27] contient sa propre définition de renseignement personnel, qui malgré sa ressemblance avec la définition québécoise, exclut expressément certaines informations de la notion de renseignement personnel. À l'article 2, la loi définit ce terme comme étant «[t]out renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéros de téléphone de son lieu de travail. »

---

[23] E. c. Office de la protection du consommateur, [1987] C.A.I. 350.
[24] Paul André COMEAU, « La vie privée : droit et culture », dans Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit, Les journées Maximillien-Caron 1995, Montréal Édition Thémis, 1995, p. 3.
[25] LE GRAND DICTIONNAIRE TERMINOLOGIQUE, précitée, note 15.
[26] Idem.
[27] Loi sur la protection des renseignements personnels et des documents électroniques, 1ère session, 36e législature, 46-47 Élizabeth II, 1997-1998, déposée le 1er octobre 1998 et réimprimée le 12 avril 1999 [ci-après PEPIDA (selon l'acronyme en anglais]. Voir aussi le calendrier de mise en œuvre de la loi, en ligne : <http://www.privcom.gc.ca/legislation/02_06_02a_e.asp>.

Malgré cela, on peut considérer des renseignements personnels, le nom d'un individu, un numéro d'identification, le numéro d'assurance sociale, le numéro d'assurance maladie, le numéro de permis de conduire, l'adresse du domicile, le numéro de téléphone du domicile, le sexe et l'âge. Outre ces informations, on estime que les informations recueillies à propos du revenu d'une personne, de son statut de propriétaire ou de locataire, ses résultats académiques, son comportement disciplinaire, ses diplômes, sa race, son statut social, sa condition économique, son état de santé, sa réputation, son comportement, ses déplacements, ainsi que sa présence dans un lieu[28], sont des renseignements personnels qui doivent être protégés.

Jusqu'ici, nous avons différencié les termes vie privée, renseignements personnels et les termes connexes à la matière. Il ne nous reste qu'à aborder l'expression sécurité informationnelle.

1.3. La définition du concept de sécurité informationnelle

Il nous paraît important de préciser que la notion de sécurité informationnelle est une notion distincte de la protection des renseignements personnels. Il est évident qu'une protection adéquate ne peut être donnée aux renseignements personnels sans des mesures de sécurité suffisantes. Cependant, la sécurité à elle seule ne permet pas d'assurer la protection des renseignements personnels, puisqu'elle n'est qu'un des principes fondamentaux de la protection accordée à ceux-ci. En fait, la protection des renseignements personnels renvoie au contrôle personnel sur les données concernant un individu, tandis que la notion de sécurité renvoie au contrôle organisationnel des informations personnelles.[29]

> « Les notions de sécurité et de protection de la vie privée n'ont pas la même signification. Cependant, les limitations imposées à l'utilisation et à la divulgation des données devraient être renforcées par des garanties de sécurité. Ces garanties comprennent des mesures d'ordre matériel (verrouillage des portes et cartes d'identité, par exemple), des mesures structurelles (telles que des niveaux hiérarchiques en ce qui concerne l'accès aux données) et, en particulier avec les systèmes informatiques, des mesures informationnelles (telles que le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face) ».[30]

Il faut surtout comprendre que le fait d'avoir des mesures de sécurité en place ne signifie pas nécessairement que la protection de la vie privée et les renseignements personnels, soit automatiquement assurée. Une mesure de sécurité efficace peut être insuffisante pour assurer la protection des renseignements personnels. Voyons, si d'une part certaines mesures de sécurité contribuent au respect de la confidentialité, d'autres en revanche constituent de véritables intrusions dans la vie privée des personnes. « Une transmission électronique, par exemple, peut être sécurisée de façon à préserver le caractère confidentiel de son contenu, mais être acheminée à une personne non autorisée à accéder aux renseignements qui y figurent. D'où le besoin d'évaluer la pertinence et l'efficacité des moyens de sécurité mis en œuvre afin de réserver aux renseignements personnels un usage qui respecte la finalité de leur

---

[28] P. GINGRAS, précitée, note 12, p. 19.
[29] Ann CAVOUKIAN (Information and Privacy Commissioner), « Privacy & Security: Totally Devoted », conférence donnée à Toronto le 7 novembre 2002, en ligne: Commissaire à la Vie Privée <www.ipc.on.ca>.
[30] O.C.D.E., Lignes directrices de l'O.C.D.E. sur la protection de la vie privée et les flux transfrontières des données de caractère personnel, 2001, Exposé des motifs du paragraphe 11, p. 47, par. 56.

collecte . »[31] Un exemple d'atteinte à la vie privée, est le contrôle des courriels des employés. Le C.c.Q. prévoit que le fait d'intercepter ou d'utiliser volontairement une communication privée peut être considérée comme une atteinte à la vie privée. En revanche, si l'employeur a émis des directives claires voulant que l'utilisation du courrier électronique à des fins personnelles au bureau soit interdite, il pourrait, dans certaines circonstances, être autorisé à consulter votre courrier électronique.

Comme nous l'avons dit ci-haut, la convergence de la protection des renseignements personnels et de la sécurité de l'information numérique, vise à première vue la notion de confidentialité. Toutefois, le champ d'intervention de la sécurité de l'information numérique inclut, en plus de la confidentialité, les préoccupations suivantes : la disponibilité de l'information, l'intégrité de l'information, l'authenticité et son irrévocabilité. Prenons le temps d'examiner chacun de ces concepts, puisqu'ils reviendront tout au long de ce mémoire et qui sont, à la base, les objectifs de la sécurité informationnelle.

D'abord, la confidentialité se résume à s'assurer que l'accès aux informations est donné seulement aux utilisateurs dûment autorisés. On préserve ainsi l'information entre les mains de ceux qui y ont un intérêt légitime. Ensuite, l'intégrité est maintenue en préservant la valeur et l'état de l'information, en d'autres termes, l'information est protégée de toute modification non autorisée. L'information a une valeur seulement si l'on est convaincu de son exactitude et l'un des objectifs capitaux d'une politique de sécurité est précisément de s'assurer que l'information n'est ni modifiée ni détruite ou détériorée de quelque façon que ce soit. Selon la Loi des technologies de l'information, l'intégrité est définie comme l'« état d'une chose qui est demeurée intacte. Employé à l'égard d'un document, on dira qu'un document est intègre si l'information qu'il contient n'a pas été altérée. »[32] Quant à la disponibilité, il s'agit de la capacité de garantir que l'information et les systèmes informatiques sont disponibles et opérationnels en temps voulu. Une bonne politique de sécurité devra aussi s'assurer de la disponibilité de l'information nécessaire au bon fonctionnement de l'entreprise ainsi que de la non-répudiation, soit le fait, pour une personne engagée dans une communication par voie informatique, d'être dans l'impossibilité de nier avoir reçu ou émis un message[33].

Ces objectifs sont globalement reconnus, spécialement dans les lois que nous allons aborder dans la prochaine partie, comme étant les caractéristiques de tout système offrant des garanties suffisantes de sécurité.

Toutes les entreprises collectent des informations à caractère personnel concernant leurs employés, leurs clients ou encore leurs potentiels partenaires commerciaux. Ces données peuvent être utilisées à des fins commerciales ou de marketing notamment sur le réseau Internet. Par conséquent, les entreprises doivent être conscientes et respecter les droits

---

[31] COMMISSION D'ACCÈS À L'INFORMATION, Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information à l'intention des ministères et des organismes publics, version 1.0., Québec, décembre 2002, en ligne : Commission d'accès à l'information <www.cai.gouv.qc.ca>.

[32] C.R.D.P., « Glossaire », dans Loi concernant le cadre juridique des technologies de l'information (L.Q. 2001, c.32) – Texte annoté et glossaire, Centre de recherche en droit public, Université de Montréal, septembre 2001.

[33] En d'autres mots, c'est la propriété d'un acte d'être définitif et clairement attribué à la personne qui l'a accompli ou au dispositif avec lequel il a été accompli.

fondamentaux et obligations légales en matière de collecte, gestion, traitement et transfert des données à caractère personnel[34].

Section 2. Rappel des principes fondamentaux en matière de protection des renseignements personnels

Avant d'abord de façon spécifique l'obligation légale de sécurité définie dans les divers textes nationaux et internationaux, il nous paraît profitable d'effectuer un bref rappel sur les principes fondamentaux que les entreprises et les gouvernements doivent respecter en matière de protection des renseignements personnels. Ces principes sont notamment décris à l'annexe 1 de la Loi sur la protection des renseignements personnels et des documents électroniques[35] (PIPEDA – acronyme en anglais) et reflètent le consensus de la communauté internationale sur la question, que ce soit dans les Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel[36] de l'O.C.D.E. ou dans les directives européennes sur le sujet.

Le premier principe à respecter est celui de la responsabilité. Ce dernier précise que l'organisation est responsable des données personnelles qu'elle détient sous son contrôle et qu'à cet égard, elle doit nommer un ou des individus qui seront responsables du respect de tous principes en matière de gestion de renseignements personnels.

Deuxièmement, le principe de la justification des finalités exige que la finalité de la collecte soit déterminée par l'organisation, avant ou pendant le moment de la cueillette de l'information, de sorte qu'elle soit en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

Encore, le principe du consentement mentionne que l'individu doit être informé de toute collecte, utilisation ou communication de renseignements personnels qui le concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. La forme de consentement dépendra de la nature et de la sensibilité des renseignements collectés. Mais, une personne peut retirer son consentement en tout temps, sous réserve de restrictions et d'un préavis raisonnable.

Quatrièmement, le principe de la limitation de la collecte veut que celle-ci soit limitée au strict nécessaire pour atteindre les finalités identifiées par l'organisation et doit être effectuée de manière juste et par des moyens licites. L'organisation ne peut recueillir des renseignements de façon arbitraire et la collecte doit se faire en tenant compte de la nature des informations et de la finalité à laquelle elles sont destinées.

À la lumière du principe de la limitation de l'utilisation, de la communication et de la conversation, les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou si la loi ne l'exige. De plus, on ne doit les conserver qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

---

[34] Garance MATHIAS, « L'impact de la Directive européenne relative à la protection des données à caractère personnel sur les entreprises européennes et extra-européennes », juriscom.net, 10 janvier 2000, en ligne : juriscom.net <http://www.juriscom.net>.
[35] PIPEDA, précitée, note 27.
[36] O.C.D.E., Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 23 septembre 1980. [ci-après Lignes directrices sur la vie privée de l'O.C.D.E.]

Le principe de la qualité des données exige que l'information personnelle recueillie soit exacte, complète et à jour pour atteindre la finalité établie par l'organisation. Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. En aucun cas, ils ne doivent être la source d'une prise de décision erronée due à l'existence de renseignements inexacts, spécialement lorsqu'il y a un transfert avec un tiers.

Le principe des garanties de sécurité stipule que les données personnelles doivent être protégées par de mesures de sécurité appropriées selon le niveau de sensibilité de l'information. Évidemment, tout ce mémoire est dédié aux mesures de sécurité des renseignements et cet aspect est discuté dès la prochaine partie.

Selon le principe de la transparence, l'organisation doit rendre disponible et facilement accessible l'information détaillée sur les politiques et les pratiques relatives à la gestion des données personnelles à toute personne qui en fait la demande et cela, dans une forme généralement compréhensible. Les renseignements transmis doivent, entre autres, identifier la personne responsable, décrire les moyens d'accès à l'information, décrire la nature des données détenues et l'usage qu'en est fait et surtout, identifier les partages effectués entre les partenaires commerciaux et filiales.

Le principe de l'accès aux renseignements garanti le droit qu'a tout individu d'accéder aux renseignements personnels qui le concernent, s'informer de l'usage qui en est fait et comment ils sont communiqués à des tiers. Ce principe lui accorde aussi la possibilité de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées. L'organisation aura alors l'obligation d'apporter les modifications nécessaires aux renseignements contestés et selon leur nature, l'organisation doit corriger, supprimer ou ajouter des renseignements.

Finalement, toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisation concernée. À cet égard, l'organisation doit faire enquête sur toutes les plaintes et donner suite aux plaintes qui s'avèrent justifiées en prenant les mesures appropriées pouvant aller jusqu'à la modification de sa politique.

Nous constatons que tous ces principes sont interdépendants. Dans le cas d'une entreprise qui voudrait donner des garanties suffisantes de sécurité aux renseignements personnels qu'elle détient, elle devra considérer chacun de ces principes et les traduire en des moyens techniques, administratifs ou même physiques de sécurité. Ainsi, le principe de responsabilité ne pourra être respecté sans une politique de sécurité adéquate précisant les rôles et les responsabilités des employés ou des partenaires commerciaux par des clauses contractuelles. Pour respecter ce principe de la qualité des données, l'entreprise devra mettre en œuvre des moyens de contrôle d'accès empêchant les modifications illicites ou accidentelles. Nous aurons la possibilité de confirmer cette corrélation au long de ce mémoire.

De plus en plus, les entreprises et les systèmes informatiques sont exposés à des menaces de sécurité fraude, espionnage, sabotage, vandalisme, feu ou inondations. Les menaces spécifiques à l'exploitation d'ordinateurs augmentent exponentiellement : virus, piratage, refus de services sont de plus en plus communs, ambitieux et raffinés. La dépendance grandissante des entreprises envers les systèmes et les services électroniques les rend encore plus vulnérables. Le surcroît de l'interconnexion des réseaux publics et privés et le partage des ressources augmentent la difficulté de contrôle d'accès.

À la lumière de cette réalité, le droit a dû s'adapter à une nouvelle culture, celle de la sécurité technique. Ainsi, au cours de dernières années, nous avons vu émerger un certain nombre de lois qui réfèrent à des normes techniques. Au Québec, par exemple, la Loi concernant le cadre juridique des technologies de l'information[37] a longuement été critiquée, par une partie de la communauté juridique, pour son caractère technique notamment du fait qu'elle accorde une grande place aux normes et aux termes jusqu'ici réservés à l'informatique.

> « Un trait commun de la mise en oeuvre des règles juridiques de la société de l'information est la place prise par la normativité technique. Ce phénomène s'illustre avec une particulière acuité par le recours croissant, dans les textes visant à procurer la sécurité juridique à des références ou des normes techniques[38]. »

Sur ce point, analysons d'emblée les sources qui de plus en plus nous font évoluer vers une culture juridique de la sécurité informatique et qui font émerger lentement mais sûrement une obligation générale de sécurité tant dans le domaine privé que public.

Chapitre 2. La protection des renseignements personnels et l'émergence d'une obligation légale de sécurité informationnelle

L'obligation d'assurer la sécurité des systèmes d'information constitue une pièce centrale des législations de protection des renseignements personnels. Il s'agit non seulement de conserver la confidentialité des données, mais également leur fiabilité, donc en d'autres mots, leur qualité, leur exactitude et leur mise à jour. L'exigence de sécurité n'épuise pas les exigences posées par les divers principes dans les diverses lois sur le sujet. Toutefois, elle apparaît comme une condition *sine qua non* du respect de chacun de ces principes. Le principe de la sécurité entretient une relation étroite avec tous les autres principes. Sans cette sécurité, comment rassurer la personne concernée que les informations recueillies sont les seules détenues? Comment affirmer qu'aucune personne non autorisée n'aura jamais accès à des données personnelles ou que les données conversées ne seront pas utilisées pour une fin illégitime ? Comment garantir qu'aucune modification erronée n'a été effectuée sur les renseignements gardés ? Toutes ces préoccupations justifient l'importance donnée aux moyens de sécurité relatifs aux renseignements personnels.

Quelle est la nature de cette obligation ? Il serait impossible d'imposer aux responsables du traitement des données à caractère personnel une obligation de résultat en matière de sécurité des données. Il faut dire que la sécurité informatique n'est jamais absolue et qu'il s'agit d'un concept qui évolue rapidement. Par conséquent, il est difficile de bien cerner « l'état de l'art » dans le domaine.

---

[37] Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c.32. [ci-après Loi des technologies de l'information]

[38] « Sécurité juridique et sécurité technique : indépendance ou métissage », séminaire organisé par le Programme international de coopération scientifique (CRDP/CECOJI), l'équipe de droit du cyberespace et du commerce électronique (CRDP) et le Centre d'étude et de coopération juridique internationale (CECOJI-CNRS), 30 septembre 2002.

> « There are several shortcomings in the state of art that must be considered when formulating privacy protection requirements. Presently, *there is no means for assuring absolute security* in automated, multi-user, resource-sharing data processing systems or computer networks. It is not feasible to prove correctness of an operating system's design to guarantee that hardware is free from design flaws. […] Even if physical security can be improved, it is impossible to assure the trustworthiness of personnel. »[39]

Vu que personne n'est tenu à l'impossible, à notre avis, les diverses dispositions dans le domaine de la sécurité des renseignements personnels imposent plutôt une obligation de moyens appréciable objectivement, c'est à dire prendre les mesures que prendrait un responsable de traitements diligent au vu des critères énumérés afin d'assurer la sécurité des renseignements personnels. Lorsqu'un dommage survient et laisse paraître un manque de sécurité, les contestataires devront démontrer que ce manque était inacceptable au regard du critère du responsable diligent.

La sécurité informationnelle est le moyen par lequel on protège les droits de personnes concernées et on maintient la confidentialité et l'intégrité des données relativement aux dangers et risques menaçant les données, les installations, les matériels informatiques, les logiciels et le personnel. Ces risques proviennent tant des causes accidentelles (feu, inondations, interruption de services, erreur de programme) que des causes intentionnelles (vandalisme ou sabotage, accès non autorisé, modification et destruction des données, etc.)[40]. Néanmoins, quelle est la justification juridique de ce principe de sécurité ?

Section 1. Les règles et les principes internationaux en matière de protection des renseignements à caractère personnel

Cette section porte sur les lois et les accords internationaux qui assurent la protection des renseignements personnels dans le cadre de certaines activités au pays et à l'étranger. Elle débute par un examen des conventions et des accords internationaux de protection des renseignements personnels dont le Canada est signataire. Elle se penche ensuite de façon plus détaillée sur la directive européenne en la matière, notamment sur les obligations relatives au niveau de protection adéquat des renseignements personnels.

1.1. Les principes et les textes internationaux

1.1.1. O.C.D.E.

La sécurité est un enjeu international puisqu'elle traverse les frontières et les solutions aux problèmes technologiques sont souvent plus efficacement tranchées par une coopération mondiale. C'est dans cet ordre d'idées que l'O.C.D.E. a préparé une série de lignes directives sur le sujet et c'est en 1980, que pour la première fois, l'organisation a jugé nécessaire d'élaborer des lignes directrices dans le souci d'harmoniser les législations nationales relatives à la protection de la vie privée et des renseignements personnels. Les Lignes directrices régissant

[39] Rein TURN, « Privacy Protection and Security in Transnational Data Processing Systems », [1980] 16 Standford Journal of International Law, 67, p. 82.
[40] F. HONDIUS, Emerging Data Protection in Europe, Amsterdam, North Holland/Elsevier, 1975, p.182.

la protection de la vie privée et les flux transfrontières de données de caractère personnel[41], adoptées le 23 septembre 1980, traduisent toujours un consensus international sur les orientations générales concernant le recueil et la gestion d'informations de caractère personnel. Bien que ces dernières ne soient qu'une simple recommandation, ces principes exercent une énorme influence sur la rédaction subséquente de documents légaux internationaux et nationaux[42] portant sur la protection des données personnelles. De plus, elles peuvent servir de base à une législation dans les pays qui n'en sont pas encore dotés.

C'est surtout l'article 11 desdites lignes qui nous semble important. Ce dernier préconise qu'« il conviendrait de protéger les données de caractère personnel, grâce à des *garanties de sécurité raisonnables*, contre des risques tels que la perte des données ou leur accès, destruction, utilisation ou divulgation non autorisés. » (Nos italiques) Les mesures de sécurité raisonnables incluent, des mesures physiques, des mesures de contrôle d'accès, des mesures organisationnelles telles les politiques de conduite et des mesures techniques informationnelles.[43] (Nos italiques)

Effectivement, la mise en place de moyens sécuritaires, tels que la cryptographie, pour l'échange d'informations personnelles en ligne est nécessaire non seulement pour garantir la confidentialité des informations, mais aussi pour renforcer la confiance des consommateurs. Cette garantie de sécurité est de mise en ce qui concerne la transmission des données, d'une part, et le stockage de celles-ci dans les bases de données, d'autre part.

L'obligation de sécurité se retrouvait également dans les Lignes directrices relatives à la sécurité des systèmes d'information[44] adoptées le 26 novembre 1992. Ces lignes directrices offraient aussi des principes facilitant l'atteinte de la sécurité des systèmes d'information et, *a fortiori*, des renseignements personnels, et garantissaient la protection des intérêts de ceux qui dépendent grandement, surtout pour la prise de décisions, de ces systèmes d'information en assurant leur disponibilité, leur confidentialité et leur intégrité[45]. L'objectif était donc d'accroître la confiance par rapport aux systèmes d'information et à la manière où ces derniers étaient utilisés, faciliter le développement et l'usage national et international de systèmes et promouvoir la coopération internationale pour assurer un niveau optimum de sécurité.

Toutefois, ces lignes ont été modifiées, en juin 2002, par les Lignes Directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information[46], qui s'avèrent être beaucoup plus complètes que les préexistantes et tiennent en compte l'évolution spectaculaire

---

[41] Lignes sur la vie privée de l'O.C.D.E., précitée, note 30.

[42] Notamment les lois nationales des pays membres comme l'Australie, Autriche, Belgique, Canada, Danemark, Allemagne, France, Angleterre, Portugal, États Unis et autres. Voir la liste complète des membres en ligne: <www.oecd.org.>

[43] O.C.D.E., Lignes directrices de l'O.C.D.E. sur la protection de la vie privée et les flux transfrontières des données de caractère personnel, 2001, Exposé des motifs du paragraphe 11, p. 47, par. 56

[44] O.C.D.E., Guidelines for the Security of Information Systems, 26 novembre 1992, en ligne: O.C.D.E. < http://www1.oecd.org/dsti/sti/it/secur/ >.

[45] Yves POULLET, « Réflexions introductives à propos du binôme « Droit-Sécurité », dans Joël HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 189.

[46] Lignes Directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information - Vers une culture de la sécurité, Recommandation du Conseil de l'O.C.D.E. du 25 juillet 2002, 1037ème session, en ligne : O.C.D.E. < www.oecd.org/pdf/M00033000/M00033183.pdf >. [ci-après : Nouvelles lignes directrices sur la sécurité de l'O.C.D.E.]

du degré d'utilisation des systèmes et de l'environnement des technologies de l'information depuis 1992.

> « Les Lignes directrices marquent une rupture nette avec un temps où la sécurité n'intervenait que trop souvent de façon incidente dans la conception et l'utilisation des réseaux et systèmes d'information. Les parties prenantes sont de plus en plus tributaires des systèmes d'information, des réseaux et des services qui leur sont liés, lesquels doivent tous être fiables et sécurisés. Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace.»[47]

Considérons brièvement chacun de ces principes fondamentaux puisqu'ils nous seront utiles lorsque nous étudierons la mise en place d'un programme de sécurité pour les données personnelles. Ces lignes directrices nous offrent neuf principes qui devront faciliter la sécurité des données personnelles stockées dans les systèmes informatiques et leur intérêt s'accroît d'autant plus que c'est le seul texte à portée internationale qui laisse percevoir si clairement l'obligation de sécurité.

Le premier principe, sans doute l'un des plus importants dans tout processus de sécurisation, est la sensibilisation tant de l'administration que de tous les utilisateurs des systèmes d'information. Il est en effet essentiel qu'une sensibilisation soit faite entre tous les acteurs et de bien montrer qu'il ne sert à rien de veiller à la sécurité si celle-ci ne s'applique pas à l'ensemble organisationnel d'une entreprise[48]. Ceux qui interagissent avec les systèmes d'information doivent être sensibilisés au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'ils peuvent entreprendre pour renforcer la sécurité. Mais, nous reviendrons sur l'importance de ce principe dans la deuxième partie, lorsque nous étudierons plus amplement le programme de sensibilisation et de formation des usagers et des responsables du traitement des données confidentielles.

Le deuxième principe, repris de plus en plus par diverses législations, est le principe de la responsabilisation. Les utilisateurs sont responsables de la sécurité des systèmes et réseaux d'information. Cette obligation est caractérisée par la possibilité qu'a l'entreprise d'identifier les actions de tous les utilisateurs et les processus qui interagissent avec des systèmes informatiques, et forcément avec des renseignements personnels. Les rôles et les responsabilités doivent être clairement déterminés, définis et autorisés en fonction du niveau de sensibilité et la confidentialité de l'information. Nous pouvons noter à ce stade le niveau d'interconnexion entre les principes des lignes directrices : la connaissance des responsabilités individuelles passe nécessairement par la sensibilisation et la formation des parties prenantes.

> « Elles doivent comprendre leur responsabilité dans la sécurité de ces systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. Elles doivent régulièrement examiner et

---

[47] Id., p. 8.
[48] Vincent GAUTRAIS, « Aspects sécuritaires applicables au commerce électronique », dans Éric LABBÉ, Daniel POULIN, François JACQUOT et Jean-François BOURQUE (directeurs), Le guide juridique du commerçant électronique (rapport préliminaire), Montréal, Juris International, 2001, p. 75, en ligne : < http://www.jurisint.org/pub/05/fr/guide_chap3.pdf >.

> évaluer leurs propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement. »[49]

Du fait de l'interconnexion des systèmes et réseaux d'information et de la facilité des dommages à se répandre rapidement et massivement, la capacité de réaction et de collaboration ne peut qu'être bénéfique. C'est justement ce que vise le troisième principe, celui de la réaction, qui propose la mise en place d'un plan de réponse et de réaction en cas d'incident. Ainsi, tous doivent agir avec promptitude et dans un esprit de coopération, dans la meilleure des hypothèses une collaboration transfrontalière, pour prévenir, détecter et répondre aux incidents de sécurité. Ceci suppose que les organisations et les entreprises doivent échanger leurs informations sur les menaces et vulnérabilités, même lorsque cela concerne des informations internes. Toutefois, un problème survient à ce stade du fait que certains hésitent à partager leur expérience d'un incident de sécurité par peur d'être mal jugés par le public ou même donner un avantage stratégique à un concurrent. C'est une erreur ! Ils peuvent se féliciter de s'en être aperçus, c'est la marque d'un système bien géré.

Le principe de l'éthique énonce la nécessité de tenir compte de l'intérêt légitime des tiers dans les renseignements détenus par un système d'information. Le même principe est soutenu par les Generally Accepted Systems Security Principles (GASSP) de l'International Information Security Foundation, et la justification donnée est la suivante :

> « Information systems pervade our societies and cultures. Rules and expectations are evolving with the regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations establish by social norms, and obligations. »[50]

Les actions ou inactions d'une partie peuvent causer un tort considérable à une autre. Une conduite chargée d'éthique est donc indispensable et chacun doit s'efforcer d'élaborer et d'adopter des pratiques exemplaires en promouvant des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes de tous.

De plus, l'intégration de la sécurité en entreprise doit se faire dans le respect du cinquième principe, celui de la démocratie. La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique, notamment la protection des renseignements personnels.

> « La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence. »[51]

---

[49] Nouvelles lignes directrices sur la sécurité de l'O.C.D.E., précitée, note 46, Principe 2.
[50] Generally Accepted Systems Security Principles (GASSP), International Information Security Foundation, version 2.0, juin 1999, principe 2.1.3. p. 36, en ligne: <http://www.auerbach-publications.com/dynamic_data/2334_1221_gassp.pdf >.
[51] Nouvelles lignes sur la sécurité de l'O.C.D.E., précitée, note 46, principe 5.

On dit souvent que « la sécurité, ça coûte cher », mais on oublie que l'absence de sécurité coûte plus cher encore. Tout l'art de la gestion du risque est de trouver le juste compromis entre « ce que ça coûte » et « ce que ça rapporte » ! Le bon niveau de sécurité, c'est celui au-delà duquel tout effort supplémentaire a un coût plus important que les avantages que l'on peut attendre. Les lignes directrices sur la sécurité de l'O.C.D.E. rehaussent aussi les bénéfices de procéder à des évaluations des risques. Ce principe peut être vu comme la nouvelle version du principe de proportionnalité des anciennes lignes directrices de 1992[52] qui obligeait les parties à adopter des mesures de sécurité proportionnelles à la valeur et aux risques de modification accidentelle ou illicite, de perte ou de divulgation des renseignements personnels.

> « L'évaluation des risques permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protéger. L'évaluation des risques doit tenir compte des préjudices aux intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information. »[53]

Ci-bas, plus précisément au chapitre 3 de la première partie, nous aurons la possibilité d'étudier plus amplement le processus de l'analyse des risques et son impact dans la mise en place de mesures de sécurité adéquates.

De plus, les lignes directrices prévoient que la conception et l'adoption de mesures de protection et solutions appropriées afin de prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées doivent recevoir une attention considérable afin que la sécurité soit intégrée en tant qu'élément essentiel des systèmes et réseaux d'information. La sécurité doit être un élément fondamental de l'ensemble des produits, services, systèmes et réseaux et faire partie intégrante de la conception et de l'architecture des systèmes.

Les entreprises doivent donc avoir une approche globale de la gestion de la sécurité. Cela présuppose que les mesures, pratiques et procédures de sécurité des systèmes informatiques doivent être coordonnés et intégrés entre eux et avec d'autres mesures de sécurité en d'autres domaines afin de créer un ensemble cohérent et fonctionnel. La gestion de la sécurité doit être fondée sur l'évaluation des risques et être dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. Elle doit inclure également, par anticipation, des réponses aux menaces émergentes et couvrir la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit. Ainsi, tout le cycle de sécurité doit être couvert.

Finalement, puisque les mesures de protection informatique changent continûment, l'examen et la réévaluation de la sécurité des systèmes et réseaux d'information et l'introduction de modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité est nécessaire. C'est ce que prévoit le principe de la réévaluation. Cette réévaluation ou mise à jour des mesures de sécurité permet à l'entreprise de prendre des décisions éclairées en la matière.

---

[52] O.C.D.E., précitée, note 44.
[53] Nouvelles lignes sur la sécurité de l'O.C.D.E., précitée, note 46, principe 6.

Ces lignes directrices ne fournissent pas une solution unique pour parvenir à la sécurité, mais un cadre plus général de principes de nature à favoriser une meilleure compréhension de la matière. Nonobstant, ces lignes sont sans aucun doute l'unique texte qui met autant en valeur une nouvelle culture juridique : la culture de la sécurité informationnelle.

1.1.2. Les Nations Unies

La protection de la vie privée a été, au long des décennies, une préoccupation constante dans la communauté internationale, mais ce n'est que dans les années 90 que l'organisation des Nations Unies s'est penchée sur la question lors de l'adoption, le 14 décembre 1990, par l'assemblée générale, des Lignes directrices pour la réglementation des fichiers informatisés de données à caractère personnel[54] (Lignes de l'O.N.U).

Ces lignes partagent et modifient les lignes initiales de l'O.C.D.E. par l'incorporation les principes suivants pour le traitement informatisé des données personnelles : légalité et éthique, exactitude, détermination des finalités, droit d'accès de l'intéressé, non-discrimination et sécurité. Tout comme celles de l'O.C.D.E., les Lignes de l'O.N.U. ne sont qu'une recommandation. Néanmoins, elles constituent la prise de position formelle de quelques 180 états membres de l'assemblée générale, symbolisant un niveau de consensus élevé sur les principes fondamentaux en matière de protection de données personnelles.

Les principes établis par ces Lignes s'appliquent en premier lieu, à tous les fichiers informatisés publics ou privés, ainsi qu'aux fichiers manuels. Ils pourraient s'appliquer aux fichiers concernant des personnes morales dans la mesure où ils contiennent des données sur des individus. Ces Lignes visent aussi les données personnelles détenues par les organisations gouvernementales internationales.

En ce qui nous concerne, le septième principe énonce le principe de la sécurité. Y est prévu, conformément aux Lignes de l'O.C.D.E., que des mesures appropriées devraient, être prises pour protéger les fichiers contre les dangers naturels, comme la perte accidentelle ou la destruction et les dangers provoqués par l'homme, notamment accès non-autorisé, usage illicite de l'information ou la contamination par des virus informatiques.[55]

1.2. L'Europe et le droit communautaire

1.2.1. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

C'est en 1981, que le Conseil de l'Europe adopte la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[56] (Convention 108/1981) et dans le souci de la protection de la vie privée, affirme pour la première fois le principe la sécurité. La Convention 108/1981 s'adresse aux mêmes enjeux sociétaux que les Lignes de l'O.C.D.E. sur la vie privée. Effectivement, son préambule annonce l'objectif de reconnaître « la nécessité de concilier les valeurs fondamentales du respect de la vie privée et

---

[54] O.N.U., Principes directeurs pour la réglementation des fichiers informatisés de données à caractère personnel, résolution 45/95 du 14 décembre 1990.

[55] Version anglaise: « Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses. »

[56] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, No. 108. Strasbourg, 28 janvier 1981, en ligne : < http://conventions.coe.int/treaty/FR/Treaties/Html/108.htm >. [ci-après Convention 108/1981]

de la libre circulation de l'information entre les peuples » et soutient qu'il est « souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés ». Mais, contrairement à celles de l'O.C.D.E., le respect de la convention est obligatoire comme tout traité international. Elle oblige les membres de l'Union européenne à appliquer ses principes aux fichiers et aux traitements automatisés de données à caractère personnel[57] dans le secteur public et privé, favorisant ainsi l'harmonisation des règles de droit.

L'article premier de la Convention 108/1981 soutient que son objectif est «[…] garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ».

Pour arriver à cela, elle établit des principes de base pour la protection des données. Ces principes reflètent les règles qu'il convient de respecter dès que l'on veut collecter des renseignements personnels, notamment de garantir la sécurité des données. À ce propos, l'article 7 précise que des « mesures de sécurité appropriées [doivent] être prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés. »[58] Cette obligation de prendre des mesures de sécurité a aussi été largement développée par les directives européennes en 1995.

1.2.2. La Directive européenne sur la vie privée de 1995[59]

La Commission européenne incarne l'intérêt général de l'Union européenne et joue un rôle moteur dans le processus d'intégration des principes communautaires dans le droit national. Le 24 octobre 1995, la Commission européenne adopte la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[60] (Directive 95/46/CE). Cette directive vise les renseignements personnels et harmonise les lois sur la protection de la vie privée des États membres. La Directive, qui a été mise en œuvre par le biais de lois nationales depuis le 24 octobre 1998, oblige tous les États membres à adopter une loi sur la protection des renseignements personnels ou à réviser leurs lois existantes pour se conformer à cette dernière. Notons qu'elle s'applique tant au secteur privé qu'au public.

La Directive prévoit que le régime de protection des données s'applique à tous les secteurs de l'industrie et des services. Elle fixe des limites strictes à la collecte et à l'utilisation des données à caractère personnel et exige la création d'un organisme national indépendant (ex. : la CNIL en France – homologue de la Commission d'accès à l'information au Québec)

---

[57] Id., Art. 3.
[58] Id., art. 7.
[59] Bien que la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOCE, 31 juillet 2002, L 201/37 soit plus récente que celle étudiée dans ce mémoire, elle ne vise que le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques en Europe. Sur la sécurité et la confidentialité consultez les articles 4 et 5 de la Directive 2002/58/CE.
[60] Directive 95/46/CE, précitée, note 16.

protégeant ces données auprès duquel chaque société doit s'inscrire, avant de compiler, copier ou transférer les informations.

Mais ce qui nous intéresse plus particulièrement ce sont les obligations de sécurité importantes qu'impose la Directive 95/46/CE en ce qui concerne l'accès aux données afin d'éviter l'intrusion, la perte ou la destruction des données.

D'un côté, l'article 16 précise qu'en matière de confidentialité des traitements, « toute personne agissant sous l'autorité du responsable du traitement […] ainsi que le sous-traitant, qui accède à des données de caractère personnel ne peut les traiter que sur instruction du responsable des traitements […]». Pour respecter cet article, l'entreprise devra s'assurer d'avoir donné des instructions claires à ses employés ou tiers qui ont accès aux renseignements personnels. L'entreprise devra aussi mettre en place une gestion adéquate des droits d'accès.[61]

En matière de sécurité du traitement, l'article 17(1) prévoit que :

> « le responsable du traitement doit mettre en œuvre des 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 forme de traitement illicite ».

Le deuxième alinéa de 17(1) prescrit un niveau régulateur : reconnaissant les coûts et les facteurs technologiques, le niveau de sécurité devrait être proportionnel aux risques associés à la nature et au traitement des données. Ainsi, les mesures doivent « 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 la nature des données à protéger. »[62] De plus, l'article 17(2) de la directive prévoit que lorsque le traitement est effectué par un sous-traitant, celui-ci doit apporter des « garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer » et doit « veiller au respect de ces mesures ».

Par cet article, l'entreprise doit d'assurer que les « employees dealing with personal data are aware of the security provisions of the Directive. This will involve training. Controllers should also consider providing written guidelines to employees on security issues. »[63]

Outre l'obligation de sécurité, selon l'article 17(4), la relation entre le responsable du traitement et le sous-traitant doit être régi par contrat écrit ou par un acte juridique les liant, prévoyant notamment, que le sous-traitant agit sous les ordres du responsable et que l'obligation de sécurité lui incombe également.

L'entreprise qui veut constituer des fichiers contenant des renseignements personnels devra rapporter la preuve que la base de données répond aux critères imposés en matière de sécurité. Cette obligation se traduit par le fait que la société doit prévoir des contrôles stricts pour empêcher l'accès illicite aux données ainsi que la manipulation illégale de ces

---

[61] MASONS Solicitors and Privy Counsil Agents , Handbook of cost effective compliance with the 95/46/CE Directive, p.62, en ligne: <http://www.cyberprivacy.or.kr/pds/a_1.pdf>.
[62] Directive 95/46/CE, précitée, note 16, art. 17(1) par. 2.
[63] MASONS, précitée, note 61, p.66.

informations. Ces contrôles peuvent se présenter sous deux formes, à savoir des dispositifs techniques (mots de passe, cryptage, etc.) et des instructions données aux employés (affiches, politiques, etc.), dont leur violation peut les exposer à des mesures disciplinaires[64].

L'article 24 de la Directive 95/46/CE permet également aux États membres « de prendre les mesures appropriées pour assurer la pleine application de [ces] dispositions » telles que des dommages et intérêts sur le plan civil et des sanctions pénales contre ceux qui violeraient cette obligation.

Bien que cette Directive fasse partie de la législation européenne, ses implications concernent non seulement les entreprises et les citoyens européens mais aussi, d'une manière générale, toutes les entreprises étrangères qui entretiennent des relations d'affaires avec les États membres de l'Union européenne ou qui échangent des données avec leurs filiales ou leurs maisons mères européennes. Selon l'article 25, les transferts de données vers des pays non-membres, peuvent être effectués dans la mesure où ces derniers peuvent assurer un « niveau de protection adéquat »[65]. L'appréciation du niveau sera jugée en fonction de certains facteurs comme la nature des données transférées, des lois nationales pertinentes, des standards professionnels et évidemment, des mesures de sécurité en place.

Section 2. La législation nationale et autres textes à portée juridique concernant la protection des renseignements à caractère personnel

Cette deuxième section porte sur les mécanismes de protection des renseignements personnels actuellement en vigueur. Elle fait l'examen des mécanismes de protection des renseignements personnels adoptés par le gouvernement fédéral et provincial. Nous terminerons par une étude de la directive du gouvernement du Québec en matière de mesures de sécurité et de protection des renseignements personnels.

2.1. Canada : Loi sur la protection des renseignements personnels et des documents électroniques

Le 1er janvier 2001, la première phase de la Loi fédérale sur la protection des renseignements personnels et des documents électroniques[66] (PIPEDA – de l'acronyme en anglais) est entrée en vigueur. En effet, cette loi entre en vigueur en trois (3) phases : le 1er janvier 2001 (il y a eu une extension du délai jusqu'au 1er janvier 2002) pour tous les employés fédéraux, en janvier 2002 elle a été étendue aux informations personnelles dans le domaine de la santé et enfin, le 1er janvier 2004, elle s'appliquera à toutes les activités commerciales sous juridiction provinciale (il y a préséance de la loi provinciale substantiellement similaire, comme au Québec) ou fédérale qui font la collecte, l'usage et la divulgation de renseignements personnels. Toutefois, la loi ne s'applique pas aux matières de compétence exclusive de la province, notamment les gouvernements provinciaux, municipalités, universités, écoles et

[64] P. MATHIAS, précitée, note 34.
[65] Voir à ce sujet la décision de la Commission du 20 décembre 2001, constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques [notifiée sous le numéro C(2001) 4539] (2002/2/CE), J.O.C.E., 4 janvier 2002, L 2/13.
[66] PIPEDA, précitée, note 27.

hôpitaux. Néanmoins, elle est d'application plus ample que la Loi sur la protection des renseignements privés[67] de 1985.

L'objectif de la PEPIDA est de fixer des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.[68]

Les influences de cette loi remontent à l'année 1984, date à laquelle le Canada a ratifié les Lignes de l'O.C.D.E. sur la vie privée de 1980[69]. Depuis, le Canada a vivement encouragé les entreprises à adopter des codes de conduite en matière de protection des renseignements personnels en s'inspirant de ces lignes. En 1996, un pas important dans la protection des données personnelles a été donné par le Canadian Standards Association (CSA) lorsque celui-ci rédige un code volontaire en matière de vie privée, qui est devenu l'annexe 1 de la Loi fédérale.

Sont des renseignements personnels au sens de la loi, « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation, des adresses et numéro de téléphone de son lieu de travail. »[70] La loi fédérale s'applique aux renseignements personnels qu'une organisation collecte, utilise ou communique dans le cadre d'activités commerciales[71]. Elle ne s'applique pas à un individu à l'égard des renseignements personnels qu'il recueille, utilise ou communique à des fins personnelles ou domestiques et à aucune autre fin[72]. Ainsi, la loi ne s'applique pas aux millions de pages Web personnelles sur Internet, ni aux informations recueillies à des fins journalistiques, artistiques ou littéraires.

Tout comme nous l'avons déjà examiné dans le premier chapitre, la loi fédérale énonce dans son annexe 1 une dizaine de principes[73] à respecter dans le domaine des renseignements personnels. Attardons-nous sur le septième principe de l'annexe 1, qui décrit l'obligation de protéger les renseignements personnels par des mesures de sécurité correspondant à leur degré de sensibilité. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous peuvent devenir sensibles suivant le contexte. Selon l'article 4.3.4., les noms et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les noms et adresse des abonnés de certains périodiques spécialisés pourront l'être.

Le degré de protection variera donc selon le degré de sensibilité des données, de la quantité, de la répartition et du format des renseignements, ainsi que des méthodes de conservation (art. 4.7.2.). Ainsi, plus les renseignements personnels présentent un caractère sensible, plus le niveau de sécurité devra être élevé. Les moyens de sécurité doivent protéger adéquatement contre la perte ou le vol ainsi que contre la consultation, la communication, la

---

[67] Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21.
[68] PEPIDA, précitée, note 27, art. 3.
[69] O.C.D.E., précitée, note 36.
[70] PEPIDA, précitée, note 27, art. 2(1).
[71] PEPIDA, précitée, note 27, art. 4(1) (a).
[72] PEPIDA, précitée, note 27, art. 4(2)(b).
[73] Voir, supra, Chapitre 1, Section 2.

copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés (art. 4.7.1.)

L'article 4.7.3 ajoute que les méthodes de protection devraient comprendre : (a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux ; (b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif ; et (c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement. En plus, les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels (art. 4.7.4.). Finalement, selon l'article 4.5.3, au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès. D'après un guide publié par le commissaire à la vie privée du Canada, pour respecter leurs responsabilités les organismes devront, entre autres :

> « Élabore[r] et applique[r] une politique de sécurité pour assurer la protection des renseignements personnels. Utilise[r] des mesures de sécurité adéquates pour assurer la protection qui s'impose : moyens matériels […], mesures techniques […], des mesures administratives. […] Sensibilise[r] les employés aux mesures de sécurité en organisant périodiquement des réunions à ce sujet. Au moment de choisir les mesures de sécurité qui s'imposent, il conviendrait de tenir compte des facteurs suivants : le caractère délicat des renseignements ; la quantité de renseignements ; l'importance de leur distribution, leur présentation […], le type d'emmagasinage. Examine[r] et mettez à jour les mesures de sécurité de façon périodique. »[74]

Nous étudierons en détail ces niveaux au cours de la deuxième partie du mémoire.

2.2. Québec

Le Québec a été la première province en Amérique du Nord à adopter une loi applicable au secteur privé, donnant ainsi au droit à la vie privée une protection à trois niveaux. D'abord, l'article 5 de la Charte québécoise des droits et libertés de la personne[75], charte de nature quasi constitutionnelle, qui reconnaît un droit à la vie privée, statuant « que toute personne a le droit à sa vie privée ». Les tribunaux québécois ont clairement reconnu dans diverses décisions que les informations confidentielles et personnelles bénéficient de la protection de l'article 5 de la Charte québécoise[76]. Le C.c.Q.[77] complète cette dernière en définissant ce qui constitue une atteinte à la vie privée. Ces deux textes législatifs s'appliquent aux entités privées et publiques, ainsi qu'aux individus. Le troisième niveau de protection est donné par la Loi sur la protection

---

[74] Commissaire à la vie privée du Canada, « Protection des renseignements personnels : vos responsabilités », Principe 7 : Mesures de sécurité, Ressource électronique en ligne : <http://www.privcom.gc.ca/information/guide_f.asp>.

[75] Charte des droits et libertés de la personne, L.R.Q., c. C.-12 [ci-après La Charte québécoise].

[76] Voir en matière de fichiers médicaux Reid c. Belzile, [1980] C.S. 717 (C.S. Québec); Centre local de services communautaires de l'érable c. Lambert, [1981] C.S. 1077 et concernant l'information personnelle sur la santé The Gazette c. Valiquette, (1996), [1997] R.J.Q. 30 (C.A.).

[77] C.c.Q., précitée, note 17.

des renseignements personnels dans le secteur privé[78] et par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[79].

Finalement, en novembre 2001, la Loi concernant le cadre juridique des technologies de l'information[80] est entrée en vigueur. Vivement critiquée pour son caractère hautement technique, cette loi est sans aucun doute une percée importante dans la mise en place d'un milieu stable pour l'utilisation des nouvelles technologies de l'information et nous donne des critères quant à la protection des documents électroniques et *a fortiori*, des renseignements personnels. Aussi, dans cette sous-section, nous aurons la possibilité d'examiner quelques directives élaborées par le gouvernement québécois en matière de sécurité des informations numérisées et sur les échanges entre les ministères qui nous éclairera sur la notion de « mesures de sécurité adéquates » en la matière. Ces principes pourront incontestablement servir de guide pour le secteur privé.

2.2.1. Loi sur la protection des renseignements personnels dans le secteur privé[81]

Selon l'article premier de la loi, le but de cette dernière est d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil du Québec en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil du Québec. Elle s'applique à ces renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles : écrite, graphique, sonore, visuelle, informatisée ou autre.

L'article 10 de la loi énonce que :

> « toute personne qui exploite une entreprise et recueille, détient, utilise ou communique des renseignements personnels sur autrui doit prendre et appliquer des *mesures de sécurité propres à assurer le caractère confidentiel* des renseignements. » (Nos italiques)

De plus, l'article 11 ajoute que :

> « toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée. »

Ceci suppose naturellement que l'entreprise détienne un système informatique garantissant une saine gestion des renseignements personnels qu'elle garde.

Selon l'article 83, au terme d'une enquête relative à la collecte, à la détention, à la communication ou à l'utilisation de renseignements personnels par une personne qui exploite une entreprise, la Commission peut, après lui avoir fourni l'occasion de présenter ses observations, lui recommander ou lui ordonner l'application de toute mesure corrective propre à assurer la protection des renseignements personnels. Elle peut fixer des délais pour l'exécution des mesures qu'elle ordonne. Si l'entreprise tarde ou refuse de respecter l'ordonnance de la

[78] Loi sur le secteur privé, précitée, note 18.
[79] Loi sur l'accès aux documents des organismes publics, précitée, note 19.
[80] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37.
[81] Loi sur le secteur privé, précitée, note 18.

commission, un avis sera publié pour en informer le public (art. 84). L'impact de cet avis pourrait être fatal pour l'entreprise en ce qui concerne son image de marque et sa crédibilité.

2.2.2. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[82]

La présente loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, indépendamment que leur conservation soit assurée par l'organisme public ou par un tiers et quelque soit la forme de ces documents : écrite, graphique, sonore, visuelle, informatisée ou autre (art. 1 et 2).

Le chapitre 3 de la loi s'intéresse à la protection des renseignements personnels. Si, dans un document, les renseignements concernant une personne physique et permettent de l'identifier, alors ils sont nominatifs et doivent recevoir une protection. L'article 69 prévoit que la communication de renseignements nominatifs doit être faite de manière à *assurer le caractère confidentiel* des renseignements nominatifs. Dans les cas où une entente écrite doit être conclue, cette entente doit mentionner les moyens mis en oeuvre pour assurer cette confidentialité. Concernant sa conservation, l'article 72 requiert que les renseignements nominatifs soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis. De cette manière, les renseignements personnels évolueront tout au long de leur cycle de vie conformément à la situation des personnes concernées. Ceci implique, par exemple, établissement de mécanismes pour gérer les mises à jour d'un renseignement personnel dupliqué ou répliqué[83]. De plus, comme la protection doit être assurée durant tout le cycle de vie du document, selon l'article 73, lorsque l'objet pour lequel un renseignement nominatif a été recueilli est accompli, l'organisme public doit le détruire et à ce propos des mesures de protection pour assurer la confidentialité doivent être mises en œuvre.

L'établissement d'un fichier doit également faire l'objet d'une déclaration à la commission en vertu de l'article 76. Le paragraphe 5 de cet article prévoit que la déclaration doit indiquer les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis. C'est à la lumière de cette déclaration que la Commission d'accès à l'information sera en mesure de prescrire les mesures de sécurité adéquate. L'importance des mesures de sécurité est dès lors directement proportionnelle au caractère sensible de l'information stockée. En effet, l'article 124 (3) prévoit que la Commission d'accès à l'information peut prescrire à l'égard d'un fichier de renseignements personnels la nature des mesures de sécurité que l'organisme public peut prendre afin d'assurer le caractère confidentiel des renseignements nominatifs.

> « Par sa formulation et la procédure qu'elle préconise, facilite l'identification des [mesures minimales]. En fait, la procédure proposée a l'avantage de prendre en considération les

[82] Loi sur l'accès aux documents des organismes publics, précitée, note 19.
[83] Max CHASSÉ (analyste), Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information - À l'intention des ministères et organismes publics, v. 1.0,Commission d'accès à l'information, Gouvernement du Québec, décembre 2002 en ligne : <www.cai.gouv.qc.ca>.

> caractéristiques propres de chaque système et permet ainsi de structurer un ensemble de mesures de sécurité répondant aux spécificités de chacun de ceux-ci. On peut parler de « sur mesure ». [84]

Si le législateur québécois avait prévu les mesures techniques à prendre dans un texte de loi, cela aurait eu pour conséquence de figer le texte législatif et de le rendre rapidement désuet en raison de l'évolution rapide des technologies de l'informatique. Hondius est d'avis que « it would be futile to try and spell out in the law any specific technical or systems approaches to data security. Any such provision would soon be obsolete on account of the rapid development of technology. »[85]

En confiant le rôle d'appréciation des mesures de sécurité à la Commission d'accès à l'information, le législateur a évité de compliquer inutilement le libellé de la loi ainsi que de lier la Commission par des critères qui risqueraient de devenir rapidement obsolètes, difficilement applicables au niveau pratique.

2.2.3. Loi concernant le cadre juridique des technologies de l'information[86]

Cette loi, considérée par plusieurs juristes comme étant hautement technique, est aussi une importante source de droit en ce qui concerne l'encadrement de certaines mesures de sécurité pour certaines activités faisant appel aux nouvelles technologies de l'information. Cette loi touche, notamment, des questions matière d'archivage de documents électroniques et des modes d'identification, thèmes servant très bien à la sécurisation des données personnelles et à la conservation des documents pouvant être admis en preuve en cas d'incident de sécurité.

Ce texte juridique a pour objectif d'assurer, entre autres,

> « la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information, qu'elles soient électroniques, magnétiques, optiques, sans fil ou autres ou faisant appel à une combinaison de technologies et la concertation en vue de l'harmonisation des systèmes, des normes et des standards techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information. »[87]

Il est vrai que cette loi ne s'applique pas spécifiquement aux renseignements personnels, mais elle offre une excellente base technique pour l'entreprise désirant mettre en place des mesures de sécurité administratives, organisationnelles ou techniques. En définissant de façon très large, à l'article 3, la notion de document, la loi permet d'englober «[toute] information portée sur un support […] qui est structurée de façon tangible ou logique selon le support qui la porte et qui est intelligible sous la forme de mots, de sons ou d'images ».[88]

---

[84] Karim BENYEHKLEF, précitée, note 14, p. 130.
[85] HONDIUS, précitée, note 40, p. 185.
[86] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37.
[87] Id., art. 1.
[88] Cet article aborde aussi la notion de « dossier » et explique qu'il peut être composé d'un ou plusieurs documents. « Un dossier réfère à un ensemble de documents relativement à une personne ou à une question spécifique, par exemple un dossier médical, un dossier de conduite automobile, un dossier

De plus, pour l'application de la loi, est assimilée au document « toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »[89] Pensons par exemple, à une base de données pouvant façonner une liste des clients de l'entreprise contenant des données à caractère personnel.

L'article 6 précise que les *mesures de sécurité* prises pour protéger le document sont considérées pour apprécier l'intégrité de celui-ci. Ainsi, au plan technologique, l'entreprise devra s'assurer d'adopter des recommandations d'ordre technique, procédural et organisationnel, notamment s'assurer que les produits informatiques utilisés dans la gestion des documents électroniques (dans la création, la conservation, la transmission et la reproduction) présentent des garanties de sécurité suffisantes de fiabilité. La finalité de cet article est donc « d'assurer l'intégrité et la fidélité des documents électroniques, conservés ou restitués, ainsi que la pérennité de l'archivage durant toute la période de conservation jusqu'à sa destruction. Ces mesures de sécurité permettent aux entreprises de prouver que l'information conservée n'a pas été altérée et a été maintenue dans son intégralité et que le support choisi lui accorde la stabilité et la pérennité voulue. C'est seulement dans ces conditions que la valeur juridique d'un document est assurée ». (art. 5)

La loi considère que les altérations non autorisées durant la conservation du document peuvent porter atteinte à l'intégrité de ce dernier. Dès lors, la personne qui a l'autorité pour effectuer les modifications devra noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand et pourquoi celle-ci a été accomplie. À ce sujet, l'article 21 prescrit que :

> « Lorsqu'une modification est apportée à un document technologique durant la période ou il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct. »

Ainsi, tout dossier tenu sur une personne et qui ferait l'objet d'une modification doit être documenté. Il peut s'agir d'un dossier tenu par un employeur sur un employé auquel une modification serait apportée. De même, à l'article 20, lorsqu'un document est détruit, l'entreprise devra s'assurer de la protection des renseignements confidentiels et personnels que peuvent comporter les documents devant être détruits et leur destruction ne doit en aucun cas mettre en péril la confidentialité.

L'article 24 peut également s'appliquer à une entreprise qui collecte des renseignements personnels. Celui-ci ajoute que :

> « l'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière est rendu public, droit être restreinte à

---

scolaire. La loi réfère à ce sens courant […]. La précision a son importance, car plusieurs entreprises gèrent leurs documents à l'aide de dossier. » Définition tirée de C.R.D.P., précitée, note 32.

[89] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37, art. 3.

> cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. »

Dans le cadre d'une entreprise, cette obligation pourrait se concrétiser par le fait que certains employés aient besoin d'accéder à une base de données contenant des renseignements personnels, mais sans que la consultation de ces renseignements soit nécessaire à l'accomplissement de leurs fonctions. Il faudra alors procéder à la dépersonnalisation des données.

L'article 25 de la loi ajoute que:

> « la personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les *mesures de sécurité propres à en assurer la confidentialité*, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement »

ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. Par exemple, on pourrait rendre illisible les données à l'écran, mettre en place des mots de passe pour les personnes autorisées avant d'accéder à l'information et mettre en place de mesures empêchant l'accès détourné à un document ou à un renseignement personnel.

Un point très intéressant dans cette loi tient au fait de l'obligation de former une sorte de « cordon de confiance » (chain of trust)[90], entre les divers partenaires commerciaux par un lien contractuel assurant la sécurité des données lors de la transmission et durant toute la durée où elles seront entre les mains d'un tiers. En effet, dans son intention de conserver la neutralité technologique de la loi, le législateur n'a pas cherché à favoriser une technologie plutôt qu'une autre. Ainsi, dans son esprit innovateur, le législateur a été conscient des investissements considérables que peuvent représenter tant l´acquisition de technologies de fine pointe que la mise en place d'un programme de sécurité informatique à l'échelle de l'entreprise.

Ainsi, selon l'article 26,

> « Quiconque confie à un prestataire de services la gestion des documents électroniques doit, au préalable, informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance. »

Quant à lui, le prestataire est tenu, durant la période de conservation des informations, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité, en protéger la confidentialité et empêcher l'accès à toute personne non autorisée à en prendre connaissance. Par exemple, dans le domaine de l'archivage électronique, le tiers archiveur doit être particulièrement attentif dans ses relations avec les tiers (sous-contractants) dans la mesure où il est le seul responsable à l'égard du donneur d'ordre des fautes commises par les autres en l'absence de relation contractuelle. Dans la mesure où l'entreprise propriétaire des données personnelles n'est souvent pas partie à

[90] Voir article 19, 25 et 36 de la loi.

ces contrats, il convient que le tiers archiveur lie juridiquement cette dernière soit par une clause contractuelle soit par une autorisation expresse.

L'article 19, la loi s'intéresse à « l'obligation des personnes responsables de la conservation en leur imposant le devoir d'assurer le maintien de l'intégralité du document électronique pendant toute la période de conservation, prescrite soit par la loi soit par le contrat, et aussi de garantir l'accessibilité et l'intelligibilité du document et de l'utiliser aux fins qu'il a été destiné. » On évite ainsi que les documents technologiques ne soient plus accessibles en raison de l'indisponibilité du système informatique ou autres instruments nécessaires à sa lecture. Dès lors, la personne responsable de la conservation du document doit disposer du matériel nécessaire à sa consultation. Ceci a donc un impact en ce qui concerne le droit d'accès aux renseignements personnels.

Ce cordon de confiance peut être garanti par des clauses contractuelles portant sur les mesures de sécurité suivantes : s'assurer que le contractant s'engage à appliquer les mesures de sécurité, particulièrement diffuser des directives à l'intention de son personnel sur le contenu du contrat ; faire signer à toute personne à son emploi, qui dans le cadre de l'exercice de ses fonctions, manipule ou a accès aux renseignements personnels visés, un engagement de confidentialité en regard de ces renseignements, et ce, préalablement à leur premier accès à ces renseignements; transmettre au propriétaire des données personnelles ces engagements à la confidentialité ; prendre toutes les mesures de sécurité relatives à l'intégrité physique des lieux où sont stockés les renseignements personnels afin que leur confidentialité soit garantie autant lors de l'utilisation que lors de leur conservation ou destruction ; détruire les renseignements personnels lorsque le contrat est exécuté (si applicable) ; informer de tout manquement à l'obligation d'assurer la confidentialité des renseignements personnels que ce manquement résulte de son fait, de celui de ses employés. Il est intéressant que l'entreprise se réserve le droit de s'assurer qu'en tout temps, le contractant a respecté les dispositions prévues au contrat visant notamment au caractère confidentiel.

De plus, lors d'une transmission sur le réseau, l'article 34 précise l'obligation d'assurer le maintient de la confidentialité du document. Ainsi,

> « lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication », et ce, de façon à garantir la valeur juridique du document reçu et prouver que son intégrité a été préservée (art. 30).

Outre cette obligation, la documentation expliquant le mode de transmission et les moyens pris pour assurer la confidentialité doit être disponible. À ce propos la commission d'accès à l'information rappelle que

> « le cryptage ou chiffrement constitue une mesure de sécurité particulière pour préserver temporairement la confidentialité d'un renseignement personnel durant sa transmission ou son entreposage. Un renseignement personnel crypté demeure confidentiel du fait que sa transformation reste passagère et réversible. »[91]

La Loi reconnaît aussi la possibilité d'utiliser plusieurs modes d'authentification de l'identité d'une personne qui fait appel aux documents technologiques pour communiquer, et en

[91] M. CHASSÉ, précitée, note 83, p. 13.

ce sens la Loi a plusieurs implications au niveau de la protection de la vie privée, particulièrement en ce qui a trait aux banques de caractéristiques ou de mesures biométriques. L'article 45 prévoit que la Commission d'accès à l'information doit être informée de toute création d'une banque de données, en service ou non, contenant des renseignements biométriques.

> « La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne ».

Là encore, l'entreprise qui désire instaurer un système d'authentification basé sur les caractéristiques biologiques de ses employés devra être consciente de ces obligations tant auprès de la commission que veiller à ne pas brimer les droits fondamentaux des employés. Sur ce sujet, l'article 44 prévoit que :

> « Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit fait au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance. […]
>
> Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus. »

La Loi vise aussi l'harmonisation des systèmes, des normes et des standards techniques, harmonisation qui *devra* se faire par le Bureau de normalisation du Québec. L'article 64 prévoit d'uniformiser les pratiques d'audit, lequel comporte l'examen et l'évaluation des méthodes d'accès, d'entretien ou de sauvegarde du support, des mesures de sécurité physiques, logiques ou opérationnelles. Malheureusement, le Bureau de normalisation n'a encore émis aucune norme ou directive sur le sujet, laissant encore une fois les entreprises à une certaine instabilité ou à un vide juridique.

2.2.4. Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale

Le Conseil du Trésor est l'une des instances québécoises qui s'est intéressée à la question de la sécurité et de la protection des renseignements personnels au sein des réseaux informatisés de l'administration québécoise. La mission de cette entité n'est pas la gestion des problèmes reliés à la sécurité sur les réseaux informatiques du gouvernement. Cependant, un « apport » au problème de sécurité devenait approprié du fait que :

> «[…] les technologies de l'information sont maintenant intégrées dans la vaste majorité des activités courantes de chaque ministère et organisme, elles favorisent une accumulation, une concentration, une

> dispersion et une circulation telles que l'information est plus facilement accessible et plus vulnérable et les risques de perte, d'altération ou d'autres manipulations sont considérablement accrus. Afin d'assurer une *sécurité adéquate* (nos italiques), des règles de conduite et un partage des responsabilités entre les intervenants portant spécifiquement sur les banques d'information électroniques, les systèmes d'information, les technologies de l'information et les installations sont nécessaires. »[92]

C'est dans cet ordre d'idées, que le 23 novembre 1999, la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale québécoise*[93]. Bien que cette directive n'ait aucun impact dans le secteur privé, elle nous paraît particulièrement intéressante au niveau de la structuration et de la gestion de la sécurité et du fait qu'elle peut être récupérée, après certaines adaptations, par les entreprises en général. L'objet de cette directive est d'identifier

> « les intervenants concernés par la gestion de cette sécurité, détermine[r] les responsabilités […] et prévoi[r] l'instauration des mécanismes de coordination et de collaboration appropriés en vue d'assurer la disponibilité, l'intégrité, la confidentialité de l'information numérique, l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent. »

La *Directive québécoise* a aussi des objectifs de sécurité, soit la mise en place d'un ensemble cohérent de pratiques administratives et de mesures de prévention, de détection et de correction des incidents de sécurité. La même directive contient aussi des indications au sujet de la gestion de la sécurité, particulièrement la planification, la réalisation, l'évaluation, la vérification, l'organisation de la sécurité, le suivi de contrôle, ainsi que la mise en commun des ressources et l'adoption de normes gouvernementales. Enfin, elle accorde une attention particulière à la responsabilisation et à l'identification des rôles des divers acteurs au sein des ministères.

La *Directive québécoise* propose un certain nombre de principes directeurs qui permettent d'atteindre une saine gestion de la sécurité informationnelle. Ainsi, elle prévoit que les ministères et organismes, qui sont responsables de la sécurité de l'information numérique qu'ils détiennent, utilisent ou échangent électroniquement, doivent mettre en œuvre un ensemble de mesures destinées à gérer les risques et leurs impacts à l'égard de : disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité[94]. Ces mesures de sécurité doivent être mises en œuvre dès la conception, la réalisation ou la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques et cela durant tout le cycle de vie de l'information numérique, soit :

> « la période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de

---

[92] P. TRUDEL, précitée, note 13, p. 7-113.
[93] CONSEIL DU TRÉSOR DU QUÉBEC, Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale québécoise, Sous-secrétariat aux inforoutes et aux ressources informationnelles, 23 novembre 1999, en ligne : < www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf >. [Ci-après *Directive québécoise*].
[94] Id., Section II, §1, art. 4.

> l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information »[95].

L'article 15 de la Directive expose clairement les mesures de sécurité devant être mises en œuvre. Elles incluent, notamment, la nécessité de définir clairement les valeurs organisationnelles et les orientations internes et de les partager avec les employés, l'établissement d'un mécanisme d'identification des risques, l'établissement d'un plan global de sécurité, l'assignation des responsabilités, l'intégration des obligations de sécurité dans les ententes et contrats, la sensibilisation du personnel, etc.

Cette directive avance l'idée que la gestion efficace de la sécurité doit respecter les principes de la vision commune, de la cohérence, de la responsabilité et imputabilité, de l'évolution et de l'universalité[96]. En effet, l'atteinte d'un niveau de sécurité adéquat nécessite « l'adhésion à une vision et une compréhension communes de la sécurité » par tous, repose sur une « approche globale et intégrée qui tient compte des aspects humains, organisationnels, physiques, techniques et juridiques et demande la mise en place d'un ensemble de mesures coordonnées de prévention, de détection, de correction et de sanction ». Mais son efficacité dépend de « l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place de mécanismes de coordination et de contrôle permettant une reddition de comptes adéquate ». Finalement, « les pratiques et solutions techniques retenues en matière de sécurité doivent être réévaluées périodiquement afin de tenir compte des changements organisationnels et technologiques ainsi que de l'évolution des menaces et des risques » et « doivent correspondre dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale. »

2.3. États-Unis

Au contraire des pays européens, les États-Unis n'ont aucune loi générale ou centrale en matière de protection des données personnelles. Bien sûr, il existait déjà dans les années 70 une ou deux lois applicables à des sujets précis, comme le Fair Credit Report Act de 1970[97] qui s'applique à la divulgation d'informations sur le crédit et qui sur ce point est très semblable aux lois en vigueur en Europe ou le Video Privacy Protection Act, résultat de la réaction quasi immédiate à la publication, dans un journal de Washington, de la liste des filmes loués par le juge Robert Bork après sa nomination à la Cour suprême. Nous sommes donc loin de la philosophie soutenue en Europe, où la protection des renseignements personnels fait partie des droits fondamentaux des individus.

Le droit Américain en matière de renseignements personnels repose sur le right of privacy, concept développé par la Cour suprême des États-Unis, sous la plume des Juges Warren et Brandeis[98]. Malgré cela, le développement des normes de vie privée repose sur les lois fédérales très spécifiques dans divers secteurs de la société. En effet, s'il est vrai que la majorité des lois américaines n'imposent pas d'obligations explicites de sécurité aux entreprises du secteur privé, le contraire se produit dans le secteur public et les échanges entre le secteur privé et le gouvernement se faisant de plus en plus nombreuses, implicitement ces compagnies sont se retrouvées liées par les garanties de sécurité imposées par les lois du secteur public. C'est notamment, le cas du Federal Privacy Act et les deux lois particulièrement intéressantes

---

[95] Id., art. 2.
[96] Id., art. 5.
[97] 15 U.S.C.S. 1681.
[98] Samuel D. WARREN et Louis D. BRANDIES, (1890) « The right of Privacy », 4 Harvard Law Review 193, en ligne: <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>.

en matière de sécurisation des renseignements personnels : le Gramm-Leach-Bliley Act (GLB) et le Standards for Privacy of Individually Identifiable Health Information.

2.3.1. Federal Privacy Act de 1974

Le Federal Privacy Act[99] de 1974 s'applique à toutes les entités fédérales qui collectent, utilisent et partagent des données à caractère personnel. La loi s'applique aux données personnelles en général, ce qui inclu les données médicales. Même avant l'adoption des Lignes de l'O.C.D.E. sur la vie privée, ce texte de loi se basait déjà sur l'idée que les individus ont le droit de savoir quelle information personnelle est détenue par le gouvernement et comment cette information est utilisée, de même que le droit de corriger ces informations. Les entités doivent donc mettre en oeuvre des pratiques qui visent à donner à l'information des mesures de sécurité garantissant leur confidentialité. Ces pratiques sont inspirées du Code of Fair Information Practice Principles[100] du département américain de la santé, établi en 1973.

La loi oblige les entités à établir des règles de conduite visant les personnes qui sont

> « involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance».[101]

Elle cherche aussi à établir des mesures administratives, techniques et physiques appropriées pour garantir la sécurité et la confidentialité des dossiers et de se protéger contre les menaces ou incidents de sécurité pouvant provoquer des dommages substantiels, inconvénients, injustice à l'individu visé par ces données personnelles.

En 2000, les États-Unis ont adopté le Safe Harbor Framework[102], qui détermine et harmonise les standards nationaux avec ceux de l'Union européenne. Ce compromis permet l'établissement de règles de base en matière de gestion adéquate des données personnelles, principes auxquels les entreprises peuvent souscrire sur une base volontaire[103]. Aux termes du Safe Harbour, les entreprises qui y adhèrent doivent s'assujettir aux obligations d'information, de consentement préalable, d'accès et de modification aux données et aussi, d'entourer la gestion des dossiers contenant de renseignements personnels par de mesures de sécurité raisonnables garantissant leur protection et leur intégrité.

2.3.2. Lois sectorielles applicables, entre autres, en matière de protection des données personnelles

---

[99] Federal Privacy Act, 5 U.S.C. 552a, en ligne: <http://www.usdoj.gov/foia/privstat.pdf>.
[100] US DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS), Code of Fair Information Practice Principles, 1973, en ligne: <www.ftc.gov/reports/privacy3/fairinfo.htm>.
[101] Federal Privacy Act, précitée, note 99, section (c) *Agency requirements*, par. 10.
[102] US Department of Commerce, Safe Harbor Framework, Washington, juillet 2000, en ligne : <www.export.gov/safeharbor/sh_documents.html>.
[103] UNION EUROPÉENNE, « U.S. Safe Harbour Arrangement, draft discussion documents », 19 novembre 1999, en ligne : <http://www.europa.int/comm/internal_market/en/dataprot/news/harbour2.htm>.

Complétés en décembre 2000 et entrés en vigueur en avril 2003, les Standards for Privacy of Individually Identifiable Health Information[104] (HIPAA Privacy Rule) forment les normes nationales en matière de protection des données personnelles relatives à la santé aux Etats-Unis. Ces standards sont le résultat de l'augmentation de l'intérêt de la part du gouvernement dans la protection de la vie privée et les transactions administratives dans le secteur.

De façon résumée, le HIPAA Privacy Rule impose des standards de sécurité semblables à ceux imposés par les lignes de l'O.C.D.E. sur la vie privée. D'après les obligations administratives de la section 164.530, les institutions « must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information ». Cette section impose aussi un devoir de protéger de façon raisonnable (« reasonably safegarding ») les données. D'autres dispositions complètent et élaborent des standards additionnels. C'est le cas notamment des mesures administratives de sécurité associées à l'accès de données codées et des standards de ré-identification. De plus, le niveau minimal de sécurité implique l'implantation de mesures de sécurité administratives et organisationnelles comme l'obligation de former des employés afin de s'assurer que ces derniers adhérent aux politiques de vie privée institutionnelles et de ses procédures.

Dans le secteur des institutions financières, la section 501du Gramm-Leach-Bliley Act[105] dispose que ces dernières ont une obligation positive et continue de respecter la vie privée de ces clients et protéger la sécurité et la confidentialité des informations personnelles. Le paragraphe (b) oblige les institutions financières à établir des standards appropriés

> « relating to administrative, technical, and physical safeguards in order (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. »

Pour conclure ce deuxième chapitre, disons qu'entre le droit et la sécurité la complémentarité est intéressante. Si le droit invite à un renforcement de la sécurité des systèmes contenant des renseignements personnels, à l'inverse, la sécurisation technique se manifeste de plus en plus comme la meilleure garantie de la protection des droits fondamentaux.

Chapitre 3. L'étude et planification d'un programme de sécurité

Nous avons vu dans le dernier chapitre, qu'une entreprise ou un organisme a la responsabilité légale de garantir la *protection adéquate* des renseignements personnels. Cette responsabilité repose grandement sur la planification, l'organisation et la réalisation d'un ensemble d'activités permettant la mise en application des règles juridiques et techniques particulières pour chacun des moments clés du cycle de vie des renseignements personnels. La protection de ceux-ci doit donc faire partie des objectifs stratégiques de l'entreprise et doit faire l'objet d'un appui et d'un engagement manifeste de la part de ses dirigeants.

---

[104] US Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information—Final Rule, Registre Féderal, 28 décember 2000; 65(250): 82462, codifé 45 *Code of Federal Register* 160 et 164, en ligne: <www.hhs.gov/ocr/hipaa>. [ci-après HIPAA Privacy Rule]

[105] 15 U.S.C.S. 6801(b).

L'un des avantages d'une gestion globale de la sécurité, sans doute le plus intéressant pour les entreprises, est la réalisation d'économies dans leurs relations tant avec les employés, qu'avec les clients ou partenaires commerciaux. Puisque la mise en place d'un programme de sécurité globale implique essentiellement le triage des informations personnelles détenues, le résultat de cet exercice sera une facilitation de l'administration et du contrôle de l'entreprise. Malheureusement, les ressources informationnelles sont mal gérées dans les compagnies : les gestionnaires n'arrivent plus à différencier les informations personnelles importantes, nécessaires au bon fonctionnement de l'entreprise et à la prise de décisions, des informations complémentaires et inutiles. En éliminant les renseignements personnels désuets, l'entreprise réalisera des économies substantielles en temps de traitement, d'analyse de l'information, de protection et d'espace de conservation, mais surtout réduit les risques d'une poursuite judiciaire en vertu des principes de la protection des renseignements personnels étudiés ci-haut, notamment les principes de justification et de la qualité des données.

Les normes et les politiques de sécurité ne sont pas seulement un outil aidant les entreprises à protéger leurs propres informations et leurs propres clients, mais réussissent également à établir un cadre contractuel menant les employés à respecter les normes de sécurité informationnelle. Il existe toutefois des règles de base à suivre pour mener à terme cette tâche. Il faut avant tout obtenir l'appui de la direction et solliciter la participation des différents niveaux hiérarchiques de gestionnaires, afin de faciliter l'acceptation des normes, et enfin il faut communiquer le bien fondé de ces normes de sécurité et de ces avantages dans un langage d'affaires.

L'information gardée par une entreprise est un actif aussi important que tout autre actif d'affaires et comme tout autre actif elle a une valeur patrimoniale pour l'organisation et par conséquent, doit recevoir une protection adéquate. La sécurité informationnelle protège l'information d'une vaste gamme de menaces afin de garantir la continuité des affaires, minimiser les dommages et maximiser les profits et les occasions d'affaires.

Ce chapitre se dédie à l'étude générale de la structure d'une politique de sécurité et à sa rédaction, ainsi qu'à la méthode d'évaluation des risques, étude qui servira de base à la mise en place d'un programme de sécurité global et cohérent, garantissant le niveau de protection adéquat des renseignements personnels détenus par l'entreprise.

Section 1. La structure d'une politique de sécurité

La sécurité c'est d'abord et avant tout s'organiser. Puisque nous aborderons, tout au long de ce mémoire, plusieurs fois le terme « politique de sécurité », il nous paraît dès lors nécessaire d'expliquer en quoi consiste le rôle d'une politique dans la mise en place de mesures raisonnables de sécurité informationnelle, en quoi elle peut être utilisée comme une partie active de l'effort d'une entreprise pour protéger ses actifs informationnels et surtout comment celle-ci est composée.

Les politiques de sécurité permettent aux entreprises d'établir des pratiques et procédures qui réduiront la probabilité d'une attaque ou d'un incident informatique et permettront de minimiser les dommages qu'un tel incident peut produire, le cas échéant. Plusieurs perçoivent les politiques de sécurité comme un « après problème » ; la touche finale dans une recette de sécurité informatique avec des murs coupe-feu (firewall), antivirus, etc. Ceux qui pensent de cette manière font fausse route.

Par exemple, aux Etats-Unis, le General Accounting Office (GAO) a conclu qu'il lui était possible de pénétrer dans les systèmes informatiques de la NASA par suite de l'absence complète de politique de sécurité. La NASA n'avait pas établi de règles concernant l'usage de

l'Internet et des réseaux sécurisés et les quelques règles qu'elle avait promulguées étaient ou bien périmées ou bien non suivies.[106] Donc, l'impact de l'absence de politique de sécurité peut être fatal pour toute entreprise.

Dans ce chapitre, nous essaierons de comprendre pourquoi les politiques de sécurité doivent être la base d'une stratégie de sécurité informationnelle cohérente et comment elles peuvent devenir un aspect pratique et efficace dans la protection des systèmes d'information, des renseignements personnels qu'ils contiennent et dans le respect des obligations légales imposées aux entreprises.

La définition la plus élémentaire du terme « politique de sécurité » est sans doute celle donnée par le Grand dictionnaire terminologique[107]. Ainsi, est une politique de sécurité l'« énoncé généralement de la direction d'une organisation, indiquant la ligne de conduite adoptée relativement à la sécurité informatique, à sa mise en œuvre et à sa gestion. » En termes pratiques la politique de sécurité est un document publié (ou un groupe de documents) dans lequel la philosophie, la stratégie, les diverses politiques et pratiques de l'entreprise relativement à la *confidentialité*, l'*intégrité* et la *disponibilité* de l'information et des systèmes d'information sont exposés. Donc, la politique est un ensemble de mécanismes par lesquels les objectifs de sécurité de l'information sont définis.

Abordons maintenant les logiques de base d'une politique de sécurité permettant la réalisation de ces objectifs. Tout d'abord, toute politique doit être rédigée en respectant une certaine philosophie. Cette philosophie présente l'approche de l'entreprise dans la mise en place d'un cadre et des lignes directrices dans la stratégie de sécurisation. Celle-ci est la base sur laquelle tous les autres mécanismes seront appliqués. Ensuite, l'entreprise devra avoir une stratégie globale, un plan qui lui permettra de respecter sa philosophie. Cette stratégie devra expliquer comment l'organisation a l'intention d'atteindre les objectifs de sécurité dans les barèmes de sa philosophie. Dans le cas des règlements internes (« policies »), ils sont de simples règles à suivre. Ils déterminent ce qui est permis ou interdit de faire en matière de sécurité des renseignements personnels. Finalement, les procédures définissent le « comment faire » pour respecter les règlements internes. Elles sont les guides pratiques, des manuels d'instruction.

La meilleure façon de louper tout projet de sécurisation d'une entreprise est de ne pas se donner un objectif. Une politique de sécurité sert avant tout de ligne directrice pour l'entreprise qui veut se doter d'un environnement fiable en procurant des objectifs de sécurité à atteindre.

> « A security policy for a system is like a foreign policy for a government. […] It defines aims and goals. […] No policy means no overall strategy. […] Good policies talk to the threats. It provides a framework for selecting and implementing countermeasures against the threats. »[108]

Même si ceci semble évident à première vue, force est de constater que, la réalité dans laquelle la majorité des entreprises se situent est autre. Selon le rapport de mars 2002 de

---

[106] Diane FRANK, « NASA systems full of holes », Federal Computer Week, 24 mai 1999.
[107] GRAND DICTIONNAIRE TERMINOLOGIQUE, précitée, note 15.
[108] Bruce SCHNEIER, Secrets and Lies: Digital Security in a Networked World, John Willey & Sons, New York, 2000, p. 308.

Ernest & Young[109], environ 50 % des entreprises à travers le monde n'ont aucune politique de sécurité et de celles qui en ont, rares sont celles qui, à l'aide d'un programme de formation, la font connaître à leurs employés. Ce sont des failles alarmantes et certaines entreprises, tant dans le secteur privé que public, peuvent être considérées comme irresponsables dans leur approche de la sécurité informatique, la gestion de laquelle est maintenant critique pour la survie du commerce et maintenir un avantage compétitif. La politique de sécurité est à la sécurité informatique ce que la loi est au droit. Sans la politique, les mesures de sécurité seront développées sans une démarcation claire des objectifs et de la responsabilité, menant à l'augmentation des vulnérabilités.

Il n'y a aucun modèle standard applicable à toutes les entreprises. Chaque politique de sécurité doit être rédigée en tenant compte de la philosophie de l'entreprise et surtout en fonction de ses objectifs. L'identification des objectifs est l'un des résultats obtenus par l'analyse des risques, processus essentiel traité en détail dans la prochaine sous partie. Elle doit être rédigée en considération des ressources financières et le type d'information qui doit être protégée. Les objectifs typiques, aussi repris par les diverses lois concernant la protection de données sensibles, incluent la confidentialité, l'intégrité de l'information et la disponibilité des systèmes, soit les 3 qualités fondamentales de la sécurité informationnelle.[110]

Toutefois, pour être efficace une politique de sécurité doit respecter certains points. Le respect de ceux-ci s'avère être la manière la plus sure de réussir le processus d'acceptation du document, tant par l'administration que par les employés. Elle doit être, avant tout, réaliste et afin d'être efficace elle doit être perçue par les utilisateurs comme profitable. La politique doit être accessible et mise à disposition des employés de manière rapide, sous peine de tomber dans l'oubli organisationnel.

En bref, la politique de sécurité devrait préférablement, et de manière non exclusive, regrouper les éléments suivants : le préambule expliquant l'objectif de la politique, la confidentialité des données personnelles, la gestion des documents, la désignation d'un point unique de dénonciation des incidents, la mise en place d'outils de préservation de preuves de l'incident, une équipe d'avertissement de risques et nouvelles menaces, détermination des responsabilités et des sanctions, procédure de sauvegarde des informations cruciales et de recouvrement, les virus et l'authentification.

Dans certains domaines de l'industrie, les entreprises ont des obligations légales relativement à l'intégrité et la confidentialité de certaines informations. Dans plusieurs cas, le seul moyen de faire la preuve de diligence raisonnable est de présenter en preuve la politique de sécurité publiée et connue. Parce que la politique de sécurité est normalement publiée, et parce qu'elle représente la décision exécutive, elle peut être tout ce que l'entreprise a besoin pour convaincre un client potentiel, un partenaire ou un investisseur du niveau de maturité de l'entreprise. De plus en plus, les entreprises requièrent de la part de leurs partenaires commerciaux la preuve des mesures de sécurité adéquates avant de conclure un accord et encore une fois une politique de sécurité est un bon commencement. Vous trouverez en annexe un exemple de politique simple en matière de sécurité et de confidentialité.

---

[109] ERNEST & YOUNG, «Global Information Security Survey 2002», Ernest & Young LLP, mars 2002, en ligne: Ernest & Young < http://www.eyindia.com/pdfs/Info%20Security%20Survey%202002.pdf>.
[110] Joël HUBIN, Sécurité informatique, entre la technique et droit, Cahiers du C.R.I.D. nº 14, Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 7.

Mais avant de rendre des décisions, à court et à long terme, concernant la sécurité, l'entreprise doit avoir une vision claire et précise de leur profil de risque. Le risque consiste en la combinaison des ressources informationnelles qui ont une valeur monétaire et les vulnérabilités qui peuvent être exploitables. La magnitude du risque est le produit de la valeur de l'information et le degré de risque d'exploitation d'une vulnérabilité.

Section 2. L'évaluation et la gestion des risques[111]

La sécurité c'est non seulement s'organiser, c'est aussi prévoir les incidents. L'illustration souvent retenue par les experts en sécurité informationnelle est que les renseignements sensibles gardés dans l'ordinateur peuvent être absolument en sécurité si l'ordinateur en question est déconnecté de tout, gardé dans un bloc de béton, largué au bon milieu de l'océan, dans un endroit inconnu de tous. Mais dans le monde des affaires, des risques doivent être pris ou assumés de façon à garantir la survie de l'entreprise et l'efficacité des systèmes de l'information. Parce qu'aucun système ne sera jamais absolument (ni presque) sécuritaire, l'alternative est de reconnaître qu'un certain niveau de risque est nécessaire pour garantir la survie de l'entreprise dans le monde commercial et prendre les mesures adéquates pour gérer ce risque, soit par l'entremise de la technologie ou procédures techniques, soit en transférant le risque résiduel à un tiers par la voie contractuelle ou par l'assurance. [112]

Les méthodes d'évaluation des menaces et des risques (EMR) permettent de déterminer la nature et le niveau des mesures que l'on devra mettre en place en fonction des exigences en matière de confidentialité, d'intégrité et de disponibilité du système d'information et des données personnelles, en fonction de leur degré de sensibilité. Bon nombre de responsables ne savent pas comment aborder les EMR. N'ayant pas de méthode, ils procèdent au coup par coup, errant du « *de toute façon, ça ne sert à rien* », au « *vaut mieux en faire de trop que pas assez* ». Une approche méthodologique explicite, soit l'élaboration des modèles, définition des procédures, caractérisation du « cycle de vie », permettra les décisions cohérentes et raisonnées.[113]

Les investissements en sécurité doivent être en équilibre avec le niveau de risque et de dégâts supportés par l'entreprise en cas de vulnérabilité informatique. Les techniques d'évaluation des risques peuvent être appliquées à toute l'entreprise, ou à certaines parties, à des systèmes informatiques individuels, à certaines composantes ou services. Le résultat de cette analyse de risques guidera l'entreprise dans le choix des mesures de protection à adopter et dans la gestion de la sécurité.

L'initiation du processus d'analyse et de gestion des risques commence par la sensibilisation aux risques encourus par l'entreprise d'une personne influente au sein de l'administration. Il faudra insister sur la nécessité d'établir et de faire respecter une politique de sécurité. De cette sensibilisation résultera deux choses : l'élaboration d'une politique brouillon et la formation d'une équipe de personnes compétentes en informatique et les représentants de

---

[111] Pour un guide détaillé sur l'analyse des risques voir, Gary STONEBURNER et al., Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, SP 800-30, Washington, 2001.

[112] Concernant les contrats d'assurance informatique voir, Paul VAN HOUTTE, « Les assurances », dans J. HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 241.

[113] R. LONGEON et J.L. ARCHIMBAU, Guide de la sécurité des systèmes d'information – à l'usage des directeurs, Centre national de la recherche scientifique, Paris, 1999, p. 42.

divers départements, dont le juridique.[114] Avant de commencer l'analyse des risques, nous rappelons l'importance des connaissances générales en droit, notamment les diverses obligations juridiques en matière de protection de renseignements personnels et l'émergence de la culture de sécurité décrite dans divers textes des organisations internationales.

Lorsqu'un individu accepte de partager des informations personnelles avec un tiers, dans ce cas-ci une entreprise, il court certains risques, c'est à dire, un événement incertain dont la survenance provoque un dommage ou une atteinte à un droit. Ces risques peuvent être résumés comme suit : la perte de contrôle sur les données, la réutilisation des données par une personne non autorisée ou non identifiée, la non conformité des données et leur inexactitude.

L'un des premiers risques rencontrés survient lorsqu'un individu visé par les renseignements ne sait plus qui sait quoi à son sujet, se résumant en une perte de contrôle sur les informations. Si en plus une entreprise ne met pas en place des mesures de sécurité adéquates, les données recueillies peuvent être réutilisées à des fins différentes de celle annoncée à l'origine ou utilisées par des personnes non autorisées. Le risque d'utilisation de données non exactes ou qui ne sont pas actuelles peut mener à la prise de décisions injustes par les utilisateurs des données. Ce risque peut causer un dommage considérable puisqu'il est normalement difficile de corriger les données une fois celles-ci partagées avec des tiers.

Nous l'avons vu, le risque de traitement des renseignements personnel pourra varier selon la sensibilité de ces derniers. Plus une donnée est de nature sensible, plus le risque augmente. Un autre facteur pouvant influencer le niveau de risque est le volume de données gardées et le nombre de personnes impliquées. Mais, la technologie employée influence grandement le risque. Un ordinateur isolé et non connecté au réseau présente à première vue moins de risque que la sauvegarde de données personnelles par des systèmes interconnectés, où un usager est en mesure de se brancher de n'importe quel poste de travail. De plus, si le transfert de données s'effectue via Internet, le risque d'interception et de réutilisation est beaucoup plus éminent que celui effectué sur un réseau fermé et privé, comme le réseau bancaire par exemple.

En tenant compte de tous ces facteurs pouvant influencer le niveau de risque auquel l'entreprise est confrontée, il faudra procéder à son découpage sur la base des ressources, des partenaires, secteurs d'activité, division géographique, départements, services ou fonctions. On sera dès lors en mesure d'établir pour chaque entité une fiche d'identité reprenant son organisation, sa situation au sein de l'entreprise, son importance, ses clients, fournisseurs et liens. Une fois ceci terminé, le pas suivant consiste en la définition du type d'accès nécessaire et des personnes pouvant y accéder. Une fois que l'entreprise comprend comment chacun usager peut accéder aux diverses informations, elle devra analyser la sensibilité de ces dernières et les risques d'être volées, endommagées ou détruites.

Avant de définir clairement nos besoins en matière de sécurité, il faut effectuer un inventaire du système informatique et une classification des informations (énoncés de sensibilité) gardées par ces systèmes. Nous aurons la possibilité d'étudier la classification des informations personnelles lorsque nous parlerons des mesures administratives dans la deuxième partie de ce mémoire. Faire l'inventaire s'agit essentiellement de repérer les biens manipulés au sein de l'entreprise. Cet exercice devra déboucher à une description des biens, indiquant pour chaque bien la description, sa localisation, le responsable. On pourra dès lors les regrouper par type de perte.

---

[114] J. HUBIN, précitée, note 110, p. 21.

Ensuite, pour chaque bien identifié, il faudra déterminer les problèmes attendus. Notons qu'un inventaire exhaustif des failles des biens est impossible. Pourtant, il est possible d'établir une grille d'analyse chiffrant les pertes prévues. D'après cette grille, nous serons en mesure d'évaluer les pertes engendrées par un type de problème ou l'absence totale de mesures de sécurité engendre une perte égale à la valeur totale du bien. Pour chacune des ressources vulnérables, faire une liste des menaces pouvant causer des dommages et déterminer leur probabilité.

La probabilité de survenance est évaluée en fonction du passé. Elle dépendra des mesures de sécurité implantées et devra être chiffrée de façon précise. En fonction de cette probabilité de la menace et de la valeur des biens, nous sommes en mesure de calculer un facteur de risque pour chacun d'eux. On doit garder à l'esprit que l'impact commercial d'un incident dépend toujours du coût et du temps.

L'analyse des facteurs de risque permettra à l'entreprise de classer les risques et les biens à risque selon leur importance (graves, légers, bénins) et se concentrer sur les mesures à mettre en œuvre avec plus d'urgence.

Finalement, le comité responsable de l'analyse des risques devra préparer un exposé pour convaincre l'administration des avantages d'un programme de sécurité. L'objectif est de persuader les personnes influentes que la sécurité est rentable à long terme et qu'il est toujours préférable de procéder à l'examen *avant* l'avènement d'un incident pouvant avoir un impact sur les activités quotidiennes de l'entreprise que procéder à l'autopsie de l'entreprise. Le rapport de l'analyse des risques devra fournir à l'administration une vision complète du niveau actuel de sécurité, ses défauts, les obligations imposées par les lois, la possibilité des pertes, l'état de sécurité de la concurrence, etc. Ce rapport donné à l'administration de l'entreprise facilitera le déroulement des phases de sensibilisation, de formation, de définition des responsabilités et permettra de diminuer les délais d'applications. Bref, le rapport sert de base à l'élaboration technique du programme de sécurité, thème que nous aborderons de manière significative dans la deuxième partie du mémoire.

Section 3. La rédaction de la politique de sécurité

La rédaction de la politique est la dernière étape de la planification de la sécurité. Cette partie du processus est la partie décisionnelle, puisque l'administration devra choisir les mesures les plus rentables, en se basant sur les résultats des étapes antérieures, par rapport aux objectifs de la compagnie.

Mais avant de se lancer dans la rédaction d'une politique de sécurité, il est préférable de revoir les politiques et les mesures de sécurité déjà en place. Cette étape donne l'occasion à l'entreprise de revoir l'efficacité des règlements internes et procédures en vigueur et surtout les changements nécessaires. Vu que la clé du succès de tout programme de sécurisation réside dans l'acceptation par ceux qui sont visés, avant de se lancer dans la définition des besoins, l'entreprise devra créer des standards quantitatifs de conformité à ces règles et procédures, tester les procédures et les pratiques de sécurité de l'organisation et évaluer l'efficacité de ces dernières. Rien ne sert conserver des règles qui ne sont pas suivies.

Ensuite, l'entreprise devra procéder à l'organisation de la protection. Ainsi, pour chaque vulnérabilité identifiée et susceptible d'être exploitée, il faudra déterminer les protections à mettre en place. Elle devra aussi déterminer ce qui demande une protection maximale, définir les meilleurs moyens de protection, établir des priorités selon les objectifs de l'entreprise,

obtenir de la direction les moyens financiers nécessaires, évaluer les méthodes de protection des informations.

Les mesures retenues et celles devant être mises en place devront améliorer de façon globale la sécurité de la compagnie et lui offrir une pérennité. Tout au long de ce processus décisionnel il faudra avoir à l'esprit l'idée suivante : maximiser son profit par une minimisation des frais et des coûts des traitements sécurisés. Plus les mesures retenues sont dispendieuses, plus celles-ci sont efficaces et diminuent ainsi l'espérance de perte. Toutefois, un investissement au-delà du nécessaire pour garantir une protection raisonnable n'est pas rentable.

Le choix des mesures de sécurité doit se faire suite à des scénarios de simulation. Ces simulations permettront de chiffrer l'impact et surtout de déterminer le niveau de risque acceptable. L'entreprise aura alors à choisir la solution qui ne maximise pas le profit, mais qui est jugée plus favorable, évolutive et moins agressive. Améliorer le niveau global de sécurité et définir un système cohérent qui minimise les failles. Définir un système global homogène au niveau de la proportion entre les mesures de prévention, détection, intervention, restauration et autres.

Une fois les mesures de sécurité appropriées choisies et le retour sur l'investissement appréhendé (return on investment), l'entreprise est en mesure de rédiger sa politique de sécurité. La plupart des politiques abordent les thèmes que nous allons définir. Ils forment une partie importante de l'établissement d'une mentalité de sécurité parmi les usagers des ordinateurs et réduisent les risques de poursuites judiciaires pour négligence ou divulgation de renseignements personnels. Une politique de sécurité doit avoir une lettre de l'administration qui met l'accent sur l'idée que la sécurité est une donne vitale pour l'entreprise. Elle doit aussi contenir un préambule énonçant l'objectif de la politique, les personnes visées par cette dernière, l'information et l'équipement concerné et les raisons économiques et commerciales d'une telle pratique.

L'une des parties les plus importantes, clairement présentée par les textes de loi, est la définition claire des responsabilités. Ceci implique la désignation de ceux qui sont responsables de la révision, de l'approbation, de l'application et de l'administration de la politique. En plus, il sera essentiel de définir les rôles de chacun, et préciser que le chef de département (par exemple) doit assurer le respect et la compréhension de la politique et des règles de sécurité par les employés. De plus, les termes techniques utilisés dans les documents de sécurité doivent être définis et expliqués de façon simple pour les employés ; ceci peut prendre la forme d'un glossaire à la fin de la politique, par exemple.

La politique de sécurité doit inclure aussi l'information sur les droits d'accès et de propriété de l'information contenue dans les ordinateurs de l'entreprise ou transmise sur le réseau externe. L'intention d'un tel énoncé est d'aviser les employés sur le fait que l'entreprise se réserve un droit de regard sur les courriels et les fichiers échangés dans le cadre des activités de cette dernière.

Finalement, la partie technique de la politique de sécurité touche les pratiques relatives à l'usage des systèmes informatiques de l'entreprise. Cette partie doit avancer l'idée que les systèmes informatiques de l'entreprise doivent être utilisés pour des fins commerciales. Elle devra stipuler si les employés peuvent ou non utiliser les ordinateurs et le réseau à des fins personnelles et dans quelle mesure cela peut être fait. Un énoncé général de responsabilité des utilisateurs est approprié dans cette section, afin que ceux-ci soient conscients de leurs

obligations en matière de sécurité, notamment, maintenir la confidentialité des renseignements personnels, des mots de passe, la protection des cartes magnétiques, etc. En d'autres mots, cette partie de la politique de sécurité doit résumer les mesures de sécurité administratives, physiques et techniques que nous allons amplement étudier dans la deuxième partie du mémoire.

Il faut aussi bien comprendre qu'une politique de sécurité est un contrat passé entre l'entreprise et les usagers du réseau interne et externe de celle-ci. Et comme dans tout contrat, chacune des parties doit être en mesure de comprendre les mesures de sécurité. De plus, l'entreprise doit prouver, en cas de litige, que ces mesures ont été acceptées. Il est donc prudent, du point de vue de la preuve, de demander la signature du document certifiant la connaissance et la compréhension des règles de sécurité en vigueur dans l'entreprise.

Les politiques de sécurité sont en soi insuffisantes. Leur plein potentiel est directement proportionnel au support et à la planification qu'elles reçoivent de l'administration de l'entreprise. Les contraintes financières ont une influence sur le choix des moyens techniques de sécurité. Ces contraintes peuvent être d'ordre technique (site des installations, matériel disponible, etc.), humaines (nombre d'employés, lois, etc.) et économiques (restriction de budget). Selon l'état de santé de l'entreprise, certaines pertes pourront être permises ainsi que certaines dépenses. Toute décision doit tenir en considération les bilans financiers de l'entreprise et doit être *raisonnable*, en d'autres mots respecter un équilibre entre la valeur des données à protéger et le coût de sécurisation. La sécurité doit constituer un investissement avantageux pour l'entreprise et non pas un fardeau. Toutefois, il est inacceptable qu'une entreprise limite la sécurité de son système informatique nonobstant les risques encourus pour les personnes concernées au seul motif que la technologie disponible est trop dispendieuse.

Notons que l'évaluation des risques est un élément fondamental de la protection des renseignements à caractère personnel. Toutefois, cette évaluation est grandement subjective et variera selon l'entreprise. Ainsi, divers facteurs[115] doivent être pris en compte lors de la rédaction du rapport de l'analyse des risques, notamment : le coût des mesures de sécurité proposées par rapport aux coûts de l'absence de mesures de sécurité, la fréquence *réelle* de chaque catégorie d'infractions à la sécurité, la question de savoir si une infraction cause des dommages *évidents*, la valeur des dommages causés par une catégorie particulière d'infractions à la sécurité, la valeur non monétaire des dommages (quelle valeur faut-il attribuer à la communication non autorisée de renseignements personnels, à l'intérêt national, à la perte d'un client ou de la confiance du public, difficulté à déceler certaines catégories d'infractions à la sécurité, la difficulté à prévenir certaines catégories d'infractions à la sécurité et la possibilité de dommages considérables qui ne risquent guère de survenir, par rapport à la possibilité de dommages moindres qui risquent davantage de survenir.

Il existe trois éléments essentiels pour une sécurité raisonnable : les personnes, les politiques de sécurité et les outils organisationnels, physiques et techniques mis à disposition des entreprises. Nous consacrerons la deuxième partie du mémoire à l'analyse de ces outils et surtout à démontrer en quoi la technique permet de plus en plus le respect du droit.

---

[115] Groupe de travail sur les questions de droit relatives à la stratégie pour la sécurité des technologies de l'information (STI), « Aperçu de la technologie, de la sécurité, de la protection des renseignements personnels et du droit pertinent », Ministère de la justice, Ottawa, p. 14, en ligne : <http://canada.justice.gc.ca/fr/ps/ec/chap/ch01.doc>.

Conclusion de la première partie

En règle générale le droit est lent. Il est le reflet de conventions sociales établies et dans le domaine des nouvelles technologies de l'information, il entre en jeu seulement après que celles-ci ont perdu leur cachet de nouveauté. De plus, le droit est une science souple. Par nature, il s'applique à un grand nombre de situations. Par conséquent, il n'est pas nécessaire d'adopter une nouvelle loi chaque fois qu'apparaît une nouvelle technologie. Puis, nos tribunaux font souvent preuve de leur volonté et compétence lorsqu'ils appliquent les anciens principes du droit à de nouvelles situations déclenchées par le développement technologique. Toutefois d'une chose on peut être certains : la co-existence du droit et de la technologie comme deux monde distincts ne bénéficie personne. En faisant référence à la technique tout en gardant son caractère flexible, le droit peut accompagner de façon aisée le développement rapide des nouvelles technologies sans courir le risque de devenir désuet et surtout, continuer à garantir la protection des droits fondamentaux des individus.

Il est vrai que trouver le juste équilibre entre les différents intérêts des personnes dans les renseignements personnels sont répertoriés et les possesseurs de ces fichiers n'est pas une tâche facile. D'un coté, si la législation en la matière est trop faible, les tentatives d'abus se feront plus nombreuses, par ailleurs, si les lois sont trop rigides nous finissons par interférer de manière inutile dans les intérêts commerciaux légitimes de diverses entreprises. De l'analyse de quelques textes juridiques à portée internationale et des lois nationales qui nous semblent les plus intéressantes pour notre thème, nous arrivons à la conclusion que l'utilisation des renseignements personnels et tous les enjeux que s'y rattachent, notamment la conservation et le niveau de protection adéquat des renseignements personnels, doivent être chaperonnés par le droit. C'est précisément de certains de ces enjeux et l'étude des mesures de sécurité offrant ce niveau adéquat que nous aborderons dans la deuxième partie de ce travail de recherche.

Partie 2. La stratégie de mise en œuvre d'un programme de sécurisation des renseignements personnels

Dans le cas d'une entreprise qui conserve un grand nombre de renseignements personnels, une faille de sécurité peut vraisemblablement résulter en une divulgation de données à caractère personnel, la perte ou la modification de l'information et même, dans un recours en dommages-intérêts pour atteinte à la vie privée. En France, par exemple, selon l'article 226-17 du Code pénal, le manquement à l'obligation de sécuriser un traitement informatique comportant des données personnelles est sanctionné pénalement par une peine maximale de 5 ans d'emprisonnement et 300000 euros d'amende. Les risques légaux reliés à la collecte de données à caractère personnel peuvent donc être très lourds de conséquences pour les entreprises.

Malheureusement, le domaine juridique n'a pas encore su prendre position sur ce point. Nous avons, évidemment, des textes législatifs qui protègent les renseignements personnels, obligeant les entreprises à établir des mesures de sécurité raisonnables et adéquates pour sauvegarder ces derniers, mais sans plus. Aucun guide, aucune harmonisation des normes techniques, aucun niveau minimal clairement défini. Pire, la majorité des juristes ne sont pas encore en mesure de donner un conseil éclairé sur ce point à leurs clients et malgré l'adoption de lois qui sont à première vue, avant-gardistes, prônant la réalité multidisciplinaire et l'augmentation de la confiance des individus face aux systèmes de l'information, nous avons oublié l'essentiel : la définition claire de ces nouvelles obligations. Pourtant, si la sécurité est inhérente aux nouvelles technologies de l'information, elle l'est aussi au droit[116].

Nous avons réservé cette deuxième partie du mémoire à l'analyse de la partie nettement moins « juridique » de la mise en place d'un programme de sécurité adéquat et global, soit la sécurisation des systèmes informatiques contenant des données à caractère personnel. Cette partie sera divisée en trois chapitres, chacun correspondant aux trois catégories de mesures de sécurité, soit les mesures organisationnelles, techniques et physiques. Avant de rentrer dans le détail, attardons-nous sur une succincte définition de ces concepts[117].

Les mesures de sécurité physiques sont constituées de dispositifs physiques permettant d'assurer la sécurité des personnes, la protection de l'environnement et des biens informatiques contre des menaces de caractère physique. Les mesures de sécurité techniques ou logiques se fondent essentiellement sur la mise en place de dispositifs logiciels empêchant l'accès aux systèmes technologiques. Finalement, les mesures de sécurité organisationnelles ou opérationnelles sont formées des procédures et des mesures de vérification relatives à l'ensemble du programme de sécurité du système. Elles établissent l'attribution des droits d'accès, la suspension et l'annulation ce ceux-ci, visent à détecter et à minimiser les erreurs dans les actions du système et dans les interactions de ses éléments. Ces mesures prévoient enfin les modalités d'urgence et de remise en état du système. Ces trois catégories de mesures jouent fondamentalement un rôle de prévention et de détection. Certains contrôles ont pour objectif prévenir l'occurrence des incidents de sécurité, tandis que d'autres visent l'identification des incidents après que ces derniers se sont produits.

---

[116] Vincent GAUTRAIS, « Aspects sécuritaires applicables au commerce électronique », dans Éric LABBÉ, Daniel POULIN, François JACQUOT et Jean-François BOURQUE (directeurs), Le guide juridique du commerçant électronique, Montréal, Juris International, 2001, p. 75.
[117] C.R.D.P., précitée, note 32, p.28.

Outre les contrôles de nature préventive et de détection, certains ouvrages[118] sur la sécurité informationnelle en proposent trois types supplémentaires. Ils sont normalement décris comme des mesures dissuasives, correctives et de récupération visant à décourager un individu qui voudrait intentionnellement violer les politiques et les procédures de sécurité, mesures qui prennent normalement la forme de contraintes qui rendent difficiles ou non attrayantes les activités illicites (ex. la crainte de sanctions pénales ou de sanctions internes).

Quant aux mesures de correction, elles corrigent les circonstances qui ont permis l'activité illicite ou permettent la mise en état du système ou de l'information avant l'incident de sécurité. L'exécution des mesures correctives peut se traduire par des changements dans les mesures physiques, techniques ou organisationnelles

existantes. Les mesures de récupération, quant à elles, recouvrent les ressources informationnelles perdues, facilitent la reprise des affaires dans l'entreprise et l'amortissent les pertes financières éventuelles provoquées par une attaque.

Nous sommes d'avis que les mesures de sécurité dissuasives, correctives et de récupération doivent être intégrées au sein des mesures physiques, techniques et organisationnelles ; elles n'appartiennent pas clairement ni aux mesures préventives ni aux mesures de détection. Par exemple, nous pouvons facilement considérer la dissuasion comme une mesure préventive puisqu'elle peut prévenir un incident de sécurité. D'un autre coté les mesures de correction ne sont ni préventives ni de détection, mais elles sont clairement liées aux mesures techniques (mise à jour des définitions des virus) et organisationnelles (procédures de sauvegarde). Finalement, les mesures de récupération ne sont ni de prévention ni de détection, mais sont incluses dans les contrôles organisationnels comme des plans de contingence. En raison de ces nombreux chevauchements entre les mesures techniques, physiques et organisationnelles, les mesures dissuasives, correctives et de récupération ne seront pas étudiées comme des contrôles distincts. Une entreprise devra considérer tous ces aspects de la sécurité lorsqu'elle décide de mettre en place des mesures de sécurité adéquates.

Chapitre 1. La sécurité organisationnelle et administrative

Section 1. L'administration du personnel

Plusieurs aspects importants de la sécurité informationnelle engagent une variété d'utilisateurs humains : usagers ordinaires, architectes de réseau, programmeurs et gestionnaires informatiques… Un large éventail de mesures administratives reliées à la sécurité aborde justement les interactions de ces individus avec les ordinateurs comme l'accès et les autorisations nécessaires à l'accomplissement de leurs tâches. Aucun système informatique n'est protégé sans ces mesures, elles s'avèrent être la base de tout programme de sécurisation des ressources informationnelles confidentielles et personnelles.

Le facteur humain est incontestablement le chaînon faible de la sécurité informationnelle en raison de divers facteurs[119], notamment, la façon dont les gens perçoivent le risque, dont ils réagissent aux imprévus, leur dépendance face à la technologie, l'incapacité de ceux-ci de prendre des décisions spontanées relatives à la sécurité et le danger des attaques

[118] Voir D. PIPKIN, Sécurité des systèmes d'information, Campus Press, Paris, 2000.
[119] B. SCHNEIER, précitée, note 108, p. 256.

internes intentionnelles ou des actions psychologiques[120]. Les personnes ne savent pas analyser le risque. Elles ne sont pas en mesure de se confronter à une vulnérabilité et prendre une décision intelligente et encore moins, décrire la gravité du problème. L'ennui n'est pas seulement le manque d'information, puisqu'elles sont incapables d'évaluer le risque même en possession d'informations suffisantes. Les humains ont tendance à surestimer le risque des évènements qui sont hors de leur contrôle et ceux qui sont amplifiés par les médias (attaques terroristes, les pirates informatiques, les accidents d'avion) et sous-estiment le risque pour les choses ordinaires, comme la perte, le vol ou l'erreur humaine. Cette incapacité vient de l'incompréhension des probabilités, et la sécurité est avant tout la compréhension et la réponse face au risque, donc face à la probabilité.

Plusieurs pourraient croire que la sécurité informatique est seulement une affaire de protection contre les menaces externes, surtout en ce qui a trait au vol de données. Mais, ce sont généralement des employés qui occupent des positions stratégiques qui sont les auteurs de ce type de crime. En français, nous les appelons généralement des taupes. Alors pourquoi aussi peu de taupes se retrouvent en prison ? La réalité est que les entreprises préfèrent congédier un employé fraudeur que le poursuivre en justice et s'exposer ainsi à une mauvaise publicité et à une perte de confiance de ses clients. Afin de réduire ces types de crimes, cette composante « humaine » du programme de sécurité s'avère être essentielle.

Les principales sous-composantes de la gestion du personnel se résument en trois catégories : la définition des postes, l'attribution des responsabilités et des rôles et la sensibilisation du personnel. En effet, avant même de mettre sur pied une méthode de sélection et de détermination appropriée des compétences du personnel, l'entreprise doit procéder à la qualification des postes et la détermination de leur niveau de sensibilité, ainsi qu'à la répartition des tâches de manière à ce qu'aucune personne ne puisse avoir le contrôle absolu de tous les aspects d'un processus informatique essentiel. Le respect de cette sous-composante réduit les risques d'infraction reliés aux enregistrements, aux matériels et aux biens de nature délicate et diminue la probabilité d'émergence d'incidents en matière de sécurité. Analysons plus amplement ces mesures préconisées pour réduire les méfaits causés par le personnel.

1.1. La définition du poste et la détermination de son niveau sensibilité suscité par le type de documents accédés

C'est seulement en ayant connaissance des fonctions et des niveaux d'accès qu'un type de poste requiert que l'on peut qualifier son niveau de sensibilité. L'entreprise devra identifier correctement la sensibilité du poste afin que des mesures de sécurité adéquates soient mises en place. La détermination du niveau optimal de sécurité est basée sur des facteurs tels le type et le degré de dommage (publication des renseignements personnels, fraude) qu'un individu peut provoquer par l'usage illicite des ressources informatiques. L'identification adéquate du niveau de sensibilité du poste est décisive, puisque toute mesure de sécurité excessive est une perte de ressources pour l'entreprise et toute carence peut lui provoquer un dommage irrémédiable.

De plus, la définition adéquate des postes servira de guide lors de l'attribution des privilèges d'accès nécessaires dans le cours normal du poste, thème que nous étudierons dans le troisième chapitre portant sur la sécurité technique.

---

[120] Comme l'obtention d'informations auprès de ceux qui les utilisent en mettant en œuvre des procédés basés sur la tromperie ou le brouillage.

1.2. La responsabilisation et l'attribution de privilèges

Une fois que le poste a été défini, l'entreprise devra déterminer le type d'accès nécessaire pour occuper et effectuer sa fonction. Toutefois, il existe deux principes qui doivent être considérés lorsqu'un accès est alloué : la *séparation des responsabilités* et les *privilèges minimaux*.

Les systèmes d'information contenant des informations personnelles doivent être organisés de façon à garantir une sécurité adéquate et satisfaisante. La notion de responsabilité sous-entend la possibilité d'identifier avec certitude l'individu qui est responsable de telle ou telle action. La notion de responsabilité va au-delà des simples employés. Elle doit s'appliquer à tous ceux qui ont accès aux informations, ce qu'implique que l'entreprise doit non seulement mettre en place des règles de conduite pour le personnel de l'entreprise, mais aussi imposer des obligations contractuelles pour les sous-traitants pouvant accéder aux données personnelles et des sanctions légales (ou disciplinaires) contre ceux qui ne respectent pas ces règles.

Mais, cette responsabilisation ne peut être faite que dans la mesure où il existe des ordres clairs ayant abouti à la connaissance de chaque individu. Il est donc nécessaire de s'assurer d'un bon niveau de connaissance des employés eu égard à leurs responsabilités et à la façon dont ils peuvent tenus responsables en cas de divulgation intentionnelle ou négligente de renseignements personnels dans un cadre autre que ceux prévus par la politique et les procédures de sécurité. Aussi, faut-il rendre les cas de non-respect des clauses de confidentialité une raison suffisante pour appliquer les sanctions disciplinaires internes. La connaissance des sanctions et de leur sévérité met l'accent sur l'importance de la sécurité des informations. Toutefois, tout comme les sanctions imposées par le droit, les sanctions internes doivent toujours être proportionnelles aux infractions. Toute action contraire pourra avoir des conséquences juridiques pour l'entreprise.

À ce propos, il est recommandé préparer une charte ou un guide expliquant aux employés leurs obligations et les conséquences de leurs actions dans ce domaine. Ce guide devra obligatoirement être porté à la connaissance des nouveaux employés. Sur ce point, la C.N.I.L. s'inquiète de la réalité suivante :

> «[…] de telles "chartes", au statut juridique mal défini, peuvent manquer à l'objectif qu'elles s'assignent lorsque, sans souci de pédagogie, elles cumulent les prohibitions de toutes sortes y compris celles des usages généralement et socialement admis de la messagerie et de l'Internet à des fins privées. En outre, dans certains cas, elles permettent mal de distinguer entre ce qui relève des obligations auxquelles est légalement tenu l'employeur de ce qui relève de la négociation collective ou encore du domaine de la discipline. […]
>
> Cette manière de procéder réalise à coup sûr l'obligation d'information préalable. Mais en se dispensant de la consultation du comité d'entreprise ou des délégués du personnel, elle peut méconnaître les dispositions du Code de travail. »[121]

[121] Rapport présenté par Hubert BOUCHET, « Cybersurveillance sur les lieux de travail», Commission Nationale de l'Informatique et des Libertés, 5 février 2002 en ligne : <www.cnil.fr/thematic/docs/entrep/cybersurveillance2.pdf >.

En plus des chartes, l'entreprise pourra aussi utiliser par exemple, des énoncés portant sur la nature délicate de sécurité ainsi que sur les exigences de disponibilité et intégrité qui s'appliquent notamment, sous la forme d'affichage à l'écran lors du démarrage des applications ou des systèmes ou par des mises en garde aux divers points d'accès physique.

Ensuite, la responsabilité de chacun en matière de sécurité des informations dépend de son rôle. Dans la mesure du possible, l'entreprise doit répartir les tâches de sorte que personne ne soit entièrement responsable d'opérations informatiques essentielles et connexes. Ainsi, les employés ne devront détenir qu'une seule responsabilité à n'importe quel moment. Par exemple, la programmation, l'administration, les essais et la production des systèmes doivent relever de personnes différentes. Afin de réduire le risque d'erreur dans le traitement des renseignements personnels, l'organisation doit veiller à ce que personne ne soit responsable de toutes les étapes d'un processus comme, l'entrée, le traitement ou la destruction de documents. Il est vrai que ce type de contrôle peut s'avérer très lourd pour une petite entreprise. Mais, toutes les mesures de sécurité qui sont proposées dans ce mémoire ne servent que de guide. Chaque entreprise qui s'en inspire, doit nécessairement les adapter à leurs besoins et au niveau de risque qu'elle encourt.

Toutefois, en procédant à cette division, nous devons garder à l'esprit la diversité des interactions[122] avec les informations à caractère personnel. Il existe premièrement des détenteurs d'informations, à qui on a donné la responsabilité de détecter la valeur et les niveaux de sécurité appropriés pour les informations qui sont sous leur contrôle. Ensuite viennent les gardiens des informations, soit ceux qui sont responsables de la gestion des systèmes sur lesquels sont conservées les informations. Ils doivent aussi le maintien de l'intégrité et de la confidentialité des informations tant que celles-ci sont sous leur contrôle. À cet égard, il serait préférable que l'entreprise nomme une personne responsable de vérifier que l'entreprise a bien effectué les notifications obligatoires à la Commission d'accès à l'information concernant la formation de fichiers de renseignements personnels sur ses employés et ses clients. Finalement, les utilisateurs d'information, les consommateurs des informations, auront enfin la responsabilité de les manipuler comme il convient les renseignements personne, et ce, dans la limite de leurs privilèges.

La principale justification de la responsabilisation est la capacité de preuve devant les autorités légales de toutes les activités effectuées par un individu en cas d'incident de sécurité ou d'attaque. Ainsi, la surveillance et l'enregistrement de l'utilisation des ressources permettent de déterminer la responsabilité de toute personne qui y a accès. Tout ce qui affecte la confidentialité, l'exactitude et la disponibilité des informations doit pouvoir être justifié *a posteriori*.

La meilleure façon de contrôle la responsabilité de chacun passe par le respect du principe des privilèges minimaux, aussi appelé le principe du besoin de connaître. Selon cette règle, l'entreprise devra limiter l'accès aux données de nature délicate aux seuls employés qui ont besoin d'en prendre connaissance. Les utilisateurs ne doivent avoir accès qu'aux dossiers contenant des renseignements personnels nécessaires à l'exercice de leurs fonctions.

> « The concept of limiting access, or "least privilege," is simply to provide no more authorizations than necessary to perform required

[122] EDIFICAS & IALTA, «Guide de l'archivage électronique sécurisé – Recommandations pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations», Version V, 12 juillet 2000, p. 10, en ligne : <www.edificas.org/ftp/Archivage/GuidArcv.PDF >.

> functions. […] Its goal is to reduce risk by limiting the number of people with access to critical system security controls […]. Best practice suggests it is better to have several administrators with limited access to security resources rather than one person with "super user" permissions. »[123]

L'entreprise doit donc définir pour chacun des utilisateurs un « profil d'accès » qui déterminera ce à quoi il a accès, ainsi que le mode d'accès. Habituellement, le gestionnaire du système informatique peut restreindre l'accès aux données aux personnes autorisées et préciser les privilèges ou la combinaison de privilèges accordés : lecture, modification, destruction ou modification.

De plus, les privilèges d'accès doivent être autorisés et contrôlés selon le rôle de l'intervenant: usagers, préposés aux opérations, au soutien et à l'entretien, préposés à l'analyse et à la programmation des systèmes. Comme mesure de protection pour l'entreprise, il faudra veiller à ce qu'avant d'accorder l'accès, chaque personne concernée signe une entente datée, avec témoin, pour attester qu'elle a lu et accepte une version précise et datée des règlements internes applicables. Cette entente devrait être conservée et prévaloir au moins pendant un an après la cessation d'emploi. De plus, l'entreprise doit avoir des profils d'accès différents pour ses employés, selon que les fichiers de renseignements sont utilisés ou non. Dans le cas des fichiers inactifs, il incombe à l'archiviste ou à une personne désignée qui remplit ce rôle, d'avoir accès à ces dossiers, et de les rendre actifs au besoin. Dans le cas du personnel de l'aide technique, ils ne doivent pas avoir accès aux données nominatives réelles que dans la mesure où celles-ci sont dénominalisées. Ainsi, chaque entreprise doit se doter de politiques et procédures administratives qui permettent de contrôler l'attribution des profils d'accès à leur personnel.

Les privilèges d'accès doivent être autorisés et contrôlés pour tous les usagers, pas seulement pour les employés, mais aussi pour les préposés aux opérations, au soutien et à l'entretien, préposés à l'analyse et à la programmation des systèmes et tous les ordinateurs. Ces privilèges doivent être attribués selon le principe du moindre privilège, soit le principe selon lequel une entité doit démontrer préalablement qu'elle a besoin de cette autorisation pour effectuer les tâches qui lui sont assignées et seulement pour le temps nécessaire. L'entreprise respecte ainsi la philosophie du moindre risque : moins il y a de privilèges, moins il y a de risques[124]. Sans une bonne planification, les droits d'accès peuvent interférer avec les plans de contingence et de reprise des activités. Certains systèmes d'information disposent de comptes d'administration tout puissants, sans limites d'accès et privilèges illimités. Ceci constitue un danger puisqu'une simple erreur peut avoir de répercussions importantes, sans parler de l'intérêt que ces comptes représentent pour les attaquants. De plus, il va contre le principe de la responsabilisation puisque plusieurs administrateurs pourront utiliser le même compte. Dans les comptes individuels, il est plus facile de garder la trace des processus d'administration et de remonter jusqu'à celui qui a accompli la tâche.

1.3 Processus d'emploi : de la sélection du personnel à la cessation d'emploi

1.3.1. La sélection du personnel interne

---

[123] Gary STONEBURNER, Clark HEYDAN, Alexis FERINGA, Engineering Principles for Information Technology Security, N.I.S.T., S.P. 800-27, juin 2001, p. 16.
[124] Donald PIPKIN, Sécurité des Systèmes d'Information, Paris, Campus Press, 2000, p. 152.

Une fois que l'entreprise a défini le niveau de sensibilité d'un poste, elle peut procéder à l'affectation du personnel. Mais la sélection du personnel ayant accès aux données nominatives doit se faire avec un grand discernement. Sur ce point, le *National Institute of Standards and Technology* conseille, pour les employés qui auront accès à des données très sensibles (crédit, médical, etc.), propose d'effectuer un filtrage, en d'autres mots, s'assurer que la personne est adéquate pour le travail[125].

De plus, conformément à ce qui est suggéré par la Gendarmerie Royale du Canada[126], l'entreprise doit vérifier si la personne choisie pour un poste a le niveau d'habilitation nécessaire selon la cote de sécurité essentielle pour les renseignements personnels auxquels elle aura accès dans le cours normal de ses fonctions. Ainsi, tous les employés qui utilisent, gèrent, entretiennent ou développent le système d'information ou qui par un moyen quelconque affectent la sécurité doivent avoir la compétence nécessaire pour accomplir leurs tâches de manière adéquate. Cette compétence doit être maintenue et développée par un système de formation et de sensibilisation avant l'embauche.

Certaines compagnies peuvent faire une enquête sur un futur employé ou alors lui donne un poste avec moins de responsabilité et moins d'accès à des renseignements sensibles à un nouvel employé. Ceci peut également s'appliquer aux travaux exécutés par les employés temporaires de l'entreprise. L'enquête est le processus qui confirme si les détails fournis par un postulant à un poste de travail disponible sont complets et véritables. Toutefois, cette vérification ne doit pas aller au-delà des informations librement données par la personne dans le curriculum vitae, le formulaire d'application ou les références données par les employeurs antérieurs. Le processus de vérification peut aussi inclure la confirmation des aptitudes et des informations financières si et seulement si, ces informations sont nécessaires à l'accomplissement des tâches dans le cours normal de ces fonctions.

Toutefois, l'employeur devra expliquer aussitôt que possible dans le processus de recrutement la nature de la vérification effectuée et les méthodes selon lesquelles celle-ci sera produite. Le processus de vérification devra être ouvert et transparent et les candidats devront être informés sur quelles informations seront vérifiées et comment.

> « Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités. »[127]

Dans tous les cas, pour respecter les principes juridiques en matière de collecte de renseignements personnels, il est essentiel d'obtenir un consentement du possible futur employé dans la mesure où ce consentement n'a pas été donné par d'autres moyens. De plus, il faut donner la possibilité à l'intéressé de s'exprimer sur les informations dans le cas où celles-ci lui sont défavorables ou qu'elles s'avèrent fausses.

---

[125] National Institute of Standards and Technology, An Introduction to Computer Security: The N.I.S.T. Handbook, Special Publication 800-12, octobre 1995, p.110.
[126] G.R.C., Normes de sécurité technique dans le domaine de la technologie de l'information (N.S.T.T.I.), Ottawa, Gendarmerie royale du Canada, août 1997, p. 19, par. 3.1. en ligne : <http://www.rcmpgrc.gc.ca/tsb/pubs/standards/tssit97_f.pdf>.
[127] Nouvelles lignes directrices sur la sécurité de l'O.C.D.E., précitée, note 46, principe 12.

Lorsque la sélection est effectuée, le nouvel employé devra alors signer la politique de sécurité et une clause de respect de la confidentialité (cette règle vaut pour toute personne extérieure qui a accès à ce type de données). Plus important, le contrat de travail devra prévoir des mesures disciplinaires (pouvant aller jusqu'au congédiement) pour toute contravention à l'intégrité des renseignements personnels ou à leur divulgation. En portant à la connaissance de l'employé ces mesures disciplinaires, l'employeur obtient dès lors un « motif sérieux »[128] pour le congédiement en cas de non-respect des obligations de l'employé. Ainsi, l'employeur pourra considérer comme motif sérieux de congédiement l'insubordination du salarié, son manquement à l'obligation de loyauté et de discrétion ou encore à son obligation de diligence[129]. De manière générale, l'employé doit respecter certaines obligations déjà imposées par la loi.

> « Le salarié doit accomplir ses tâches de façon diligente, c'est-à-dire avec intérêt, de façon ordonnée, productive et appliquée. […] Son devoir de prudence lui impose certaines normes de conduite dans l'accomplissement de ses tâches. Ainsi, le salarié doit éviter de poser des gestes de négligence, d'insouciance et d'imprudence. Cette obligation impose une conduite prudente non seulement à l'égard des biens matériels de l'employeur, mais également des personnes que le salarié doit côtoyer dans son milieu de travail. »[130]

Aussi, avant la prise des fonctions, tout nouvel usager du système doit recevoir des directives spécifiques sur les actions qu'il peut, et plus spécifiquement, celles qu'il ne peut pas faire en relation avec les données personnelles. Ces directives, qui sont un résumé de la politique de sécurité, devront être distribuées, par écrit de préférence, par papier puisqu'elles doivent être signées par le nouvel employé. Comme toujours, ces documents pourront servir de preuve en cas d'action en justice et réfuteront les défenses de non-connaissance des obligations.

En cas de mutation d'un employé, lors d'une nomination, une affectation, un déploiement ou un détachement, l'entreprise doit avoir à sa disposition des procédures écrites à suivre afin que les privilèges d'accès aux systèmes, aux renseignements ou aux biens soient modifiés ou annulés en conséquence. De même, lorsqu'un employé-clé quitte l'emploi, il faudra s'assurer que la confidentialité des renseignements auxquels il avait accès ou les mesures de sécurité connues sont protégées. À ce propos, il peut s'avérer intéressant d'avoir un entretien avec l'employé pour lui rappeler ses responsabilités permanentes en matière de confidentialité des renseignements sensibles et dès son départ considérer les points cruciaux en matière de sécurité. L'une des premières mesures à prendre est de retirer immédiatement à l'employé ses privilèges d'accès. Dès ce moment, l'identification et le mot de passe de l'utilisateur doivent être effacés ou modifiés et tous les insignes d'identification et clés doivent être reprises. Il importe également de s'assurer de fournir tous les renseignements nécessaires permettant à l'administrateur de réseau local ou à la personne responsable du contrôle d'accès au système d'annuler le compte d'utilisateur. De plus, il faudra procéder à l'archivage ou au transfert des

---

[128] Art. 2094 C.c.Q.
[129] art. 2088 C.c.Q.
[130] Robert BONHOMME et Laurent LESAGE, « Le contrat de travail », Montréal, 2001, en ligne : avocat.qc.ca < http://www.avocat.qc.ca/affaires/iicontravail.htm >. (Dernière mise à jour: 15 février 2001)

dossiers à un successeur, retourner tout le matériel, logiciels et documentation en sa possession.[131]

Afin d'éviter le plus possible des incidents malicieux et les départs « à risque », une évaluation périodique du travail des employés représente une excellente possibilité pour l'entreprise de procéder à un dépistage comportemental des altérations qui pourraient influencer leur relation avec l'entreprise et la sécurité, comme les modifications de mode de vie, situation financière, etc. Cette pratique peut se montrer avantageuse pour les employés ayant des responsabilités accrues en matière de renseignements personnels et de la sécurité au sein de l'entreprise.

1.3.2. Mesures de sécurité pour le « out-sourcing » ou les employés externes

Les développements récents dans les technologies informatiques ont fait en sorte que les entreprises qui exercent des activités diverses et complexes, engageant des renseignements personnels, font appel aux services d'entreprises spécialisées dans la gestion informationnelle, et ce, afin d'offrir un meilleur service à leurs clients et d'améliorer le rendement de l'organisation.

Bien que la mise en place d'une telle politique de vérification soit compliquée, il demeure vital de contrôler l'accès de certaines personnes qui ne travaillent pas pour l'entreprise, mais qui par divers contrats doivent faire des travaux liés à l'exploitation des ordinateurs. Dans la majorité des cas, il s'agit du personnel de compagnies spécialisées dans l'offre de services informatiques, comme la configuration des réseaux, l'entretien de logiciels ou encore, des compagnies d'entretien des appareils de climatisation, des téléphones ou de nettoyage. Plusieurs entreprises dans les domaines de pointe obligent ces employés externes, de même les visiteurs à souscrire à une politique de confidentialité et de protocole d'accès[132].

Sur ce point, l'entreprise devra porter une attention particulière dans la rédaction des contacts signés avec des organismes externes et préciser les exigences de sécurité applicables au matériel, aux services et surtout à l'accès aux renseignements informatiques de nature délicate. Ces organismes externes doivent, conformément à l'entente contractuelle, mettre leurs employés au courant de leurs obligations notamment, assurer la disponibilité et la sécurité des données en cas de conflit de travail. L'entente doit clairement indiquer la nature des données traitées et l'exigence de tous les auteurs impliqués. L'entreprise est responsable de la sécurité et de la confidentialité des données traitées pour son compte en exécution du contrat. Elle doit veiller à ce que son prestataire prenne les mesures nécessaires à cet effet, particulièrement par des clauses contractuelles appropriées.

À cet égard, la Directive 95/46/CE aux articles 16 et 17, précise les obligations incombant aux prestataires traitant des données pour le compte de l'entreprise responsable du traitement. Ceci veut dire que, dans le cas où l'entreprise fait appel aux services d'un tiers concernant les renseignements personnels, elle doit s'assurer de choisir un tiers qui pourra manipuler les informations avec un niveau suffisant de protection et ce dernier doit garantir, par la voie contractuelle ou autre mesure légale, que les instructions aux employés sont connues et appliquées, que la confidentialité des données personnelles est maintenue, que la transmission

---

[131] Charles MILLER, Manuel de la sécurité de la technologie de l'information, Services gouvernementaux, Ottawa, 1993, p. 18.

[132] Charles MILLER, La sécurité des micro-ordinateurs et des réseaux locaux, Service de gestion de l'information des SGC et la Direction de la sécurité industrielle et ministérielle des SGC, Ottawa, Services gouvernementaux Canada, 1993.

des données aux d'autres parties est strictement interdite, que la responsabilité en cas d'incident ou faute est clairement définie. La directive ajoute également, au paragraphe 4 de l'article 17, que l'entreprise devra conserver le contrat, de forme écrite ou enregistrée sur un support technologique durant toute la période que les données personnelles sont gérées par une entreprise tierce.

1.4. Le programme de sensibilisation du personnel

Puisque les mesures préventives diminuent la liberté d'usage des utilisateurs, leur efficacité varie en fonction de leur acceptation par les divers usagers des systèmes de l'information. À ce propos, un programme de sensibilisation adéquat augmente considérablement le niveau de tolérance face à ce type de contrôles dans la mesure où les utilisateurs sont informés des avantages de telles restrictions.

La référence légale à l'état de l'art[133], dans notre cas la technique de sécurité, oblige les entreprises à s'informer des diverses techniques de sécurité présentes sur le marché. Selon le premier principe des lignes directrices de l'O.C.D.E. sur la sécurité des réseaux[134], tous les intervenants doivent être sensibilisés au besoin d'assurer la sécurité des systèmes et des réseaux d'information ainsi qu'aux actions qu'ils peuvent entreprendre pour renforcer la sécurité. C'est l'occasion idéale pour réfléchir à la configuration du système, aux mises à jour disponibles pour les divers logiciels de protection du système et à la place qu'ils occupent dans le réseau. À ce moment, l'entreprise pourra aussi ajuster ses bonnes pratiques (« good practices »), renforçant ainsi la sécurité et la qualité des relations avec les partenaires commerciaux.

Les termes « formation », « sensibilisation » et « éducation » sont fréquemment utilisés comme synonymes dans les divers ouvrages portant sur la sécurité informationnelle. Toutefois, s'il est vrai que ces concepts font tous partie d'un programme efficace de sensibilisation, chacun a un objectif et un impact distinctif. Ces différences sont présentées dans le tableau suivant, tiré du N.I.S.T. Handbook[135] :

	Sensibilisation	**Formation**	**Éducation**
Attribut :	« Quoi? »	« Comment? »	« Pourquoi? »
Niveau :	Information	Connaissance	Perspective
Objectif :	Identification	Talent	Compréhension
Méthode d'apprentissage :	Média	Pratique	Théorique
Évaluation :	Choix Multiple	Cas pratiques	Réponses à développement
Impact:	Court terme	Intermédiaire	Long terme

Figure: Tableau comparatif pour la sensibilisation, formation et éducation des utilisateurs en contact avec les systèmes d'information

La sensibilisation est la pédagogie donnée aux utilisateurs d'un système d'information afin de leur faire comprendre l'importance des mesures de sécurité. Cette diffusion ou prise de conscience aux bienfaits de la sécurité est un processus clé dans la mise en place de la sécurité de l'entreprise, puisque avant d'appliquer correctement toute politique de sécurité, les

[133] Directive 95/46/CE, précitée, note 16, art. 17.
[134] Nouvelles lignes directrices sur la sécurité de l'O.C.D.E., précitée, note 46.
[135] National Institute of Standards and Technology, précitée, note 125, p. 147.

utilisateurs, surtout les employés non spécialisés, doivent bien comprendre l'implication de la sécurité dans l'exécution de leurs tâches quotidiennes. Bien souvent, ceux-ci ne comprennent pas leur rôle dans la préservation de la sécurité des informations qu'ils manipulent : la sécurité est chose des informaticiens, oubliant que ce sont eux qui jouent souvent le rôle essentiel dans la prévention et la signalisation des incidents. Donc, tout programme de divulgation et d'instruction sur le pourquoi de la sécurité et principalement sur la valeur de celle-ci, augmente sérieusement la qualité de la sécurité. Notons que le plan de sensibilisation doit être inclus dans la politique de sécurité, document clé, que nous avons abordé dans le chapitre 3 de la première partie du mémoire.

La politique de sensibilisation doit aborder divers thèmes comme, à quoi servent les systèmes d'information, pourquoi la sécurité est importante, comment utiliser les moyens de sécurité existants, la définition des rôles de chacun, la responsabilité correspondante à ce rôle, la signalisation les manquements à la sécurité et enfin les conséquences d'un comportement anormal menant à l'imposition de sanctions.

À ce stade une question importante se pose : quand faut-il amorcer la campagne de sensibilisation ? Le *National Institute of Standards and Technology* soutien que:

> «[…] Employees must receive initial computer security training before they are granted any access to computer systems. Others argue that this must be a risk-based decision, perhaps granting only restricted access (or, perhaps, only access to their PC) until the required training is completed. Both approaches recognize that adequately trained employees are crucial to the effective functioning of computer systems and applications.»[136]

Tout comme en droit, le « je ne savais pas » ou le « je ne connaissais pas cette règle » ne doit pas constituer une excuse et la qualité de la divulgation fait sans aucun doute la différence en cas de litige. De tels avis sont commodément donnés lors de l'embauche de nouveaux employés, de l'affectation à de nouvelles fonctions et lors d'un changement dans les mesures de sécurité de l'entreprise. Mais, il est prudent de faire un « rappel » de ces mesures de sécurité de manière soutenue par l'utilisation de bannières d'avertissement aux points d'entrée. En gros, l'entreprise doit retenir quelques mots clés qui garantissent le succès de la sensibilisation : elle doit être faite en permanence, de façon globale et cohérente et surtout, avec rentabilité.

Les individus ont différents rôles au sein de l'entreprise et par conséquent, différentes responsabilités et devoirs. De ce fait, la sensibilisation doit se faire à des niveaux distincts. Le personnel doit recevoir une formation sur les principes de la sécurité, sur les dispositifs de sécurité et sur les faiblesses dans l'exercice de leurs fonctions. Par conséquence, elle doit être adaptée à chaque catégorie de personnel (coordonnateur, gestionnaire, utilisateurs). En faisant une pareille distinction, on permet ainsi une meilleure adéquation en donnant la formation au niveau de chaque individu en relation avec leur rapport quotidien avec l'information au sein de l'organisation. Ces différences demandent des procédures précises pour bien séparer les devoirs de chacun et impliquent l'organisation des séances d'information sur la sécurité à l'intention du personnel et entrepreneurs qui auront accès aux systèmes (privilèges, cotes de sécurité, responsabilités, articles et lois applicables, règles de sécurité internes applicables), de

[136] Idem, p. 111.

séances données en personne avec document écrit indiquant la date et le contenu de la séance. L'employé doit signer ce document à titre de preuve qu'il a pris connaissance des consignes à suivre et accepte de les respecter.[137] Il faut également s'assurer de la formation pertinente des employés jouissant de privilèges d'accès spéciaux et surveiller les activités de ceux-ci afin de maintenir un niveau de sécurité acceptable durant les périodes où ces personnes ont accès aux systèmes.

La sécurité, l'information, la technologie et aussi les utilisateurs sont de notions dynamiques, qui changent avec le temps. Il sera nécessaire pour l'entreprise de déterminer des moyens pour évaluer l'efficacité du processus de sensibilisation. Ainsi, les entreprises peuvent s'assurer que le personnel est au courant de ses responsabilités en matière de sécurité, des normes de sécurité applicables et, si nécessaire, de la façon de faire pour réajuster la formation.

Le défaut de sensibilisation peut se traduire en une variété de pertes pour l'entreprise. Les mesures de sécurité impliquent inévitablement un changement comportemental de tous les utilisateurs des systèmes informatiques et un investissement d'efforts et de temps de la part de tous. Par exemple, il faut se souvenir des mots de passe, se soumettre à des contrôles d'accès, ne rien laisser traîner sur les bureaux, etc. Si les usagers des systèmes informatiques ne sont pas conscientisés aux implications des dispositifs de sécurité, ils ne se rendront à la longue pas compte des conséquences de leurs actes. De plus, le manque d'instruction sur la façon de dénoncer un comportement anormal ou simplement un incident de sécurité peut facilement faire en sorte que toute menace ou vulnérabilité passera inaperçue, et ce, même si tout le monde est au courant de la politique de sécurité en vigueur.

La collaboration entre les responsables de la sécurité, les gestionnaires et le personnel des ressources humaines, est vitale dans l'information du personnel sur les éléments pouvant influer leurs fonctions et leur milieu de travail (dispositifs de sécurité et leurs faiblesses, dernières nouvelles, infractions et préoccupations sur la sécurité et procédures de compte rendu).

La sensibilisation est donc une formation, qui à long terme, deviendra l'éducation adéquate des divers acteurs qui dans leur quotidien entrent en contact avec des données à caractère personnel.

Section 2. Mesures concernant l'administration des documents et du matériel informatique contenant des données à caractère personnel

Dans la dernière section nous avons étudié les mesures organisationnelles devant être appliquées au personnel de l'entreprise. Dans cette deuxième section, nous nous attarderons sur l'étude des mesures de gestion et d'administration applicables au matériel informatique et aux documents contenant des renseignements à caractère personnel. De manière plus concrète, ces mesures se traduisent par l'élaboration d'un guide de classification et de désignation du matériel informatique et des documents contenant des données personnelles qui doivent être protégées, par la rédaction des directives concernant la destruction des supports informatiques qui les hébergent et aussi, la mise en place d'une directive touchant les copies de sauvegarde. Finalement, la sécurité n'étant pas absolue, la nécessité d'avoir un plan de

[137] N.I.S.T., précitée, note 125, p. 113.

réponse fonctionnel face aux incidents de sécurité s'avère une mesure de protection vitale pour l'entreprise.

2.1 Le guide de classification et de désignation

Selon les principes juridiques fondamentaux[138] applicables aux données conservées par une entreprise, la collecte de données à caractère personnel doit être faite en fonction de la finalité et l'entreprise doit en tout temps assurer la qualité des données gardées. Ceci implique qu'elle examine les informations détenues et détruise celles qui ne lui sont plus nécessaires.

Et afin de bien gérer les données conservées, l'entreprise devra procéder à la classification compte tenu de leurs caractéristiques et de leur sensibilité, dans le but d'appliquer les mesures de sécurité imposées par les divers textes de loi. Pour ce faire, l'entreprise devra élaborer un guide de classification et de désignation qui explique la marche à suivre pour la classification, la déclassification des renseignements à caractère personnel et des biens informatiques contenant ces derniers. Ce guide devra renfermer des instructions sur tous les types de renseignements traités dans le milieu informatique et comme toutes les mesures de sécurité, il devra être revu de façon périodique afin de tenir en compte des changements récents au niveau de la sécurité et des besoins de l'entreprise.

En principe, ceci aidera l'entreprise à donner une description du contenu des informations, la spécification de la finalité pour laquelle les renseignements sont conservés (fichiers de clients ou de patients, par exemple), la description de son emplacement dans le système informatique. Par ces mesures, l'organisation sera en mesure d'avoir un contrôle adéquat sur les renseignements personnels.

La classification des données doit se faire selon les critères suivants[139] : la valeur intrinsèque ou la nature des données (confidentiel et utilisation), le mode d'exploitation (support et moyen de traitement), la valeur temporelle ou son cycle de conservation et la dynamique des données (rôle actif ou passif). La sensibilité de l'information est le principal facteur de détermination du niveau de sécurité. Pour assurer la sécurité en fonction de leur importance l'entreprise devra clarifier et distinguer les données clés et leur assigner une valeur ou un degré de sécurité. Afin de déterminer la valeur de l'information (et le coût des moyens pour la protéger), l'entreprise devra définir l'impact financier et légal d'une perte de l'information. Ses obligations légales, contractuelles et sanctions possibles déterminent le niveau minimal de sécurité requis pour l'information à laquelle s'applique la loi ou le contrat.

Nous avons vu que les législations nationales et les textes internationaux ne se prononcent pas sur les mesures de sécurité à mettre en place pour se conformer aux obligations légales. Ainsi, l'entreprise pourra se baser sur les standards et les règles générales définies par l'industrie[140]. Elle devra déterminer l'interdépendance entre les données importantes et leur accorder une protection similaire. Le paramètre de durée de vie des informations affecte grandement la classification des données puisque leur importance varie en

---

[138] Voir, supra, Partie 1, Chapitre 2, Section 2.1.
[139] Pierre GRATTON, La gestion de la sécurité informatique, Boucherville, Vermette, 1998, p. 167.
[140] Voir entre autres la norme ISSO 17799, A Code of Practice for Information Security Management (British Standard 7799), National Communications System, Public Switched Network Security Assessment Guidelines, Septembre 2000.

fonction du temps. Plus l'information est rapidement détruite ou tombe en désuétude, plus bas sera son niveau de classification et de protection.

Quant à la classification du matériel, il faudra structurer la sécurité selon la nature des articles à protéger, du volume des données en cause, du niveau hiérarchique des utilisateurs et de leur nombre ainsi que la valeur monétaire ou du contenu des données. Mais, que ce soit pour les données ou pour le matériel, la classification de sécurité résulte de la combinaison des classifications de disponibilité, d'intégrité et de confidentialité de chaque donnée.

2.2. Les directives concernant la destruction des données personnelles et du matériel informatique

L'un des grands défauts des programmes de sécurité est le manque de politiques et de procédures touchant la conservation et la destruction de l'information personnelle. Il faut veiller à ce que les enregistrements classifiés ou périmés soient détruits sans que leur contenu puisse être récupéré. Par exemple, dans le cas des supports informatiques, « la seule suppression ou ne reformatage n'efface pas les données et elles peuvent être récupérées facilement à l'aide d'outils d'utilisation courante. »[141] Sur ce point, il existe des méthodes spécifiques approuvées par le Gouvernement du Canada[142].

L'accès à la fonction de destruction des renseignements personnel doit être limité à quelques intervenants et à des conditions très précises afin que celles-ci soient faites de façon à ce que leur caractère confidentiel soit protégé. Ainsi, lorsque l'entreprise envisage la destruction de certaines données ou même de certains programmes contenant des renseignements personnels, elle devrait procéder de façon méthodologique et enregistrer tout le processus, évitant ainsi la destruction accidentelle d'information. Des directives sur ce sujet devraient au moins aborder les questions de la procédure de destruction (étiquetage sur le matériel devant être détruit ou séparation des données devant être détruites des autres informations) la description des outils techniques et la description des responsabilités et des rôles.

Ainsi, dans le cas où l'entreprise déciderait de se défaire du matériel physique, elle devra décider s'il est nécessaire de détruire complètement le matériel contenant des renseignements personnels afin de préserver la confidentialité des informations sensibles, notamment par un processus de démagnétisation et oblitération les données de façon à ce qu'elles ne soient plus accessibles.

De plus, en ce qui concerne la destruction de documents, l'article 17 de la Loi concernant le cadre juridique des technologies de l'information prévoit expressément une obligation de documenter la destruction. En effet, cet article précise que :

> « pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur juridique, le transfert doit être documenté de sorte qu'il puisse être

[141] Charles MILLER, Manuel de la sécurité de la technologie de l'information, Services Gouvernementaux, Ottawa, 1993, p. 21.
[142] Voir notamment, GOUVERNEMENT DU CANADA, Démagnétiseurs approuvés par le CST pour l'effacement de supports magnétiques, (CTIB 7/96) et GOUVERNEMENT DU Canada, Guidelines for Clearing and Declassifying Automatic Data Processing Storage Devices, (CTIB 19/87).

> démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée. »[143]

2.3. La politique de sauvegarde (back-up)

L'entreprise doit avoir des politiques de sauvegarde pour le matériel, pour les données et pour le personnel. Les renseignements informatisés jugés essentiels à la poursuite des activités normales de l'entreprise doivent faire l'objet de sauvegardes régulières. Un « back-up » des données est une copie des données utilisables par l'ordinateur, copie que l'on garde afin de pouvoir récupérer les données en cas de perte des données originales. Ces copies sont préférablement gardées dans des locaux distancés pour éviter la double destruction. L'idéal serait de garder une copie de toutes les données contenues dans le système. Mais pour une raison de coûts, il faut faire la sélection des données les plus importantes. Une variété de facteurs influence la fréquence de sauvegarde, et, l'étendue ainsi que le nombre de générations de sauvegarde. La fréquence dépend en premier lieu du type de matériel utilisé : certains supports sont plus rapides que d'autres. La capacité de sauvegarde varie grandement d'un support à l'autre et limite grandement la quantité de copies de sauvegardes d'une entreprise. Ensuite, le niveau de risque encouru et le risque pouvant être amorti par l'entreprise influence la quantité de données à sauvegarder. Certaines compagnies peuvent se permettre de perdre les données d'une journée de travail, alors que pour d'autre ce type de perte pourrait s'avérer fatal.

À la lumière de ces éléments et afin de faciliter la gestion des renseignements personnels détenus par l'entreprise, celle-ci devrait éliminer la collection de données à caractère personnel qui s'avère inutile ou excessive pour le but initialement donné. En effet, nous avons vu que les informations ne doivent être conservées que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées[144]. Au-delà de cette période, elles ne peuvent être conservées. Après, un tri est donc opéré en accord avec l'administration des archives, qui, à des fins historiques, statistiques ou scientifiques, peut en conserver certaines sous réserve d'avoir été anonymisées. Il faudra procéder à l'examen de chaque type de donnée conservée (clients, employés,…) et déterminer si l'information peut être effacée ou s'il importe de modifier les critères de collecte. Ceci permettra à l'entreprise, non seulement de vérifier que la collecte et le traitement des données personnelles respectent les divers principes imposés par les lois applicables au sujet, mais aussi facilite l'identification des données essentielles et qui réclament une copie de sauvegarde.

Si les renseignements sont enregistrés sur des supports amovibles comme les disquettes, les bandes, CD-ROM ou disques dures portables, ils doivent être protégés, en dehors des heures d'utilisation, en les plaçant dans la bibliothèque de soutien dûment sécurisée. Les renseignements très sensibles, comme les dossiers médicaux par exemple, devraient préférablement être emmagasinés sous une forme chiffrée, soit les rendre illisibles sans l'utilisation d'une clé de décodage. Cette obligation peut être annulée si l'évaluation des risques établit clairement que d'autres mesures de protection peuvent être suffisantes.

En conclusion, des procédures doivent être élaborées afin d'assurer la la confidentialité, la disponibilité et l'intégrité des sauvegardes. Elles visent essentiellement, la vérification de la réussite de la sauvegarde et la possibilité de récupération des données, l'essai périodique des

---

[143] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37, art. 17.
[144] Voir Partie 1, Chapitre 2, Section 2.1, p. 30.

données sauvegardées et de leur support ainsi que l'assurance qu'une copie de la sauvegarde est envoyée hors de bureaux pour éviter la double destruction.

2.4. La réaction aux incidents et le plan de reprise des opérations

Un programme de sécurité, même s'il est bien mis en place, ne protégera pas l'entreprise contre la totalité des incidents de sécurité. Ainsi, lorsque survient un incident, la réaction des responsables de l'entreprise est déterminée par un ensemble de règles dans lesquelles interviennent de façon prioritaire les pratiques et les objectifs définis dans la politique de sécurité. Un plan de reprise des opérations est l'ensemble des mesures prises au niveau du matériel, du logiciel, des données en général et du personnel pour permettre à l'entreprise, après un incident, de reprendre le plus rapidement possible un maximum d'activités. L'objectif est donc de dominer et de réparer le dommage causé par un incident et prévenir le dommage ultérieur.

Dans le cas de la protection des données confidentielles et personnelles, l'objectif déterminant sera alors d'assurer la disponibilité et l'intégrité des informations et leur protection en ce qui concerne leur existence et leur confidentialité. Un bon plan doit envisager un maximum de problèmes et apporter des solutions physiques, logiques et humaines et prévoir les réactions de chacun au cours de toutes les étapes de recouvrement. Sur ce point,

> « un plan de reprise après sinistre (en cas de sinistre, de panne, d'intrusion, etc.) des systèmes en activité doit être mis par écrit et éprouvé régulièrement au moyen d'exercices de récupération des informations. Ce plan doit préciser, entre autres, le seuil de tolérance à l'interruption de chaque actif ainsi que les processus de relocalisation et les façons de revenir à la normale ; il doit également consigner l'historique des événements. »[145]

Naturellement, le temps de réaction et le niveau de préparation de l'entreprise face aux incidents a un impact important quant à leurs conséquences. Et pour que la réponse soit efficace, il est vital que le plan ait été soigneusement préparé et testé : un plan non testé n'est que légèrement meilleur que pas de plan de tout. Théoriquement, le plan de réponse devrait être la procédure de sécurité la mieux définie et la plus complète possible, mais c'est rarement le cas. Pour chaque incident, l'entreprise doit parcourir les étapes de base suivantes[146] : sa documentation, sa détermination, sa notification, la limitation des dégâts, la suppression et la remise en état. Analysons brièvement chacune d'entre elles.

Il est plus difficile que l'on peut croire de savoir si l'on est en présence d'un incident de sécurité, d'où l'importance d'avoir un système de détection fonctionnant en permanence. En effet, seulement 40% des organisations se disent confiantes dans leur capacité de détecter une attaque[147]. Mais le plus important est sans doute savoir à qui un incident doit être notifié (direction, département juridique, police,…) et surtout à quel moment. Tous ces thèmes auront dû être planifiés et étudiés préalablement dans le programme de formation et de sensibilisation du personnel.

---

[145] GOUVERNEMENT DU QUÉBEC, Cadre global de gestion des actifs informationnels appartenant aux services du réseau de la santé et des services sociaux – volet sur la sécurité, Québec, septembre 2002, p. 26.
[146] D. PIPKIN, précitée, note 124, p. 262.
[147] ERNEST & YOUNG, «Global Information Security Survey 2002», Ernest & Young LLP, mars 2002, en ligne: Ernest & Young < http://www.eyindia.com/pdfs/Info%20Security%20Survey%202002.pdf>.

Pour que l'entreprise puisse analyser et étudier les mécanismes d'un incident, ce dernier doit être le plus documenté possible. Cette documentation de référence doit contenir les informations spécifiques pour un type d'incident afin de le rendre compréhensible pour ceux qui doivent être informés et qui auront en charge de tenter de réparer les dommages. Ce résumé technique de l'incident doit donner une description de la cause de l'épisode (qui, quoi, comment, quand et où?). Il doit aussi exposer son impact tant sur le matériel comme sur le logiciel et surtout les données qui ont été compromises. Cette documentation servira lors des futures séances de formation. D'ailleurs, selon le principe de réaction décrit dans les *Lignes directrices sur la sécurité*[148], les entreprises doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité. Ceci implique la conservation des traces écrites et enregistrées de manière détaillée après que l'incident ait été observé, et ce, tant pour des fins de poursuites judiciaires ou d'évaluation de la sécurité de l'entreprise.

L'entreprise doit avoir rédigé des procédures visant la diminution des dégâts et sa mise en œuvre doit être le plus rapide possible. Elle doit définir par écrit les niveaux de services essentiels et le temps d'arrêt maximal, classer les systèmes par ordre de priorité de rétablissement selon les besoins de continuité et de sauvegarde, tenir à jour des plans permettant la continuité et surtout, voir à ce que les plans de rétablissement ne compromettent pas la confidentialité ou l'intégrité des données. Il est conseillé de conserver des copies actualisées des plans d'urgence, procédures et des sauvegardes en 2 endroits différents.

Lorsqu'un incident survient, apparaît aussi l'occasion d'apporter les changements nécessaires aux mesures de sécurité en place dans le cas où celles-ci présenteraient des faiblesses, ainsi que réévaluer les objectifs initiaux de l'entreprise. Plus vite se fera cette remise en état, plus vite reprendrons les activités de l'entreprise. Cette réévaluation est l'un des principes déjà étudiés des nouvelles lignes directrices de l'O.C.D.E.[149] Elle permet à l'entreprise de tester et d'apprécier les objectifs, la stratégie et l'organisation de la sécurité au regard des objectifs énoncés dans la politique de sécurité. La réévaluation doit porter au moins sur les points suivants : les résultats des audits internes et les contrôles effectués par une autorité publique (ex. la C.A.I. au Québec); résultats des analyses de risques, rapports sur les changements affectant les obligations de sécurité de l'entreprise; rapports sur les besoins de changements dans l'organisation des systèmes de l'information.

Même sans la survenance d'un incident, les mesures de sécurité organisationnelles doivent être examinées de façon périodique. Une fois encore, suite à cette revue l'entreprise devra pondérer la nécessité d'ajuster les mesures existantes, et adopter des nouvelles mesures ou, de façon plus drastique, changer la stratégie de sécurité. Ainsi, l'entreprise devra effectuer

> « des vérifications et des audits, de façon périodique et au besoin, pour s'assurer du respect des mesures, des pratiques et des procédures relatives à la sécurité des actifs informationnels. [Elles] produiront des bilans périodiques portant sur les menaces ainsi que sur les mesures en place et celles qui sont prévues. Les menaces non contrées doivent être identifiées et la mise en place de nouvelles mesures de sécurité sera ensuite planifiée. »[150]

La structure du plan de réponse dépend des intentions de l'entreprise. Certaines préfèrent régler le problème et revenir rapidement aux conditions normales, d'autres voudront

---

[148] Nouvelles lignes sur la sécurité de l'O.C.D.E., précitée, note 46.
[149] Nouvelles lignes sur la sécurité de l'O.C.D.E., précitée, note 46.
[150] GOUVERNEMENT DU QUÉBEC, précitée, note 145, p. 29.

traîner les coupables en justice. Mais indépendamment de l'approche retenue, le plan de réponse doit toujours exister définissant les procédures à suivre et les responsables qui doivent prendre la situation en main. Ce traitement est nécessaire si l'on veut que la réponse soit rapide, méthodique et efficace.

Chapitre 2. Les mesures de sécurité physique concernant le matériel informatique et de milieu

La sécurité physique est un aspect fondamental de tout type de sécurité. Si quelqu'un réussit à accéder au système informatique de l'entreprise, il peut l'endommager ou même le détruire. Le terme sécurité physique du matériel et du milieu pour garantir l'intégrité, la confidentialité et la disponibilité des informations, réfère aux mesures prises pour assurer la protection des systèmes informatiques, des bâtiments et de l'infrastructure de support contre les menaces liées à leur environnement physique. La sécurité physique consiste aussi en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle.

Il existe beaucoup de menaces physiques pouvant porter atteinte à l'intégrité, la disponibilité et la confidentialité des ressources d'une entreprise. La sécurité physique étant un domaine complexe traité dans une panoplie d'ouvrages spécialisés[151], il nous sera impossible d'aborder tous les thèmes dans ce mémoire. Concentrons-nous alors sur l'essentiel, soit l'identification des menaces, le contrôle du matériel informatique et le contrôle de l'accès physique aux locaux et aux équipements.

Section 1. Bref survol des menaces physiques

La protection du matériel informatique n'est guère différente de la protection physique habituelle. Il suffit d'adapter les techniques classiques de protection contre les incendies, les inondations, tremblements de terre, les interruptions du courant électrique, les pannes, etc. Les risques associés à ces menaces varient selon la localisation géographique de l'entreprise. Normalement, les plans établis pour de telles circonstances ont toujours mis l'accent sur la préparation et la capacité de réaction[152]. Voyons brièvement quelques risques liés à l'environnement.

D'abord, les causes d'un incendie peuvent être soit intérieures (court-circuit, échauffements des câbles, etc.), soit extérieures (incendie provenant d'autres bâtiments). La prévention des incendies doit être prévue dès la construction des édifices qui hébergeront les équipements informatiques. Lors du choix de l'emplacement, l'entreprise devra considérer divers critères comme éviter les zones à risques, la qualité d'accès pour les équipes de secours (police, pompiers, etc.), la résistance du bâtiment, voire à la limitation du risque interne par

---

[151] Voir entre-autres : National Bureau of Standards, Guidelines for ADP Physical Security and Risk Management, Federal Information Processing Standard, Publication 31, juin 1974; Mary Lynn GARCIA, The Designs and Evaluation of Physical Protection Systems, Butterworth-Heinemann, 2001; Carl A. ROPER, Physical Security and the Inspection Process, Butterworth-Heinemann, 1996; Lawrence J. FENNELLY, Effective Physical Security, 2e éd., Butterworth-Heinemann, 1997.

[152] D. PIPKIN, précitée, note 124, p.38.

l'instauration de diverses règles, comme l'interdiction de fumer, portes coupe-feu ou le vidage fréquent des poubelles. L'entreprise devra aussi veiller aux moyens de détection et d'intervention, comme les systèmes de détection automatique de chaleur et de fumée et les systèmes d'extinction automatique par arroseurs. Aussi, pour faciliter la reprise des activités de l'entreprise, la technique classique pouvant être utilisée dans la plupart des accidents est le dédoublement physique des installations et le compartimentage des ressources matérielles selon leurs fonctions.

Dans le cas de fumées, des gaz toxiques et autres polluants peuvent provenir soit de l'extérieur, comme les poussières transportées par l'air et qui passent par le système d'aération, soit de l'intérieur, comme des cheveux humains et les poussières de papier, pouvant provoquer des bris et des pannes dans les matériaux informatiques plus fragiles, notamment dans les disques rigides des ordinateurs. Une fois encore, le choix de l'emplacement des locaux est crucial[153].

L'eau représente une menace aussi pour les ordinateurs, les supports magnétiques et même pour le papier. Que l'accident ait lieu dû à l'environnement naturel (sources d'eau, pluies abondantes) ou artificiel (rupture des tuyaux, fuites, état des locaux …), l'entreprise doit prévoir des mesures de sécurité qui protégent le matériel contre l'humidité et les pertes partielles ou totales des ressources physiques.

Bien que généralement plus facile à maîtriser, la sécurité physique doit également couvrir l'infrastructure, puisque les dommages causés à celle-ci peuvent être aussi dévastateurs pour une entreprise que ceux causés par les menaces naturelles. Par exemple, des pannes d'approvisionnement électrique peuvent entraîner différents risques tels que l'arrêt de l'exploitation, la perte d'informations, les modifications accidentelles, la destruction des supports contenant des données protégées, des erreurs de traitement, etc.

Il est vrai que les périphériques par lesquels transitent les réseaux sont souvent situés dans des zones non sécurisées, et l'énergie électrique ainsi que la climatisation ne sont pas l'objet d'une surveillance aussi soutenue que les ordinateurs eux-mêmes. Cependant, s'ils cessent de fonctionner, les ordinateurs s'arrêtent. Mais, dans une économie où la dépendance face à l'infrastructure grandit, l'entreprise doit être prête à gérer les pannes du matériel. L'indisponibilité du système et des communications est inadmissible pour les filiales et partenaires commerciaux (qui sont de plus en plus dispersés), ainsi que pour celles qui offrent leurs services par le biais d'Internet et joindre leurs clients. La solution à ce défi est encore une fois le fameux principe du dédoublement des moyens. Ce principe consiste à multiplier les éléments pour une fonction particulière de telle façon que le défaut de l'un d'eux n'entraîne pas l'arrêt complet du système[154]. Certaines entreprises optent pour une substitution du matériel considéré plus fragile, d'autres préfèrent l'installation en parallèle des systèmes complets pour assurer la continuité des traitements. Le choix dépendra de la capacité financière de l'entreprise.

Quoi qu'il en soit, l'entreprise n'a pas un contrôle total sur les menaces et il y a peu de choses qu'elle peut faire contre celles-ci, sinon les comprendre et être prête à leur éventualité. Néanmoins, toutes les décisions prises pour augmenter la sécurité devront être fondées sur l'exercice que nous avons déjà étudié dans le premier chapitre, l'évaluation des risques et la probabilité de pertes.

---

[153] J. HUBIN, précitée, note 110, p. 43.
[154] J. HUBIN, précitée, note 110, p. 48.

Section 2. Contrôle d'accès physique aux installations, au matériel informatique contenant des renseignements personnels

Tout comme l'accès aux locaux, l'accès aux équipements (matériel) renfermant des renseignements personnels ou encore les informations concernant les mesures de sécurité applicables à ces renseignements, doit obligatoirement être contrôlé. En sécurisant le matériel, l'entreprise est en mesure de contrôler de manière adéquate les ordinateurs, les fonctions remplies, les traitements, les sauvegardes et les transferts de données effectués par ces derniers. Ainsi, on pourra mieux prévenir la perte accidentelle, la modification des informations et s'assurer de la disponibilité des services. À cet égard, il est recommandé pour l'entreprise non seulement de dresser et tenir à jour un inventaire du matériel, spécialement le matériel destiné au traitement de données sensibles mais aussi d'attribuer la responsabilité de tenir à jour les dossiers concernant le matériel. Une copie de cet inventaire doit être conservée à l'extérieur de l'entreprise, dans la bibliothèque de soutien.

La disposition de l'équipement informatique doit être soigneusement étudiée de manière à éviter toute observation importune et tout accès non autorisé. Il faudra, notamment, que les écrans des ordinateurs ne soient pas tournés vers les fenêtres ou les portes, les imprimantes et les télécopieurs doivent être adéquatement protégés[155].

L'accès physique doit également être strictement étudié, puisque le risque couru par les systèmes informatiques est proportionnel au nombre d'accès autorisés. Certains accès physiques ne sont nécessaires que pour un nombre limité d'activités, comme le montage ou le démontage de l'équipement. Mais la notion d'accès va plus loin que le simple accès physique aux machines. Il doit s'appliquer aux informations écrites : documents contenant des informations personnelles laissées sur les bureaux, formulaires, courrier, fax, etc. Il ne faut pas oublier que le personnel de nettoyage peut ne pas fait pas partie de l'entreprise, mais a un accès direct à certaines données sensibles si elles sont laissées sans protection. Toutefois, il faut s'assurer ne pas mettre trop l'accent sur la propreté mais plutôt sur les problèmes de sécurité. On facilite ainsi la compréhension des employés et par conséquent, le respect des consignes. Les employés ne peuvent pas se contenter de mettre à la corbeille les documents, les disquettes ou tout autre document contenant des informations personnelles. Les notes et les documents « anodins » peuvent tenir des renseignements intéressants pouvant aller jusqu'à des mots de passe.

Une vulnérabilité fréquente au niveau de la protection du matériel informatique dans les entreprises est le manque de politiques et de procédures qui abordent le contrôle des changements effectués aux informations, notamment les modifications résultant des activités de maintenance. Ceci crée une menace pour l'entreprise, et ce, malgré le fait que le coût de réduction du risque est souvent minime. Par conséquent, il est vital que l'entreprise développe et applique des politiques internes et des procédures qui vise la sécurité du matériel.

L'accès physique englobe d'autres types d'accès comme les conversations, susceptibles d'être interceptées. Il est donc important que l'entreprise veuille à la sécurité des communications avec ses clients. Nous n'aborderons pas ce thème dans ce mémoire, mais

[155] G.R.C., précitée, note 126, p. 22.

nous conseillons la consultation des *Normes de sécurité technique dans le domaine de la technologie de l'information (NSTTI)* de la Gendarmerie royale du Canada[156].

Ainsi, si l'entreprise veut se doter d'une protection physique suffisante des locaux qui hébergent le matériel informatique et les documents contenant des renseignements personnels, elle devra nécessairement établir une routine permettant de contrôler l'accès physique à ces locaux. Cette routine peut, notamment, contenir les points suivants: des lignes directrices pour l'attribution ou la révocation les droits d'accès et les autorisations d'accès concernant les droits d'accès temporaires, la rédaction de règles internes rappelant la nécessité de verrouiller les locaux et de maintenir une supervision constante des ces derniers. Elle peut aussi se traduire par la mise en place d'un processus d'accompagnement des membres du personnel non autorisés ou étrangers au service, par la rédaction de directives concernant la conservation des journaux de bord de tous les accès autorisés et les tentatives d'accès ou accès non autorisés et surtout, par la description claire de l'autorité et des rôles des employés en la matière. De plus, l'accès aux ordinateurs et aux données à caractère personnel peut être restreint par l'imposition de divers contrôles d'accès basés sur des systèmes d'identification, d'authentification et d'autorisation. À cet égard, au sein de l'entreprise il serait approprié de mettre en place différents points d'accès ayant des niveau de sécurité propres, dépendamment de la sensibilité du contenu. Les responsables de la sécurité au sein de l'entreprise doivent désigner diverses zones de sécurité et établir diverses mesures de contrôle d'accès selon la sensibilité de l'information traitée. Ces zones ou niveaux de sécurité doivent être établies d'après le rapport de l'analyse des besoins d'accès et la nécessité d'échange de renseignements entre chaque utilisateur du système informatique de l'entreprise.

De plus, l'entreprise devra se constituer une bibliothèque et évidemment, devra en contrôler tous les accès. Cette bibliothèque de soutien conserve tous les fichiers de données, de programmes et d'objets, les copies originales des programmes, des systèmes et des logiciels, la documentation relative aux données, les copies d'archivage de données personnelles, les manuels et les consignes d'exploitation de tout le système d'information d'une entreprise. La bibliothèque ne doit pas seulement être constituée comme un local d'entreposage, mais doit être vue comme une voûte de sécurité. Elle permet l'assurer la sécurité et l'intégrité des données, des programmes, des systèmes et de la documentation. Elle permet aussi de prévenir l'accès non autorisé, la modification, la manipulation et l'utilisation frauduleuse des données et autres ressources informatiques de l'entreprise.

Ainsi, la bibliothèque devrait être séparée physiquement des autres locaux de l'entreprise. De plus, il faudra confier le contrôle de la bibliothèque de soutien à un responsable de la garde, de l'entretient, de l'enregistrement et du contrôle des supports de sauvegarde et de la documentation. Pour préserver l'intégrité des données, l'accès doit être réservé aux personnes responsables. Ni les employés ni le personnel d'analyse ne doivent avoir accès à la bibliothèque, sauf si le plan de contingence l'exige (encore faut-il que la personne soit clairement identifiée). Sans ce contrôle, il est peu probable que l'on puisse prouver l'intégrité et la pérennité des données gardées, et ce, tant au niveau de la protection des renseignements personnels, qu'au niveau de la preuve judiciaire.

---

[156] G.R.C., précitée, note 126, p. 39 et ss.

La sécurité de la bibliothèque doit être faite de manière constante. Ceci implique donc de tenir un registre des entrées et sorties des supports et de la documentation de la bibliothèque, l'actualisation de l'inventaire, la révision de l'étiquetage et d'effectuer des vérifications régulières et à l'improviste de la bibliothèque**.** L'entreprise doit aussi instituer des directives pour assurer la sécurité des données lorsqu'elles sont transmises à un service ou à une entreprise pour être traitées. Même si l'entreprise assure la sécurité des données à l'interne, lorsqu'elle envoie ses fichiers à un tiers pour être traités ou être reproduits, le fait de ne prendre aucune mesure de sécurité garantissant une sécurité adéquate tout au long du processus, et tant le caractère confidentiel que l'exactitude des données ne sont plus protégés.

Chapitre 3. La sécurité technique des documents contenant des données à caractère personnel et des programmes les hébergeant

Les orientations de sécurité et les grands principes énoncés dans les politiques et les procédures doivent devenir réalité et se traduire par un paramétrage adéquat des composantes techniques des systèmes, principalement en ce qui concerne les accès logiques. Ceci suppose donc une protection technique adéquate des donnés confidentielles et personnelles emmagasinées, transmises et reçues par une entreprise.

La sécurité technique réfère à la protection de l'intégrité, de la confidentialité et de la disponibilité des informations par la mise en place d'un processus qui permet de protéger, contrôler et surveiller tout l'accès à l'information. Dans ce chapitre, nous nous consacrerons à l'étude des différentes techniques et méthodes préconisées afin d'assurer la sécurité des données et des programmes qui emmagasinent des données personnelles dans les systèmes informatiques des entreprises. Nous aborderons des thèmes souvent mentionnés par la législation nationale et internationale, comme les contrôles techniques de l'accès (identification, authentification et autorisation) aux informations et la journalisation (logging) des accès et des modifications.

Il faut tout d'abord comprendre qu'une sécurisation efficiente des données passe par la prévention et la limitation de l'accès aux personnes non autorisées. Cet accès représente le premier degré de sécurité et concerne les mesures de sécurité matérielle mentionnées dans la partie antérieure. En principe, si les contrôles d'accès physique aux locaux et les mesures de protection physique du matériel sont efficaces, on s'assure que l'information confidentielle n'est pas perdue ou modifiée dans ou entre les divers systèmes informatiques par une attaque physique. On garantit aussi de cette manière, la disponibilité des services et l'accès aux informations en temps opportun.

Lorsque nous parlons de données en sécurité informatique, nous visons essentiellement ces types de données : les stratégiques, personnelles et confidentielles, tactiques (stocks, commandes livraisons, inventaires, etc.), fonctionnelles (transactions quotidiennes de comptabilité, dépenses, ventes, achats, statistiques, etc.) et techniques (normes, les procédures, manuels d'entreprise, attributions des responsabilités et autres méthodes de gestion). Celles-ci sont directement liées aux buts et objectifs de l'entreprise et à toutes les données confidentielles reliées à son exploitation. C'est à l'égard de ces données personnelles confidentielles que la plupart des lois s'appliquent.

Section 1. Les contrôles d'accès techniques aux documents contenant des renseignements personnels

Si l'accès physique ne peut être accordé qu'à des personnes, l'accès logique, lui, touchera aussi bien des personnes que d'autres entités, tel un système informatique ou un ordinateur. En matière d'accès technique ou logique, le risque a changé de nature et de dimension. En effet, il ne se limite plus à l'accès physique d'un contrôle de sécurité, mais bien à la possibilité d'un individu situé à l'autre bout de la planète de copier des fichiers ou de rendre un système indisponible. L'erreur n'est plus l'affaire d'un groupe de logiciels, mais bien de plusieurs maillons qui composent un réseau.

L'accès, c'est donc la façon dont l'utilisateur obtient des informations. Dans le dernier chapitre, nous avons étudié l'accès physique. Mais il existe un deuxième type d'accès, appelé accès logique. Les contrôles d'accès logiques (ou technique) sont conçus de manière à décourager l'entrée non autorisée, utilisant des informations connues uniquement des personnes autorisées. Le type d'accès dépend des exigences de sécurité des renseignements personnels conservés dans le système. Différents types d'accès demanderont différents niveaux de sécurité et de responsabilité. Aussi faut-il soigneusement peser toutes les autorisations d'accès aux données en s'appuyant sur les guides de classification des données déjà abordés dans le chapitre sur la sécurité organisationnelle[157]. Les contrôles généralement utilisés sont les mots de passe et les cartes d'identification. Ceux-ci se basent tous sur trois étapes fondamentales que nous allons analyser d'emblée : l'identification, l'authentification et l'autorisation.

1.1. L'identification

L'identification est le fondement de toute la sécurité. Tous, que ce soit un ordinateur ou un consommateur de données, doivent posséder un identificateur[158] unique qui permet d'effectuer l'identification sans ambiguïté. Sans identification, l'entreprise ne sera pas en mesure d'accorder une autorisation ou, le plus critique, d'attribuer les responsabilités. Elle sera aussi en mesure d'assignation des privilèges spécifiques à un usager ou à un ordinateur, de garantir la non-répudiation des opérations, de mettre en oeuvre des décisions sur les contrôles d'accès et de prévenir les accès déguisés par des étrangers[159].

Ainsi, pour éviter les erreurs d'identité, les usagers doivent être clairement identifiés avant d'avoir accès aux données à caractère personnel. Il existe plusieurs types de processus d'identification. Normalement, c'est l'entreprise elle-même qui crée les identificateurs qu'elle a l'intention d'utiliser. Mais, elle peut toujours faire appel à des identificateurs externes (ex. : permis de conduire, carte assurance-maladie), ceux-ci ayant l'inconvénient d'affaiblir la sécurité puisque le processus de création et de révocation n'est pas contrôlé. Dans tous les cas, l'identificateur doit comporter certaines caractéristiques[160] : il doit être unique, universel, vérifiable, infalsifiable, transportable et facile à utiliser. Ainsi, chaque utilisateur ne doit avoir qu'un seul identificateur, même si l'utilisateur joue plusieurs rôles, facilitant tant l'association entre l'identificateur et l'individu que la gestion et la délivrance. Cet identificateur ne doit pas être partagé, surtout pour un contrôle efficace des informations personnelles, faute de quoi, il ne serait plus possible de responsabiliser un individu.

De plus, chaque individu doit utiliser le même type d'identificateur (universalité). On simplifie ainsi le stockage et la gestion. Le processus de vérification doit être le même partout dans l'entreprise pour simplifier les interfaces d'accès et garantir une meilleure acceptabilité. Si

---

[157] Voir Partie 2, Chapitre 1, section 2, supra, p. 80.
[158] Un identificateur est une entité qui représente un utilisateur pour un système informatique quelconque.
[159] G. STONEBURNER, précitée, note 123, p. 15.
[160] D. PIPKIN, précitée, note 124, p. 130 – 131.

l'identificateur est difficile à utiliser, on peut entraver gravement son acceptation ou même le rendre inutilisable s'il présente une forte dépendance à la structure, surtout lorsque celle-ci est indisponible. De plus, l'identificateur doit être difficile à falsifier. L'utilisation d'hologrammes (comme ceux utilisés sur les cartes de crédit VISA) rend la falsification d'une carte coûteuse. Si l'entreprise utilise les cartes à puces comme identificateur, il faut s'assurer que la carte empêche des méthodes de falsification, notamment l'utilisation de moyens cryptographiques, qui protègent les données stockées. En cas de destruction de la carte, il faudra s'assurer de que la réutilisation après désactivation soit impossible. Le but est de causer des dommages matériels suffisants au support pour prévenir toute récupération des données qui y sont emmagasinées.

De plus, en matière de sécurité informatique, il faut se rappeler qu'un système inutilisé est souvent le plus dangereux. Ainsi, dans le cas des identificateurs, il faut se souvenir que plus il est transportable, plus facilement il sera utilisé par les usagers. Toutefois, dans la majorité des cas, un système ne sera pas utilisé s'il est trop irritant ou compliqué (par exemple, les programmes servant à crypter et signer les messages électroniques, comme P.G.P). La sécurité est un pacte. Cette dernière est plus facile si elle est visible pour l'utilisateur lors de l'interaction et la prise de décisions. D'un autre côté, les utilisateurs ne veulent pas voir les mesures de sécurité.

> « […] A smart security designer doesn't want users to see security. A smart security designer knows that users find security measures intrusive, that they will work around then whenever possible, that they will screw with the system at every turn. People can't be trusted to implement security policies, just as they can't be trusted to lock their car doors, not to loose their wallet […] ».[161]

Une fois l'identificateur choisi, l'entreprise devra se pencher sur les questions de la portée et de l'administration de l'instrument. La portée de l'identificateur dépendra du niveau de confiance dans sa qualité. Si une portée restreinte offre un contrôle plus local des systèmes, en contrepartie, celle-ci oblige les utilisateurs à s'identifier chaque fois qu'ils se servent d'une ressource différente. Un identificateur à portée étendue réduit le nombre d'identifications nécessaires, mais demande un niveau de confiance accru au moment de la délivrance de ce dernier.

Quant à l'administration des identificateurs, soit leur création, leur révocation, leur distribution et leur destruction, on peut adopter un système de gestion centralisé ou décentralisé[162]. Une administration centralisée permet d'appliquer les mêmes standards de preuve lors de l'identification. On facilite ainsi la gestion des comptes, mais les délais de délivrance et de vérification sont plus grands. Ce type de système s'applique mieux dans une entreprise avec peu d'employés. Toutefois, si l'on prend comme exemple les identificateurs pour le gouvernement, il serait préférable d'adopter un système d'administration décentralisée. Ce dernier facilite l'attribution des identificateurs en réduisant le temps d'attente et le temps de résolution de certains problèmes techniques locaux. Cependant, il est difficile de conserver le caractère universel de l'identificateur et on peut rencontrer des problèmes de synchronisation[163].

---

[161] B. SCHNEIER, précitée, note 108, p. 261.
[162] D. PIPKIN, précitée, note 124, p. 133.
[163] Gaston PARADIS, « Authentification dans les environnements de traitement distribués », Journal 13.3 Association des Professionnels de la Vérification et du Contrôle des Systèmes d'information, Montréal, 2002 en ligne : APVCSI <http://www.apvcsi-montreal.ca/fr/publications/contact133f.htm>.

1.2. L'authentification

L'étape suivante est celle de l'authentification. En d'autres termes, le processus de vérification de l'identité de l'utilisateur. Une identification certaine assure l'accès adéquat à une ressource donnée. Sans cette étape, on ne peut être assuré que l'information à laquelle on accède est bien celle à laquelle l'on veut accéder ou on est en droit d'accéder. C'est donc une composante indispensable pour garantir la confidentialité, l'intégrité et la disponibilité de l'information. Une forte authentification est nécessaire dans tous les aspects de la sécurité et durant tout le cycle de vie des informations. Si l'une des étapes d'authentification est faible, on court le risque de compromettre le reste. Alors que l'identification est la partie physique de l'accès, l'authentification est la partie logique, nécessitant l'intervention directe de l'usager.

Actuellement, il existe trois facteurs de base pouvant être utilisés à des fins d'authentification : quelque chose que l'on *possède* (un objet – ex. : clé, carte magnétisée ou à puce), quelque chose que l'on *sache* (un secret – ex. : mot de passe, numéro d'identification personnelle ou une clé cryptographique) ou quelque chose que l'on *est* (caractéristique biologique)[164]. Ces moyens peuvent être utilisés seuls ou combinés ; le choix de l'un ou l'autre dépendra encore une fois des besoins spécifiques de l'entreprise. Généralement, les systèmes utilisant les mots de passe impliquent que l'utilisateur inscrive son identification et son code secret. L'avantage des mots de passe c'est la grande facilité avec laquelle ils sont utilisés. Toutefois, même si ce type de contrôle d'accès donne une certaine protection aux systèmes contenant des renseignements personnels contre l'accès, il s'avère insuffisant pour stopper une intrusion intentionnelle d'un malfaiteur quelque peu persévérant. Les mots de passe présentent aussi d'autres désavantages. Ils ne peuvent procurer une protection que dans la mesure où ils demeurent secrets. Mais, il existe plusieurs façons de dévoiler un secret: deviner un mot de passe évident ou emprunté, surveillance électronique des mots de passe utilisés et accéder aux fichiers contenant les mots de passe. Malgré ça, les mots de passe peuvent donner une sécurité suffisante aux entreprises qui veulent protéger les informations à caractère personnel qu'elles détiennent. Il faut seulement respecter quelques règles de base que tous les employés doivent connaître.

D'abord, pour un ordinateur, un mot de passé fonctionne un peu comme une clé. Permettre à plusieurs personnes d'utiliser le même mot de passe revient à donner une clé à plusieurs personnes et évidemment à la perte du contrôle. Idéalement, le mot de passé devrait être composé par des chiffres et de lettres et contenir aux moins six caractères. Ils devront être changés périodiquement, au moins tous les 3 mois et s'assurer que les utilisateurs du système informatique sont informés lorsque leur mot de passe expire[165].

Des protections techniques peuvent aussi être utilisées pour augmenter l'efficacité des mots de passe : limites dans les tentatives, changement sporadique des mots de passe et la protection des fichiers de mots de passe par la cryptographie, etc. De plus, ces mots de passe doivent être adéquatement gérés. Ceci implique l'utilisation d'une liste contenant l'historique des mots de passe utilisés au cours dernières années pour empêcher l'utilisation des mots de passe communs. À ce stade, il serait pertinent de donner aux utilisateurs une liste des mots de passe interdits comme les noms communs, marques ou autres combinaisons faciles à deviner. Certains systèmes génèrent automatiquement des mots de passe. Le désavantage d'un tel

---

[164] J. CRUME, Inside Internet Security: What Hackers Don't Want You To Know; London, Addison-Wesley, 2000.

[165] Un bon exemple de ce système est celui utilisé par le site du registraire de l'Université de Montréal en ligne : <www.umontreal.ca>.

système est que les utilisateurs ont tendance à oublier les mots de passe et écrivent leurs codes d'accès sur des bouts de papier, créant ainsi une vulnérabilité dans le système.

Un système d'accès basé à la fois sur quelque chose que l'on sait (N.I.P., mot de passe) et sur quelque chose que l'on a (carte magnétique) est beaucoup plus sécuritaire. Même advenant que le mot de passé soit découvert, les données protégées restent inaccessibles sans la possession de la carte. Il existe deux types de cartes. Tout d'abord, les cartes à bande magnétique. Tout comme son nom l'indique, ce type de carte contient une bande magnétique qui contient l'information confidentielle qui doit être utilisée avec le code personnel de l'utilisateur. Ensuite, les cartes à puce qui, à la place de la bande magnétique, utilisent un microchip et sont souvent dotées d'un système de cryptage. La différence entre les deux cartes est la capacité de traitement de l'information par la carte à puce : la faculté d'enregistrement du chip est plus élevée que celle d'une bande magnétique. Ce système présente de nombreux avantages, notamment le fait qu'il offre une sécurité accrue qui réduit considérablement le risque de falsification et le nombre d'authentifications nécessaires pour accéder aux ressources. Cependant, ce système requiert un investissement significatif de la part de l'entreprise dans l'installation initiale des lecteurs, des frais additionnels en cas de perte des cartes, mais surtout les utilisateurs semblent être plus réticents à ce type de contrôle.

Les systèmes hautement confidentiels utilisent une troisième méthode de contrôle d'accès basé sur quelque chose que l'on *est*. Ce système biométrique se base sur les caractéristiques physiologiques d'une personne, par exemple l'empreinte digitale, la digitalisation de la rétine, la configuration de la main ou sur des attributs comportementaux comme la voix ou une empreinte manuscrite. Malheureusement, la biométrie est une mesure de sécurité encore trop coûteuse et complexe pour certaines entreprises, ce qui explique qu'elle soit très peu répandue, et ce, malgré le fait que certaines lois proposent ce système pour garantir une identification adéquate, comme la Loi concernant le cadre juridique des technologies de l'information[166].

Cette technique d'authentification présente un autre inconvénient majeur : en effet « aucune des mesures des mesures utilisées ne se relève être totalement exacte car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent. »[167]

L'autre désagrément de cette technologie est que, malgré le fait qu'elle soit utilisée pour protéger la vie privée, elle peut dans certains cas être une ennemie encore plus redoutable. Sur ce point, le commissaire à la vie privée de l'Ontario prétend que :

> « If there is a general reliance on biometric identification and authentication for a variety of daily transactions, our movements and behaviors could be efficiently tracked. […] But, the greatest danger would be the expansion of such use for well-meaning purposes (augmentation de la sécurité) to other went beyond the original purposes and failed to address the limitations of the original collection activity. […] An additional danger surrounding the reliability of biometrics is not only their true reliability but also their perceived

[166] Voir Loi concernant le cadre juridique des technologies de l'information, précitée, note 37, articles 44 et 45.
[167] SECURITEINFO, « Le grand livre de la sécuritéinfo.com », 18 février 2002, p. 117, en ligne <http ://www.securiteinfo.com>.

> reliability. If the exception exists that they are irrefutable, then questioning them will become extremely difficult, not only in legal realm but also in the everyday realm. »[168]

Lorsque l'administration d'une entreprise met en place des nouvelles directives ou procédures, elle devrait étudier l'impact que celles-ci auront sur le traitement des informations personnelles des employés. Vu que ces derniers seront les acteurs directs sur le plan de la sécurité de l'entreprise, il est toujours préférable de tenir compte de leurs suggestions et préoccupations. À ce propos, il serait pertinent de consulter le syndicat des travailleurs ou tout autre représentant des employés de l'entreprise concernant des questions de développement et l'implantation de processus de sélection d'emploi ou toutes autres procédures qui touchent le traitement des données personnelles des employés. Il faut dire que ce type de contrôle peut se compliquer si l'entreprise fait appel aux services à un tiers pour la gestion et la manutention de la sécurité.

L'administration des données d'authentification est un élément essentiel tant pour les mots de passe, que pour les cartes ou la biométrie. Les systèmes d'identification et d'authentification doivent être créés et distribués de manière à ce que données soient adéquatement gardées. Dans un système utilisant des mots de passe, il importe de les créer, les attribuer aux usagers et de maintenir une liste des registres. Pour les cartes, l'administration de l'authentification implique la fabrication des cartes, leur distribution et la configuration des ordinateurs. Pour la biométrie, il faut créer et sauvegarder correctement les profils. Nous avons vu précédemment que les fichiers d'identification et d'authentification doivent être tenus à jour par l'addition de nouveaux utilisateurs et la destruction de ceux qui ne sont plus nécessaires. De plus, des lignes directrices doivent s'adresser aux problèmes de la perte et du vol des identificateurs et aussi de la détection de comptes d'accès inutilisés ou partagés. La valeur de l'authentification réside dans la confidentialité, l'intégrité et la disponibilité des fichiers. Si l'une de ces caractéristiques est compromise, l'entreprise ne peut ni contrôler les accès aux données personnelles, ni vérifier l'exactitude de ces données. Ainsi, une personne doit être spécialement mandatée pour révoquer ou suspendre le code d'identification et le moyen d'authentification d'un autre utilisateur. Ces révocations ou suspensions devront être faites, notamment, lorsque cet utilisateur quitte définitivement l'organisme ou est congédié, lorsqu'il a terminé son contrat, lorsqu'il change de fonctions à l'intérieur de l'organisme et que ses nouvelles fonctions n'exigent pas l'accès aux données personnelles, lorsqu'il y a abus ou indice d'usage abusif ou lorsque l'utilisateur doit s'absenter pour une période déterminée par l'organisme.

1.3. L'autorisation

En plus des mesures l'identification et l'authentification fiables de l'usager, il doit exister un ensemble de règles qui contrôlent ce à quoi l'usager à accès et quelles sont les limites de ses les actions. Autrement dit, ses « privilèges ». Ainsi, l'autorisation est une permission, et la permission offre un privilège à une entité pour effectuer une action. Ensemble, elles permettent de surveiller les actions des utilisateurs et à limiter les usages abusifs. L'autorisation doit aussi être basé sur le concept des privilèges minimaux, d'où l'importance d'avoir bien défini les rôles et les fonctions des usagers du système.

---

[168] Commissaire à la vie privée de l'Ontario, « Biometrics and Policing : Comments from a Privacy Perspective», Ontario, septembre 1999, en ligne : <http://www.ipc.on.ca/scripts/index>.

En matière de contrôles d'accès, le Rapport final de l'examen des mesures de sécurité en place à la Société de l'assurance automobile du Québec[169], élaboré en mai 2001, considère que les mesures suivantes (entre autres) sont adéquates :

> « Tous les accès locaux et à distance sans exception sont pris en charge par une validation basée sur l'individu qui accède au système [où] les utilisateurs doivent changer leur mot de passe aux 30 jours, […] un identifiant est annulé après 90 jours d'inutilisation, […] effacé après cinq tentatives de connexion infructueuses en 24 heures, [..] révoqué selon certains codes d'absence saisis par les ressources humaines (exemple: maladie prolongée), […] et surtout, un utilisateur doit signer un engagement à ne pas divulguer son mot de passe pour obtenir un code d'accès et lors d'un départ le code d'accès est révoqué, lors d'un changement de fonction, le code d'accès est révisé. »

Si un système de protection d'accès garanti l'identification, l'authentification et l'autorisation, il est aussi en mesure d'assurer la non-répudiation des opérations (transferts, modifications, effacements, etc.) effectuées en rapport avec les renseignements personnels. Le mécanisme de non-répudiation empêche une personne ou un organisme de nier qu'il a reçu, transmis ou consulté certaines données.

Section 2. La sécurité technique des logiciels contenant des renseignements personnels

À l'intérieur d'un cycle de vie d'un système de fréquentes modifications, des mises à jour et des conversions sont nécessaires. Or tout ceci se doit d'être planifié afin que les programmes ne soient modifiés qu'au bon moment et que par les personnes autorisées. Ainsi, il est souhaitable que les fonctions de programmation et de gestion des systèmes, gestion des bases de données contenant des renseignements personnels, contrôle et entretient du système et des logiciels soient attribuées à des personnes différentes relevant d'entités organisationnelles distinctes, dans la mesure où la taille de l'entreprise permet une telle dépense[170].

Les systèmes dont les composantes sont modifiées, retirées ou ajoutées doivent faire l'objet de tests et d'essais dans un environnement isolé jusqu'à ce qu'il soit fiable. Son avènement doit être planifié et minutieusement contrôlé. Il faut ici contrôler l'exploitation de l'ensemble des programmes nécessaires à la marche des ordinateurs, des périphériques et des réseaux. Une bonne administration de ces ressources nécessite l'intervention d'employés spécialisés qui assurent le fonctionnement global du système.[171]

Dans plusieurs cas, le logiciel peut être considéré comme des renseignements de nature délicate par lui-même, car il peut contenir des virus. Ils doivent alors être protégés par des mesures qui servent à garantir la sécurité des programmes informatiques, des systèmes d'exploitation, des langages de programmation, etc. D'une perspective de sécurité, on peut considérer le logiciel de trois manières : comme une protection, une production ou une menace. Le premier type renferme les logiciels qui fournissent les contrôles d'accès, la cryptographie, la gestion du réseau, les sauvegardes… En d'autres mots, ce sont les outils de protection de

[169] M. CHASSÉ, précitée, note 83, p. 10.
[170] G.R.C., précitée, note 126, p. 49.
[171] CHASSÉ, précitée, note 83, p. 15.

l'entreprise. Le deuxième type englobe tous les logiciels utilisés quotidiennement par l'entreprise (bases de données, traitements de textes, etc.).

Il est donc important d'utiliser des logiciels qui sont capables de différencier les utilisateurs les uns des autres de sorte qu'aucun d'eux ne puisse nuire à un autre dans les conditions normales. Les logiciels d'accès doivent protéger adéquatement les fichiers et les répertoires individuels en mode lecture, écriture, modification, exécution ou suppression. Toutefois, certains logiciels sont capables de passer outre les barrières de sécurité de l'entreprise et peuvent être utilisés pour gagner un accès non autorisé aux renseignements personnels. Ils peuvent aussi être utilisés pour prendre contrôle du système informatique et rendre indisponible les données. L'entreprise doit mettre en place des mesures de sécurité qui préviennent et détectent la présence de programmes malins ou destructeurs dans les systèmes informatiques, comme les vers, les virus, cheval de Troie, bombe logique, etc.

Le virus, par exemple, est un programme qui, à l'insu de l'utilisateur, exerce une action nuisible à son environnement : modification ou destruction de fichiers, effacement du disque dur, allongement des temps de traitement, manifestations visuelles ou sonores plus ou moins inquiétantes, etc. Mais on sait moins que les virus peuvent aussi servir à crocheter les systèmes les plus secrets en créant des vulnérabilités « cachées » qu'un autre processus exploitera ultérieurement[172]. Ils ne perturbent pas le système et ne détruisent pas de données. Sur une machine ainsi contaminée, votre système d'information est un livre ouvert. Il n'est plus question alors de parler de sécurité ! On voit ici que les virus s'attaquent à tous les aspects de la sécurité définie dans la trilogie : confidentialité, intégrité, continuité de service.

Puis, une fois ces zones critiques modifiées ou détruites, le contenu du disque peut être considéré comme perdu. D'où l'importance d'avoir des directives de sauvegarde pour protéger les systèmes en cas d'incident informatique. Pour la protection contre les virus, il est recommandé de contrôler toutes les nouvelles applications à installer, de verrouiller les supports de stockage quand ils n'ont pas besoin d'être en écriture et d'avoir un antivirus à jour.

Les mesures servant à la découverte de tels programmes doivent être fréquemment actualisées. Dans le cas où de tels programmes malicieux seraient décelés, l'entreprise doit avoir une routine de sécurité en place, facilitant ainsi la protection et la remise en état du système.[173] De plus, la responsabilité du personnel dans ce domaine doit être clairement répartie surtout dans les secteurs d'élaboration, de l'essai et de l'assurance de la qualité, de l'utilisation d'un nouveau logiciel où cette transition doit être bien définie et soigneusement contrôlée.

Section 3. Les mesures de sécurité technique des opérations affectant les renseignements personnels

Des procédures bien définies encadrant les opérations de l'entreprise assurent l'efficacité des politiques de sécurité. La sécurité des opérations a trait à la gestion quotidienne de la sécurité informatique : aux fonctions de contrôle des changements, à la sauvegarde du système et à sa surveillance, etc. Ces procédures permettent aussi de garder la trace de tous les évènements et actions effectuées sur un système et facilitent une action corrective. Ce principe doit s'appliquer à l'ensemble de l'organisation. L'entreprise doit adopter des mesures

[172] R. LONGEON et J.L. ARCHIMBAU, précitée, note 113, p. 66.
[173] DATATILSYNET, Information Security Guidelines for the processing of personal information, TR-100E: 1998, Data Inspectorate (Datatilsynet), avril 1999, p. 16, par. 18.3.

de sécurité qui permettent un contrôle adéquat de l'échange d'information personnelle et la communication des mesures de sécurité concernant la conservation de cette information. Le manque de mesures de sécurité touchant ce point peut être fatal pour l'image d'une compagnie. En 2001, la Société de l'assurance automobile du Québec fut prise avec un problème de bris de confidentialité de renseignements personnels attribué à un (ou des) employé(s) et à une employée d'un mandataire. Suite à ces évènements, la Société a dû mettre en place des mesures de sécurité et de surveillance en place notamment en ce qui regarde l'accès aux données et les mesures de contrôle *a priori* et *a posteriori* quant à ces accès. En effet, le rapport sur les mesures de sécurité en place à la S.A.A.Q. recommande à la société de revoir son mécanisme d'attribution des accès pour que celui-ci soit suffisamment rigoureux pour permettre que l'attribution se fasse en fonction des responsabilités confiées à une personne et non en fonction de la structure administrative. De plus, il conseille la société à rechercher un moyen qui permettra de restreindre l'accès (accès par ailleurs justifiés) aux organismes externes aux seules données nécessaires pour la réalisation de leur travail.[174]

Les opérations quotidiennes de l'entreprise impliquent aussi la transmission de données, surtout en ce qui a trait aux renseignements personnels entre les partenaires commerciaux. Mais les renseignements personnels et l'information concernant les mesures de sécurité qui leur sont applicables doivent être échangés avec un tiers (à l'extérieur de l'entreprise) seulement dans la mesure où cela est nécessaire aux opérations de l'entreprise. De plus, les exigences relatives à la sécurité de la transmission de renseignements personnels sur le réseau de communication exigent que tous les renseignements soient chiffrés au moyen d'une méthode de chiffrement approuvée. De cette façon, l'entreprise est en mesure de garantir la confidentialité, l'authenticité, l'intégrité des données transférées et la non-répudiation des transmissions.

L'entreprise doit alors mettre en place des mesures de sécurité et des directives visant le contrôle des opérations externes. Ces dernières doivent au moins toucher : les directives empêchant la modification ou la destruction des données durant le transfert en utilisant, par exemple un contrôle d'intégrité, des directives assurant la confidentialité des informations, nécessitant ainsi la mise en place d'un système de cryptage, la conservation des journaux de bord sur tous les échanges vers l'extérieur et la définition des responsabilités et des rôles en la matière.

Mais, afin de dépister les modifications effectuées au système et détecter les anomalies rien ne vaut les fichiers de journalisation. Que ce soit à des fins de contrôle ou pour respecter la loi, il est indispensable de conserver un enregistrement des activités de chaque utilisateur du système informatique.

Par exemple, l'article 41 de la Loi concernant le cadre juridique des technologies de l'information[175] exige que la consultation d'un document technologique ayant servi à l'identification d'une personne soit journalisée. Donc, toute information relative à la consultation devra être portée à un journal de bord, permettant de savoir qui et quand la consultation s'est réalisée.

Si la surveillance de la structure de la banque de données et de la sécurité qui l'entoure procure une certaine protection, il faut aussi implanter des mesures qui permettent de vérifier si

[174] M. CHASSÉ, précitée, note 83, recommandation 4 et 5, p. 19-20.
[175] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37.

l'utilisation des données se fait conformément à ce qui est autorisé par l'organisation[176]. Bien sûr, la détermination des informations à enregistrer dépend de la sensibilité du système.

Un système de journalisation est destiné à assurer la sécurité, le bon fonctionnement d'un système ou d'une application informatique et surtout de détecter les activités illégales. Il n'a pas pour vocation première de contrôler des utilisateurs, mais découvrir les incidents de sécurité. Les enregistrements doivent être eux-mêmes sécurisés, faute de quoi on pourrait facilement modifier les données et l'enregistrement serait inutilisable en cas de poursuite judiciaire. La règle d'or des journaux de bord est qu'ils doivent être conçus de façon à pouvoir constituer des preuves. « La période de conservation des journaux dépend de la Loi sur les archives. Cependant, si une enquête ou des procédures judiciaires sont entamées, les journaux seront conservés tant que le dossier ne sera pas fermé. »[177]

Ainsi, le calendrier de conservation de la journalisation doit être établi en fonction des lois, normes et règlements en vigueur[178]. Toutefois, si, sur le plan technique ces éléments peuvent être considérés comme suffisants, ils ne peuvent pas toujours être regardés comme des preuves irréfutables, ne serait-ce qu'en raison de la facilité de falsification de tout document informatique. Selon la Loi concernant le cadre juridique des technologies de l'information par exemple,

> « un document technologique a même la valeur juridique dans la mesure où son intégrité est assurée. L'intégrité du document est assurée lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité durant son cycle de vie, depuis sa création jusqu'à sa conservation, archivage ou destruction. »[179]

Ces articles démontrent clairement l'importance de garantir la protection des journaux de bord par des mesures de sécurité adéquate, notamment celles empêchant les modifications et la conservation dans la bibliothèque de sécurité dûment protégée. Même si elles ne permettent pas de traîner le coupable devant les tribunaux, ces informations sont précieuses pour aider la police à identifier l'auteur d'une intrusion.

Dans le cours normal des activités d'une entreprise, de nombreux ajouts et retraits se font dans la structure d'une banque de données au cours de son cycle de vie. Ces modifications, créations et mises au rancart doivent être planifiées et se réaliser selon un cheminement qui évite que des données ne soient manquantes ou ne se retrouvent au mauvais endroit. On peut ainsi préserver la disponibilité, l'intégrité et la confidentialité des données. Tout ceci exige qu'une organisation s'assure de la cohérence de la structure et de l'évolution des banques de données qu'elle détient. Si la surveillance de la structure de la banque de données et de la sécurité qui l'entoure procure une certaine protection, il faut aussi implanter des mesures qui permettent de vérifier si l'utilisation des données se fait conformément à ce qui est autorisé par l'organisation et notamment, par le biais de la journalisation des accès.

Étant donné le grand nombre de transactions effectuées par une entreprise, l'exploitation sur une base régulière de la journalisation peut s'avérer fastidieuse. Cependant, la

---

[176] M. CHASSÉ, précitée, note 83, p. 14.
[177] GOUVERNEMENT DU QUÉBEC, précitée, note 144, p. 39.
[178] Sur ce propos consulter notamment l'article 20 de la Loi concernant le cadre juridique des technologies de l'information, précitée, note 37 et la Loi sur les archives, L.R.Q., chapitre A-21.1.
[179] Loi concernant le cadre juridique des technologies de l'information, précitée, note 37, art. 5 et 6.

protection des renseignements personnels et des autres données sensibles demande des efforts parfois contraignants. L'entreprise peut alors considérer la possibilité de procéder à la journalisation par échantillonnage, réduisant considérablement le nombre d'informations à traiter[180]. Cette activité peut-être bénéfique si elle est faite dans un but de détection, mais aussi de dissuasion. En effet, les journaux de bord sont de mesures de sécurité technique aidant l'entreprise dans la responsabilisation de leurs employés. Et en avisant les usagers qu'ils pourront être tenus personnellement responsables pour les actions, qui sont enregistrées sur les journaux de bord, l'entreprise parviendra à promouvoir un comportement adéquat en matière de sécurité. Les usagers seront alors moins tentés de contourner les règles de sécurité sachant que leurs activités sont saisies. Aussi, si l'on ne peut empêcher un usager d'utiliser son autorisation valable pour des fins prohibées, la journalisation permet d'effectuer un contrôle a posteriori. L'avantage est considérable. L'utilisation des journaux de bord aidera aussi l'entreprise à se protéger contre les usagers non identifiés. Bien sûr, elle ne sera pas en mesure d'attribuer la responsabilité du contrevenant, mais facilitera néanmoins la mise en œuvre du plan de contingence et de la réévaluation de son système de sécurité.

Conclusion de la deuxième partie

L'information est devenue une ressource primordiale pour la bonne marche des entreprises et des organismes publics. Le fonctionnement de beaucoup d'entreprises repose en effet sur leurs systèmes d'information. Plusieurs finissent par découvrir que leur entrepôt de données a bien plus de valeur que leur entrepôt de marchandises.

Les informations en revanche sont plus fragiles que les biens, plus fragiles que les biens matériels car il est facile de les perdre, les détruire ou de les voler. Aussi les mesures de protection qui leur sont appliquées doivent-elles être plus rigoureuses et plus complètes que celles qui s'appliquent aux biens physiques. En raison des constants changements qui interviennent dans les techniques informatiques, ces mesures doivent être suffisamment souples pour s'adapter rapidement aux circonstances.

Il est bien entendu illusoire de vouloir donner en un espace aussi court un aperçu complet des diverses mesures de sécurité à mettre en oeuvre pour protéger les données à caractère personnel. Les risques diffèrent d'un environnement à l'autre et les protections devront y être adaptées de manière proportionnée, de manière cohérence.

La mise en place de ces mesures adéquates impliquent nécessairement une initiative active de la part de l'entreprise en matière de planification et de définition de la sécurité comme un processus variable demandant une réévaluation épisodique et une adaptation constante à l'état de la technique et aux besoins de l'entreprise. En d'autres mots, la simple mise en place d'une protection technique ne soustrait pas l'entreprise à son obligation de contrôle adéquat des renseignements personnels qu'elle détient. Ainsi, la sécurité est un processus continu qui requiert une mise à jour et une adaptation constante : la surveillance de la mise en place et de l'efficacité du programme de sécurité est depuis longtemps considérée comme l'une des meilleures pratiques en la matière.

De plus pour être efficace, la sécurité requiert l'attention soutenue de la haute direction. Il est important que les responsabilités et la ligne d'autorité soient clairement identifiées sur le plan organisationnel en matière de sécurité de l'information. La direction doit aussi instaurer des contrôles permanents propres à assurer la protection des systèmes, des programmes et des

[180] M. CHASSÉ, précitée, note 83, p. 13.

données sensibles, des biens et des personnes. De plus, les systèmes et les mesures de sécurité pour être crédibles se doivent d'être régulièrement exposées à un regard critique et indépendant et c'est là qu'intervient l'audit ou la vérification.

La sécurité dépend de tous, et tous les facteurs interagissent entre eux. La qualité des hommes – compétence, motivation, formation – est importante ; il faut y porter un effort constant. Si les techniques et les moyens financiers sont vitaux et ne doivent pas être négligés. De tous les facteurs et acteurs qui interviennent dans les systèmes d'information et contribuent à la force ou à la faiblesse de l'ensemble, les directeurs d'unité jouent le rôle essentiel. La sécurité des systèmes d'information est une fonction de direction. Cela ne veut pas dire que les directeurs doivent mettre une casquette et contrôler les identités. Cela signifie simplement qu'ils mettent en place une organisation et ont un style de direction qui favorise la prise en charge de cette question ; ce sont donc eux qui déterminent la politique de sécurité de leur laboratoire et qui sont également chargés de l'appliquer. Il n'y a qu'eux qui peuvent le faire, et rien ne se fera s'ils ne sont pas personnellement convaincus de l'importance de cette tâche. De même, à l'autre bout de la chaîne, l'utilisateur final a la charge de l'exécution de tous les actes élémentaires de sécurité. S'il ne voit ces mesures que comme une somme de contraintes mises en place pour lui gâcher la vie, la partie est perdue d'avance. D'où l'importance des recommandations de sécurité et des chartes informatiques qui, accompagnées des explications nécessaires, sont avant tout un moyen de sensibilisation.

Il faut donc rappeler que la sécurité n'est pas une fin en soi. Il ne s'agit pas de partir à la quête de l'absolu, mais de déterminer un seuil de vulnérabilité acceptable en fonction de contraintes et d'objectifs, et d'en contrôler les défaillances par des alarmes, des audits et l'enregistrement des accès réseau.

Conclusion générale

L'objectif de ce mémoire visait à proposer non seulement un encadrement « juridico technique » pour les dirigeants qui veulent s'assurer de la conformité de leur entreprise aux obligations légales en matière de données personnelles, mais aussi à fournir à la communauté juridique une étude simplifiée du domaine de la sécurité informationnelle. Ce travail de recherche conscientise la société de la pluridisciplinarité du droit et ensuite de l'importance de la sécurité dans la protection des droits fondamentaux des individus. Le droit n'est plus une matière isolée et les juristes doivent être certains d'appréhender cette nouvelle culture de sécurité qui émerge dans les divers textes de loi. Il importe aussi de bien comprendre la collaboration étroite qui doit exister entre la protection juridique et la technique employée pour sécuriser les réseaux. Nous pouvons d'ailleurs donner de nombreux exemples de cette collaboration : la norme P3P[181] visant la protection de la vie privée sur Internet, le développement des contrats électroniques et du commerce sur le réseau par l'apport des technologies informatiques comme la cryptographie, les signatures numériques et les certificats. La technologie a aussi joué un rôle important dans la protection et la conservation des droits intellectuels surtout dans le domaine de l'industrie de la musique et des oeuvres cinématographiques sur DVD en ce qui concerne la réduction du nombre de contrefaçons. L'Organisation mondiale de la propriété intellectuelle explique :

> «Various practical measures can be undertaken in order to combat piracy. To some extent protection can be obtained through various types of copy-protection systems, that is, that mechanisms ("spoiler signals" or "water marks" in sound or video recordings) are built in which prevent unauthorized copying. »[182]

Ces exemples démontrent clairement les avantages et la croissance de la coopération entre le juridique et la technologie.

Si les lois actuelles peuvent être critiquées en ce qu'elles ne définissent pas clairement la portée de l'obligation de sécurisation des renseignements personnels imposée aux entreprises et en ce qu'elles offrent encore moins des critères servant de guide à ces dernières, les lignes directrices émergeant, tant du secteur privé ou public et au niveau international, notamment celles de l'O.C.D.E., réussissent à baliser la notion de « mesures de sécurité adéquates » en la matière et contribuent à réduire le « vide juridique apparent » sur ce point.

Si à l'heure actuelle, les entreprises doivent avoir un comportement positif face à la protection de données personnelles qu'elles détiennent, le futur exige une implication plus active de la part du domaine juridique dans le contrôle et la mise en place de critères clairs en la matière, vu le manque de décisions juridiques cernant correctement la question. Puisque nous trottons lentement mais sûrement vers l'administration électronique, le gouvernement a aussi un rôle capital sur ce point. En effet, la mise en place des technologies de l'information au service de la modernisation des services publics, qui permettrait d'améliorer l'efficacité de l'action des

---

[181] Concernant la norme P3P consulter Roger CLARKE, « Platform for Privacy Preferences: An Overview », 2 Privacy Law & Policy Reporter 5, juillet 1998, p. 35-39, en ligne <http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html> et le site électronique du W3C en ligne <http://www.w3c.org>.

[182] Organisation mondiale de la propriété intellectuelle (O.M.P.I), WIPO Intellectual Property Handbook: Policy, Law and Use, « Enforcement of Intellectual Property Rights », publication no. 489 (E), Genève, 2001, par. 4.60, p. 218.

administrations de l'État et la qualité des relations avec les usagers, ne peut s'effectuer sans une attention accrue portée à la sécurité. Pour préserver la confiance des citoyens, la mise en place d'un cadre juridique complet en matière des droits et obligations dans la protection des informations personnelles et données sensibles est essentielle. La perspective d'une protection par la technique demande deux choses: foi dans la technologie et foi dans la responsabilité individuelle. Or, sans un cadre légal stable en matière de « mesures adéquates » pour la protection des données personnelles, la responsabilité individuelle ne peut être correctement garantie.

Pour terminer, dans un séminaire[183] donné à l'Université de Montréal, la question suivante a été lancée: sécurité juridique ou sécurité technique : Indépendance ou métissage ? Nous répondons à cette question par une courte histoire d'un avion et d'un passager. Lorsque le passager entre dans l'avion, il y a une distinction claire entre les deux éléments, l'humain d'un côté et la technologie de l'autre. Lorsque survient le décollage, le passager est surpris par la vitesse de l'avion et durant quelques secondes, ressent un inconfort, une sensation de perte de contrôle, la sortie de son environnement naturel. Malgré cela, lorsqu'il parvient à s'habituer à ce changement et peut profiter pleinement du voyage, de ces avantages. Le droit (ou la communauté juridique) a ressenti exactement la même chose lors du développement massif de l'informatique et de ses impacts dans la réalité juridique. Il a été déstabilisé par sa vitesse, sa nature et par la peur de la perte de contrôle, mais après un certain moment, il a dû s'adapter et ce n'est qu'après ce moment d'ajustement, qu'il a réalisé tous les avantages de la technologie et a pu en tirer partie. En aucun moment, le passager ne deviendra l'avion. Mais durant le voyage, les deux tirent des bénéfices et deviennent des partenaires et se complètent. Pour ceux qui ne prennent pas l'avion, l'opportunité d'explorer de nouveaux horizons, de nouvelles cultures, peut être perdue.

Plus nous allons pénétrer dans ce nouvel environnement où les décisions d'affaires sont automatisées, où les ordinateurs pensent et agissent pour notre compte et où ils deviennent omniprésents, plus de nouvelles bases de sécurité doivent être mises en place afin de constituer une infrastructure de sécurité stable pour l'avenir. Dans cet environnement, il est bien évident que les contrôles de sécurité sont une nécessité. Sans eux, chaque aspect de notre vie quotidienne, personnelle et professionnelle, serait exposé à être espionné ou modifié. La sécurité des informations demandera à être facilement comprise et mise en place. Elle va devenir aussi courante que la présence d'une serrure sur une porte ou le scellement de l'enveloppe. Ce sera une activité quotidienne faisant partie intégrante non seulement de notre vie, mais du droit.

[183] « Sécurité juridique et sécurité technique : indépendance ou métissage », séminaire organisé par le Programme international de coopération scientifique (CRDP/CECOJI), l'équipe de droit du cyberespace et du commerce électronique (CRDP) et le Centre d'étude et de coopération juridique internationale (CECOJI-CNRS), 30 septembre 2002.

Annexe I – Tableau de la qualification des renseignements nominatifs ou non nominatifs[*]

Renseignements nominatifs	Renseignements non nominatifs
❑ Nom ❑ Date de naissance ❑ Âge ❑ Adresse personnelle ❑ Numéro de téléphone ❑ Numéro d'assurance sociale ❑ Numéro de permis de conduire ❑ Rapport médical d'une personne ❑ Dossier médical ❑ Certificat médical ❑ Curriculum Vitae ❑ Sexe ❑ Grandeur ❑ Poids ❑ Couleur des cheveux ❑ Langue parlée ❑ Race ❑ Offre de services ❑ Chèque ❑ Relevé de carte de crédit ❑ Bordereau de dépôt ❑ Numéro de compte de banque ❑ Absence d'un travailleur ❑ Liste de rappel ❑ Rentes et fonds de pension des employés ❑ Lettre de rétrogradation ❑ Scolarité d'une personne ❑ Résultats de tests sanguins ❑ Date des vacances d'une personne ❑ Demande d'aide financière ❑ Dossier disciplinaire	❑ Opinion d'un fonctionnaire public dans l'exercice de ses fonctions ❑ Opinion d'une personne privée (quand le nom est masqué) ❑ Prénom seul ❑ Nom de la banque (avec qui l'individu fait affaires) ❑ Renseignements relatant les activités d'un travailleur (et non pas une évolution de rendement) ❑ Billet d'infraction (nom, adresse et numéro de téléphone sont masqués)

[*] Tableau tiré de l'ouvrage de Lecorre & ass., La protection des renseignements personnels, Yvon Blais, Montréal, 1995, p. 10.

Annexe II – Exemple de politique de sécurité

Cette politique porte sur la sécurité de l'information, des renseignements à caractère personnel détenus par L'ENTREPRISE (inclusivement le matériel informatique, logiciels et données) et tous les aspects de la confidentialité reliée aux objectifs et philosophie de l'ENTREPRISE. Elle comprend les responsabilités de l'ENTREPRISE prescrites par la législation en vigueur et normes internationales en matière de protections des renseignements personnels.

1. Définitions

<Définir tous les concepts généraux de la politique >

2. Portée

Cette politique s'applique à :

1. À toute personne ayant accès aux ressources informationnelles et aux systèmes informatiques de L'ENTREPRISE, notamment tout personnel au service de L'ENTREPRISE ou contracté par celle-ci, inclusivement le personnel temporaire ou occasionnel (associés, stagiaires,…), personnel d'entretient, cocontractants ou mandataires.

2. À tous les ordinateurs (ordinateurs, ordinateurs portatifs), périphériques et logiciels détenus par L'ENTREPRISE, utilisés dans les installations de L'ENTREPRISE ou à partir de l'extérieur, notamment du domicile.

3. À tous les serveurs, matériel informatique et logiciels essentiels au fonctionnement du réseau et des systèmes de l'information.

4. À tous les fichiers et informations contenant des renseignements personnels utilisés par ou concernant le personnel ou les cocontractants de L'ENTREPRISE.

3. Philosophie

Cette politique respecte les procédures qui promulguent la sécurité et la confidentialité sans toutefois restreindre la capacité d'accomplissement des tâches du personnel. Lors de la rédaction de cette politique, toutes les mesures de sécurité ont été étudiées et appliquées, en vertu d'une méthode d'une analyse des risques et leur application est faite en proportionnalité du risque encouru par L'ENTREPRISE.

Tous les risques significatifs ont été identifiés et analysés. Toutes les sections de cette politique ont été rédigées afin de garantir la sécurité et la confidentialité permettant l'accomplissement des activités de L'ENTREPRISE de manière pratique et efficace.

4. Révision de la politique

Cette politique sera révisée régulièrement, soit lors de la réévaluation annuelle des politiques de sécurité de L'ENTREPRISE ou plutôt si nécessaire. Tous seront informés de tout changement effectué à la politique. La politique est disponible sur un format électronique sur le réseau interne de L'ENTREPRISE et tous recevront une copie papier.

5. RESPONSABILITÉ

5.1. Responsabilités du personnel

L'ENTREPRISE a la responsabilité de garantir la sécurité globale et la confidentialité des renseignements personnels détenus par elle. Les membres du personnel, désignés par L'ENTREPRISE pour contrôler et diriger le personnel, sont responsables d'assurer la compréhension de la politique de sécurité par le personnel et doivent s'assurer que ces derniers respectent adéquatement la politique. Chaque employé est personnellement responsable de s'assurer que l'utilisation qu'ils font des ordinateurs, logiciels et renseignements personnels est conforme à la politique.

5.2. Formation et sensibilisation

1. Le responsable de la formation est chargé d'informer les nouveaux membres du personnel de l'existence de cette politique, de la leur transmettre une copie et répondre à leurs questions.

2. Tout le personnel signera une entente de confidentialité et la politique de sécurité lors de l'embauche au sein de L'ENTREPRISE.

3. Tout le personnel devra signer une déclaration concernant l'usage acceptable des ordinateurs et d'autres équipements informatiques lorsque l'usage est fait en dehors les locaux de l'entreprise.

4. Les séances de formation et de sensibilisation concernant la politique seront données annuellement ou plus fréquemment dans l'éventualité de changements dans la politique. Tout le personnel devra assister à ces séances et signer une déclaration de présence.

5.3. Cessation d'emploi

1. Lors du départ d'un membre du personnel, tous les codes de sécurité doivent être changés et toutes les clés, badges d'identité doivent être remis.

2. Toutes les procédures de départ doivent être enregistrées, complètes et signées.

5.4. Code de conduite

Tout le personnel de L'ENTREPRISE doit comprendre et respecter cette politique. Ils doivent se familiariser avec la législation en vigueur applicable et effectuer leurs fonctions conformément à la lettre et à l'esprit de cette politique et des textes législatifs. Toutes leurs actions, durant et après la fin de leurs fonctions au sein de l'entreprise, doivent faire preuve de diligence et de loyauté envers L'ENTREPRISE.

5.5. Manquement à la politique

1. Cette politique lie toutes les personnes ayant accès au système informatique et aux renseignements confidentiels détenus par L'ENTREPRISE.

2. Toute atteinte à cette politique sera considérée comme une offense disciplinaire grave. Toute atteinte sera rapportée. Toute personne qui suspecte une offense ou une situation pouvant provoquer une atteinte à la politique est encouragée à dénoncer la situation à la personne responsable.

3. L'accès ou la divulgation illicite et intentionnelle de renseignements de caractère personnel à des tiers non autorisés est un manquement disciplinaire pouvant mener au congédiement. Des poursuites pénales pourront être intentées, dépendamment de la nature de l'atteinte.

4. L'usage inapproprié de l'Internet ou du courrier électronique résultera toujours en des sanctions disciplinaires pouvant aller jusqu'au congédiement.

6. SÉCURITÉ

6.1. Sécurité physique

1. Tout le personnel de L'ENTREPRISE doit respecter les mesures de sécurité stipulées dans cette politique et dans les règlements internes de L'ENTREPRISE. Une copie de ces règlements internes est disponible sur le serveur de l'entreprise et dans la bibliothèque de sécurité.

2. Les locaux contenant le matériel informatique et renseignements à caractère personnel doivent être verrouillés lorsqu'ils ne sont pas utilisés et à la fin de chaque journée.

3. Les copies des clés de tous les locaux et cabinets d'archivage contenant des renseignements à caractère personnel doivent être gardées en lieu sûr.

6.2. Mots de passe

1. Tout utilisateur recevra un identificateur et un mot de passe.

2. Le mot de passe distribué devra être changé le plus tôt possible (en aucun cas plus de 30 jours après). Le mot de passe ne devra pas être évident et devra comporter un minimum de 6 caractères alpha numériques, minuscules ou majuscules.

    a. les mots de passe évidents ont ces caractéristiques :
        i. Mots contenus dans les dictionnaires (français ou étranger)
        ii. Mots de passe populaires :
        iii. Noms de famille, animaux, amis, collèges de travail, date d'anniversaire, numéros de téléphone ou autres informations personnelles, etc.
        iv. Termes ou noms d'ordinateurs, compagnies, marques, etc.
        v. Séquences numériques ou de lettres comme aaabbb, qwerty, zyxwvuts, 123321, etc.
        vi. Mots à l'inverse.
        vii. Tout mot courant procédé ou suivit d'un numéro (ex. secret1, 1secret). 4. La confidentialité des mots de passe doit être protégée et en aucun cas ne doit être divulguée.

3. Chacun est personnellement responsable de la confidentialité de son mot de passe. En aucun cas, le mot de passe ne doit être écris ou conservé sur le poste de travail. Chacun doit se souvenir de son mot de passe. L'utilisation de phrases pour se rappeler mot de passe est conseillée. Par exemple, « Voici un bon exemple pour se rappeler » peut être utilisé pour se souvenir du mot de passe : VuBepsR.

* Note : Cet exemple ne pourra plus être utilisé comme mot de passe.

4. Les usagers devront fermer toute session inutilisée durant une longue période.

5. Les écrans de veille (« screensaver ») doivent être protégés par des mots de passe de manière à sécuriser l'ordinateur lorsque le poste de travail est laissé pendant de courtes périodes. Ces mots de passe doivent respecter les mêmes critères décrits au point 2.

6.3. Copies de sauvegarde

1. Tous les fichiers contenant des renseignements à caractère personnel doivent être sauvegardés sur le serveur ou un support sécurisé.

2. Si un travail contenant des renseignements personnels est stocké temporairement sur un disque dur local (par exemple un ordinateur portatif ou un ordinateur personnel), il est de la responsabilité de l'utilisateur de s'assurer de l'enregistrement sur un support proportionné a lieu.

3. L'ENTREPRISE est responsable de procéder aux sauvegardes régulières des données gardées sur le réseau, serveurs, disques et de la conservation des copies de sauvegarde.

6.4. Protection contre les virus

1. Tous les ordinateurs sont protégés par des programmes antivirus reconnus.

2. Le personnel doit s'assurer que le programme antivirus et la liste de définitions des virus sont actualisés régulièrement (au moins une fois par semaine).

3. Le personnel doit respecter tous les avis émis par L'ENTREPRISE concernant les nouvelles menaces informatiques.

4. Le personnel utilisant des ordinateurs portatifs doit également respecter ces dispositions.

6.5. Matériel informatique

1. L'achat de matériel informatique (ordinateurs individuels, imprimantes, disques, etc.) à l'usage du personnel doit se faire par les personnes dûment autorisées par L'ENTREPRISE.

2. Dans chaque département, l'installation de l'équipement doit seulement être effectuée seulement le personnel autorisé.

3. Les personnes étrangères au service, qui une raison quelconque accèdent aux ordinateurs et au réseau de l'entreprise, doivent être sous la surveillance d'un membre du personnel autorisé et signer une déclaration d'utilisation, indiquant le nom, l'heure et la raison d'accès.

6.6. Logiciel

1. Dans chaque département, seules les personnes autorisées pourront installer ou désinstaller les logiciels.

2. Avant, l'installation ou la désinstallation d'un logiciel, une permission doit être obtenue auprès de la personne responsable. Aucun logiciel non autorisé ne devra être installé sur les ordinateurs ou sur le réseau de l'entreprise (inclus les services de messagerie, IRC, etc.).

3. Tout le logiciel installé sur les ordinateurs de L'ENTREPRISE doit être utilisé conformément à l'autorisation donnée par la personne responsable et l'utilisation doit se cadrer dans les activités normales de l'entreprise.

6.7. Travail hors site

1. L'équipement informatique peut seulement être sorti des lieux de travail avec l'autorisation de L'ENTREPRISE doit seulement être utilisé pour les activités normales de celle-ci.

2. Hors les locaux de L'ENTREPRISE, le personnel est responsable d'assurer la sécurité et de l'utilisation de l'équipement et du logiciel en leur possession.

3. Aucun ordinateur portatif ou autre équipement ne doivent être laissés sans surveillance dans les endroits publics. Ils devraient être maintenus dans une valise verrouillée et ne pas être laissés à la portée de quiconque.

4. Les supports magnétiques et les documents contenant de l'information confidentielle concernant L'ENTREPRISE ne doivent pas être laissés sans surveillance, même lorsqu'ils sont dans une valise verrouillée ou dans l'auto.

5. Une autorisation spécifique doit être donnée, par écrit, pour utiliser ou modifier l'information à caractère personnel hors les locaux de l'entreprise.

6. Le personnel doit s'assurer de la protection des données à caractère personnel en dehors des locaux de l'entreprise.

7. Tout logiciel installé sans autorisation est illégal et sera enlevé.

8. Toute sortie de logiciel de la bibliothèque de l'entreprise doit être contrôlée, enregistrée et signée.

7. POLITIQUE DE CONFIDENTIALITÉ

7.1. Demande d'accès aux renseignements de caractère personnel

L'ENTREPRISE doit informer toute personne qui en fait la demande de l'existence de renseignements personnels la concernant et lui permettre de les consulter. La personne concernée pourra contester l'exactitude et l'état complet des renseignements et y faire apporter les corrections appropriées. Cette demande et ces corrections devront être effectuées par la personne désignée par l'entreprise.

7.2. Conservation de renseignements personnels

1. Les renseignements personnels ne peuvent pas être utilisés pour un but différent de celui pour lequel ils ont été rassemblés. Les renseignements personnels ne seront conservés qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées.

2. Tous les renseignements personnels doivent être stockés sur un serveur sécurisé.

3. S'il est nécessaire de stocker temporairement renseignements personnels sur un disque dur local ou supports magnétiques (par exemple, disquette, Cédérom) il est la responsabilité de l'utilisateur de s'assurer que c'est mot de passe protégé et a enlevé ou a détruit comme bientôt possible.

4. Toutes les copies de sauvegarde et de documents contenant des renseignements personnels seront stockées dans un meuble d'archivage verrouillé, dans une salle verrouillée, lorsqu'ils ne sont pas utilisés.

7.3. L'utilisation de renseignements à caractère personnel

1. Toute collecte, constitution ou sauvegarde de données, dossiers ou documents contenant des renseignements personnels doit être discutée avec le département juridique de L'ENTREPRISE ou avec le responsable de la protection de la confidentialité de l'information.

2. Des détails de toutes les bases de données contenant des renseignements à caractère personnel doivent être transmis au responsable de la confidentialité de l'information.

3. Tout accès aux données personnelles sera accordé sur la base du critère de connaissance sélective et de privilèges minimaux. Toute personne aura accès aux seules données nécessaires pour l'accomplissement de leurs fonctions au sein de L'ENTREPRISE.

4. Tout accès aux données à caractère personnel doit être protégé par mot de passe.

7.4. Contractants externes

1. Tout transfert de données à caractère personnel avec des tiers doit être effectué dans le cadre d'un contrat écrit et dûment signé.

2. Tous les cocontractants doivent accepter de se conformer aux conditions de cette politique et offrir des garanties de sécurité suffisantes pour la protection des renseignements à caractère personnel.

3. Cette obligation couvre également la protection des supports électroniques et des documents papier contenant des renseignements personnels.

7.5. Destruction de données à caractère personnel

1. Tous les renseignements personnels désuets ou dont la conservation n'est plus nécessaire (sur support électronique ou papier) doivent être détruits.

2. Les documents contenant des renseignements à caractère personnel ou autres informations sensibles ne doivent pas être jetés dans les corbeilles à papier. Toute l'information confidentielle contenue sur papier devant être détruire doit être déchiquetée.

3. Pour assurer la protection adéquate des renseignements personnels, tous les supports magnétiques (disquettes, disques durs, bandes magnétiques, etc.) devant être conservés aux fins de réutilisation ou de réaffectation dans le même milieu doivent être purgés à l'aide de techniques d'effacement ou d'écrasement approuvées.

4. Si la confidentialité ne peut être garantie par le seul effacement, les supports doivent être détruits et en attendant de l'être, doivent être dûment protégés, notamment par un contrôle de l'inventaire.

7.6. Divulgation de renseignements de caractère personnel

1. Aucune information personnelle ne sera transmise à l'extérieur de L'ENTREPRISE, à moins qu'elles soient anonymisées ou que le destinataire emploie ces données pour de véritables buts de recherches ou d'audit et qu'il garantisse leur sécurité et les détruisent une fois qu'on a conclu son utilisation. Le destinataire doit signer une entente de confidentialité et de conformité de l'utilisation.

5. La communication d'informations personnelles par téléphone pourra être faite seulement après avoir des garanties suffisantes sur l'identité de la personne demandant l'accès.

2. Aucun renseignement personnel ne doit être laissé sur les répondeurs des téléphones.

3. Si l'information confidentielle doit être transmise par fax, le document sera identifié comme étant « confidentiel » et le destinataire doit être au courant quand la transmission aura lieu et doit se tenir prêt à recevoir l'information. La confirmation immédiate de réception doit être demandée.

4. Aucune information confidentielle ne devrait être transmise par courrier électronique ouvert. S'il est essentiel d'envoyer l'information confidentielle électroniquement, elle devrait être rendue illisible et protégée par mot de passe. Le mot de passe devrait être transmis directement par courrier ou par téléphone.

CONSEILS SUR LA POLITIQUE
Afin de mieux respecter cette politique de sécurité, suivre les conseils suivants :

- Avant de signer, lisez et assurez-vous de bien comprendre la politique de sécurité de L'ENTREPRISE. Si vous avez des doutes, dirigez-vous aux responsables de l'application de la politique.

- N'accédez pas à des informations à caractère personnel concernant les employés ou les clients de L'ENTREPRISE sans avoir une autorisation spécifique. En cas de doute, informez-vous auprès des personnes responsables.

- Informez les responsables lorsque vous suspectez une activité non autorisée ou un incident de sécurité. Vous êtes la première ligne de défense des ressources informationnelles de l'entreprise.

- Lorsque vous consultez, modifiez des fichiers contenant des renseignements personnels sur les employés ou des clients de L'ENTREPRISE sur un système informatique, assurez-vous d'enregistrer toutes les actions effectuées et spécifiez dans quel but ces modifications ont eu lieu.

DATE :
SIGNATURE :

Bibliographie

Table de législation

Lois fédérales canadiennes

Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21

Loi sur la protection des renseignements personnels et des documents électroniques, 1ère session, 36e législature, 46-47 Élizabeth II, 1997-1998, déposée le 1er octobre 1998 et réimprimée le 12 avril 1999

Lois québécoises

Charte des droits et libertés de la personne, L.R.Q., c. C-12

Code Civil du Québec, L.Q. 1991, c. 64

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1.

Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c.32.

Lois américaines

15 U.S.C.S. 1681.

Federal Privacy Act, 5 U.S.C. 552a, en ligne: <http://www.usdoj.gov/foia/privstat.pdf>.

US Department of Health and Human Services (DHHS), Code of Fair Information Practice Principles, 1973, en ligne: <www.ftc.gov/reports/privacy3/fairinfo.htm>.

US Department of Commerce, Safe Harbor Framework, Washington, juillet 2000, en ligne : <www.export.gov/safeharbor/sh_documents.html>.

US Department of Health and Human Services, Standards for Privacy of Individually Identifiable Healthn Information—Final Rule, Registre Féderal, 28 décember 2000; 65(250): 82462, codifé 45 *Code of Federal Register* 160 et 164, en ligne: <www.hhs.gov/ocr/hipaa>.

Textes juridiques internationaux

Conseil de l'Europe, Convention nº108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, en ligne : < http://conventions.coe.int/treaty/FR/Treaties/Html/108.htm >.

Conseil de l'Europe, Directive 95/46/CE du Parlement européen et du Conseil de l'Europe du 24 août 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E., 23 novembre 1995, n°. L.282, en ligne : < http://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html >

O.C.D.E., Lignes directrices régissant la protection de la vie privée et le flux transfrontalière de données à caractère personnel, Paris, 23 septembre 1980, en ligne : <http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html>

Lignes Directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information - Vers une culture de la sécurité, Recommandation du Conseil de l'O.C.D.E. du 25 juillet 2002, 1037ème session, en ligne : O.C.D.E. <www.oecd.org/pdf/M00033000/M00033183.pdf >.

O.C.D.E., Guidelines for the Security of Information Systems, 26 novembre 1992, en ligne: O.C.D.E. < http://www1.oecd.org/dsti/sti/it/secur/ >

O.C.D.E., Orientations for an action plan in the field of the security of information systems, J.O.C.E., 8.5.92, nº L123/22

O.N.U., Lignes directives pour la réglementation des fichiers informatisés de données à caractère personnel, 1989, en ligne : <www.unhchr/french/html/intlinst_fr.htm>.

Jurisprudence

Canadienne

R. c. Dyment, [1998] 2 R.C.S. 417.

Québécoise

Antonio Sergi c. Ville de Mont Royal, [1997] C.A.I. 198 (97 01 67)
Centre local de services communautaires de l'érable c. Lambert, [1981] C.S. 1077

Claude Stébenne c. Assurances générales des Caisses Desjardins, [1994] C.A.I. (94 03 66)
E. c. Office de la protection du consommateur, [1987] C.A.I. 350.
Godbout c. Longueuil (Ville de), J.E. 95-1848 (C.A.), p.17.
Myriam Ségal c. Centre de services sociaux de Québec, [1988] C.A.I. 315 (88 01 92); Reid c. Belzile, [1980] C.S. 717 (C.S. Québec)
The Gazette c. Valiquette, (1996), [1997] R.J.Q. 30 (C.A.).

Doctrine

Ouvrages

BENYEKHLEF, Karim, La protection de la vie privée dans les échanges internationaux d'information, Montréal, Éditions Thémis, 1992, p.49 et ss.

C.R.D.P., Loi concernant le cadre juridique des technologies de l'information (L.Q. 2001, c.32) – Texte annoté et glossaire, Centre de recherche en droit public, Université de Montréal, septembre 2001

CRUME, Jeff; Inside Internet Security: What Hackers Don't Want You To Know; London, Addison-Wesley, 2000

EMMEL, Vincent; Gestion des renseignements personnels, S.O.Q.I.J., 1997

GINGRAS, Patrick, Analyse juridique des méthodes de protection des renseignements personnels sur Internet, Mémoire de Maîtrise, Faculté des études supérieures, Université de Montréal, août 2000

HONDIUS, F., Emerging Data Protection in Europe, Amsterdam, North Holland/Elsevier, 1975

GRATTON, Pierre, La gestion de la sécurité informatique, Boucherville, Vermette, 1998

LINANT DE BELLEFONDS, Xavier et HOLLANDE, Alain; Pratique du droit de l'informatique : logiciels, systèmes multimédia & réseaux, Dalloz, Paris, 1998

MARTEL, Louise, et VÉZINA, Michel, La cyberPME et la gestion du risque, Ordre des CGA, Série performance financière, Montréal, Édition Guérin, 2000

MILLER, Charles, La sécurité des micro-ordinateurs et des réseaux locaux, Service de gestion de l'information des SGC et la Direction de la sécurité industrielle et ministérielle des SGC, Ottawa, Services gouvernementaux Canada, 1993

MILLER, Charles, Manuel de la sécurité de la technologie de l'information, Services gouvernementaux,Ottawa, 1993

PÉLADEAU, Pierrôt, LAPERIÈRRE, René ; Le droit sur la protection des renseignements personnels : étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international, Montréal, S.Q.U.I.J., 1986

PIPKIN, Donald, L., Sécurité des Systèmes d'Information, Campus Press, 2000

ROSZAK, Theodore, The Cult of Information, The Folklore of Computers and the True Art of Thinking, Phanteon Books, New York, 1986.

SCHNEIER, Bruce, Secrets & Lies: Digital Security in a Networked World, New York, John Willey, 2000

VENNE, Michel; Vie privée et démocratie à l'ère de l'informatique, Institut québécois de recherche sur la culture, Québec, 1994

Articles

ANDERSON, J.; «Computer Security Technology Planning Study», ESD-TR-73-51, US Air Force Electronic Systems Division, 1973, en ligne: National Institute of Standards and Technology < http://csrc.nist.gov/publications/history/index.html>

ANDERSON, Ross; «Why Information Security is Hard - An Economic Perspective»; Cambridge, University of Cambridge Computer Laboratory, 2001, en ligne < http://www.acsac.org/2001/papers/110.pdf>

Association des banquiers canadiens, « Confidentialité – Modèle de code : Pour protéger les renseignements personnels des clients des banques », Toronto, Association des banquiers canadiens, 1996

BENNETT, Colin, "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association", en ligne: <http://www.cous.uvic.ca/poli/bennett/research/cba.htm>

BENYEKHLEF, Karim, « Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes », (1992) 2 M.C.L.R. 149

BONHOMME, Robert et LESAGE, Laurent, « Le contrat de travail », Montréal, 2001, en ligne : avocat.qc.ca < http://www.avocat.qc.ca/affaires/iicontravail.htm >. (Dernière mise à jour: 15 février 2001)

CARLIN, F.M., « The Data Protection Directive: the introduction of common privacy standards », (1996) 21 European Law Review 65

CHASSIGNUEX, Cynthia, «La protection des données personnelles en France », Lex Electronica, Vol. 6, No. 2, hiver 2001, en ligne: Lex Electronica <http://www.lex-electronica.org/articles/v6-2/chassigneux.htm#introduction>

COMEAU, Paul André, « La vie privée : droit et culture », dans Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit, Les journées Maximillien-Caron 1995, Montréal Édition Thémis, 1995

Common Criteria for Information Technology Security Evaluation (CC), Version 2.1., août 2001, en ligne: Common Criteria <http://www.commoncriteria.org/>

EDIFICAS & IALTA, «Guide de l'archivage électronique sécurisé – Recommandations

pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations», Version V, 12 juillet 2000, en ligne : <www.edificas.org/ftp/Archivage/GuidArcv.PDF >

ERNEST & YOUNG, «Global Information Security Survey 2002», Ernest & Young LLP, mars 2002, en ligne: Ernest & Young < http://www.eyindia.com/pdfs/Info%20Security%20Survey%202002.pdf>
FARNSWORTH, F.; "What Do I Put in a Security Policy?", 2000, en ligne: Sans Institute <http://www.sans.org/infosecFAQ/policy/policy.htm >

GAUTRAIS, Vincent, « Aspects sécuritaires applicables au commerce électronique », dans Éric LABBÉ, Daniel POULIN, François JACQUOT et Jean-François BOURQUE (directeurs), Le guide juridique du commerçant électronique (rapport préliminaire), Montréal, Juris International, 2001, en ligne : < http://www.jurisint.org/pub/05/fr/guide_chap3.pdf >

GLENN, H. Patrick, « Le droit au respect de la vie privée », (1979) 39 R. du B. 879, 881.

HIGGINS, Huong Ngo; «Corporate system security: towards an integrated management approach», 5/7 [1999] Information Management & Computer Security 217-222

INTERPOL, « IT Security and Crime Prevention Methods», en ligne: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp

KABAY, Mich ; «Information Security Midyear 2002 Update: An Overview for Network Executives», 2002

LAWLOR, Allison, « Hundreds warned as data disappears », The Globe and Mail, 11 mars 2003, édition électronique en ligne: <http://www.globeandmail.com/>.

LEJEUNE, Bruno, « Aspects contractuels », dans Joël HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 225

LIVINGSTONE, G.; "How to Develop Your Company's First Security Baseline Standard", 2000, en ligne: Sans Institute <http://www.sans.org/infosecFAQ/policy/baseline.htm>

LLOYD, Ian, « An Outline of the European Data Protection Directive », (1996) 1 The Journal of Information, Law and Technology, en ligne: <http://elj.warwick.ac.uk/elj/jilt/dp/intros/>

LONGSTAFF, T.A., CHITTISTER, C., PETHIA, R. and HAIMES, Y.Y., «Are We Forgetting the Risk of Information Technology?», Computer, décembre 2000, p. 43-51

MASSE, M. "Information Security Policy for Administrative Information." Administrative Information Technology Services, University of Illinois. avril 1999. http://www.aits.uillinois.edu/security/securestandards.html

MATHIAS, Garance, « L'impact de la Directive européenne relative à la protection des données à caractère personnel sur les entreprises européennes et extra-européennes », juriscom.net, 10 janvier 2000, en ligne : juriscom.net <http://www.juriscom.net>.

Generally Accepted Systems Security Principles (G.A.S.S.P.), International Information Security Foundation (I^2SF), version 2.0, juin 1999, en ligne: <http://www.auerbach-publications.com/dynamic_data/2334_1221_gassp.pdf >.

OTUTEYE, Eben; «Framework for E-Business Information Security Management»; Fredericton, University of New Brunswick, mai 2001

OWENS, Richard and al., Privacy and Financial Services in Canada, mémoire prepare pour the Task Force of the Future of the Canadian Financial Services Sector, septembre 1998, en ligne: Canadian Financial Services Sector Task Force <http://www.finservtaskforce.fin.gc.ca>

POITRAS, Diane et DESBIENS, Lina, Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, textes annotés , S.O.Q.U.I.J., 1996

POULLET, Yves, « Réflexions introductives à propos du binôme « Droit-Sécurité », dans Joël HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 189

POULLET, Yves « Protection des données à caractère personnel et obligation de sécurité », dans Joël HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 207

REIDENBERG, Joel, « Privacy in the Information Economy: A Fortress or Frontier for Individual Rights », (1992) 44 Fed. Comm. L. J. 195.

SECURITEINFO, « Le grand livre de la sécuritéinfo.com », 18 février 2002, en ligne <http ://www.securiteinfo.com>

STANDAGE, Tom, « Securing the Cloud: a Survey of Digital Security », The Economist, 24 octobre 2002, en ligne: The Economist <http://www.economist.com>.

SWANSON, Marianne; "Guide for Developing Security Plans for Information Technology Systems", NIST SP 800-18, Gaithersburg, décember 1988, en ligbe: NIST <http://csrc.nist.gov/nistpubs/Planguide.PDF>

SWANSON, Marianne et GUTTMAN, Barbara; "Generally Acceptable Principles and Practices for Securing Information Technology Systems", NIST SP 800-14, Gaitherburg, septembre 1996, en ligne: NIST <http://csrc.nist.gov/nistpubs/800-14.pdf>
Securify Inc., «The Changing Nature of Information Security in a Networked World»; 2ième éd., août 2001

TURN, Rein, « Privacy Protection and Security in Transnational Data Processing Systems », [1980] 16 Standford Journal of International Law 67

VAN HOUTTE, Paul, « Les assurances », dans Joël HUBIN, Sécurité informatique, entre la technique et droit, C.R.I.D., Facultés universitaires, Notre-Dame de la Paix de Namur, Story-scientia, 1998, p. 241

VARIAN, Hal R.; «Managing Security Risks online, Economic Science Column», The New York Times, 1er juin 2000, en ligne: New York Times < http://www.nytimes.com/library/financial/columns/060100econ-scene.html>

VIRTA, Sirpa; «Local Security Management: Policing through networks», Policing An International Journal of Police Strategies & Management, Vol. 25 No. 1, 2002, pp. 190-200, en ligne: Emerald Insight <http://www.emeraldinsight.com/1363-951X.htm>

SANDERSON, Ethan, FORCHT, Karen; «Information security in business environments», 4/1 [1996] Information Management & Computer Security 32-37

SCHNEIER, Bruce; «Risk, Complexity, and Network Security»; Counterpane Internet Security, août 2001

SPINELLIS, D., KOKOLAKIS, S., et GRITZALIS, S., «Security requirements, risks and recommendations for small enterprise and home-office environments», 7/3 [1999] Information Management & Computer Security, 121-128

WARREN, Samuel D. et BRANDIES, Louis D., « The right of Privacy", 4 Harvard Law Review 193 (1890), en ligne: <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>.

Documents gouvernementaux

Canada

Centre de la sécurité des télécommunications, COMSEC Installation Planning (TEMPEST Guidance and Criteria) (CID/09/7A), 1983 (confidentiel),

Centre de la sécurité des télécommunications, Manuel de contrôle du matériel de sécurité des technologies de l'information (INFOSEC) (CID/01/10), version provisoire, septembre 1991 (Protégé A)

Centre de la sécurité des télécommunications, COMSEC Planning - TEMPEST Guidance (CID/09/7) (anglais seulement),

Conseil du Trésor du Canada, Politique de sécurité du gouvernement, Secrétariat du Conseil du Trésor du Canada, 1 février 2002

Conseil du Trésor du Canada, Politique du gouvernement du Canada sur la sécurité; (BT52-6/3)

CAVOUKIAN, Anne, Moving Information: Privacy and Security Guidelines, Information and Privacy Commissioner/ Ontario, juillet 1997, en ligne: Information and Privacy Commissioner <http://www.ipc.on.ca>

Ann CAVOUKIAN (Information and Privacy Commissioner), « Privacy & Security: Totally Devoted », conférence donnée à Toronto le 7 novembre 2002, en ligne: Commissaire à la Vie Privée <www.ipc.on.ca>.

G.R.C., Normes de sécurité technique dans le domaine de la technologie de l'information (NSTTI), Ottawa, Gendarmerie royale du Canada, août 1997, en ligne : http://www.rcmp-grc.gc.ca/tsb/pubs/standards/tssit97_f.pdf

Groupe de travail du Comité interministériel de la sécurité informatique, Informatique: normes et méthodes de sécurité à l'usage des ministères et des organismes du gouvernement], Ottawa, Gestion de l'information technologique, Conseil du trésor du Canada, 1986

G.R.C, Guide d'évaluation de la menace et des risques pour les technologies de l'information; GRC, novembre 1994

G.R.C., Norme pour la transmission et le transport de renseignements et de biens de nature délicate, Gendarmerie Royale du Canada, juin 1994

Industrie Canada, Protection de la vie privée et autoroute de l'information: Les options en matière de réglementation, Ottawa, 1996, en ligne : Industrie Canada <http://strategis.gc.ca/SSGF/ca00259.html>

Industrie Canada, The Protection of Personal Information: Building Canada's Information Economy and Society, Industrie Canada, janvier 1998, en ligne: Industrie Canada <http://strategis.ic.gc.ca.privacy>

Industrie Canada, Voluntary Codes: A Guide for their Development and Use, Industrie Canada, mars 1998

Information and Privacy Commissioner, "Privacy Models for the Private Sector", Information and Privacy Commissioner, Ontario, décembre 1996, en ligne: Information and Privacy Commissioner <http://www.ipc.on.ca>

Information and Privacy Commissioner, « Biometrics and Policing : Comments from a Privacy Perspective», Ontario, septembre 1999, en ligne : <http://www.ipc.on.ca/scripts/index>.

Commissaire à la vie privée du Canada, « Protection des renseignements personnels : vos responsabilités », Principe 7 : Mesures de sécurité, Ressource électronique en ligne : <http://www.privcom.gc.ca/information/guide_f.asp>.

Québec

Conseil du trésor du Québec, Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale québécoise, Sous-secrétariat aux inforoutes et aux ressources informationnelles, 23 novembre 1999, en ligne : < www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf >.

CHASSÉ, Max (analyste), Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information - À l'intention des ministères et organismes publics, v. 1.0, Commission d'accès à l'information, Gouvernement du Québec, décembre 2002 en ligne : <www.cai.gouv.qc.ca>.

PARADIS, Gaston, « Authentification dans les environnements de traitement distribués », Journal 13.3 Association des Professionnels de la Vérification et du Contrôle des Systèmes

d'information, Montréal, 2002 en ligne : APVCSI <http://www.apvcsi-montreal.ca/fr/publications/contact133f.htm>.

Allemagne

Federal Agency for Security in Information Technology (BSI), IT Baseline Protection Manual - Standard Security Safeguards, Bonn, Federal Agency for Security in Information Technology (BSI), juillet 2001, en ligne: BSI < http://www.bsi.bund.de/gshb/english/menue.htm>

Angleterre

COMMISSAIRE À L'INFORMATION, Guide to Data Protection Auditing, Gouvernement de l'Angleterre, en ligne : <http://www.dataprotection.gov.uk/dpaudit/download/>

ISSO 17799, A Code of Practice for Information Security Management (British Standard 7799), National Communications System, Public Switched Network Security Assessment Guidelines, September 2000

États-Unis

Department of Defense, Department of Defense Global Information Grid Information Assurance, Department of Defense Chief Information Officer Guidance and Policy Memorandum No, 6-8510, en ligne: <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>

National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, National Institute of Standards and Technology, septembre 1996, en ligne: NIST <http://csrc.nist.gov/publications/nistpubs/index.html>

National Institute of Standards and technology, Introduction to Computer Security: NIST Handbook, SP 800-12, octobre 1995

STONEBURNER, Gary, HAYDEN, Clark et FERINGA, Alexis; Computer Security: Engineering Principles for Information Technology Security (A Baseline for Achieving Security); SP 800-27, Gaithersburg, National Institute of Standards and Technology, juin 2001

STONEBURNER, Gary, HAYDEN, Clark et FERINGA, Alexis; Computer Security: Risk Management Guide for Information Technology Systems, SP 800-30, Gaithersburg, National Institute of Standards and Technology, janvier 2002

STONEBURNER, Gary; Computer Security: Underlying Technical Models for Information Technology Security, SP 800-33, National Institute of Standards and Technology, décembre 2001

SWANSON, Marianne; Computer Security: Security Self-Assessment Guide for Information Technology Systems, SP 800-26, National Institute of Standards and Technology, Gaithersburg, novembre 2001

US GAO, «Information Security Management: Learning From Leading Organizations», GAO/AIMD-98-68, US GAO, mai 1999, en ligne: US GAO < http://www.gao.gov/special.pubs/ai9868.pdf>

US GAO, «Information Security Management: Learning From Leading Organizations», GAO/AIMD-00-33, US GAO, novembre 1999, en ligne: US GAO <http://www.gao.gov/special.pubs/ai00033.pdf>

France

BOUCHET, Hubert, « Cybersurveillance sur les lieux de travail», Commission Nationale de l'Informatique et des Libertés, 5 février 2002 en ligne : <www.cnil.fr/thematic/docs/entrep/ cybersurveillance2.pdf >.

Union européenne

Commission des communautés européennes, Glossary of Information Systems Security, DGXIII, Programme INFOSEC/s2001, 1993

Commission des communautés européennes, Risk Analysis Methods Database, DGXIII, Programme INFOSEC/s2014/WP08, 1993

Conseil de l'Europe, « U.S. Safe Harbour Arrangement, draft discussion documents », 19 novembre 1999, en ligne : <http://www.europa.int/comm/internal_market/en/dataprot/news/harbour2.htm>.

Union Européenne, «Network and Information Security: Proposal for a European Policy Approach», COM (2001) 298 final, Bruxelles, 6 juin 2001, en ligne: Commission Européenne < http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0298en01.pdf>

Articles techniques (White papers)

BASELINE Software Inc., Information Security Policies Made Easy, Version 4, CIPR-10, Baseline Software Inc., juillet 1996

Control Data Inc., Why Security Policies Fails?, Control Data Inc., 1999, en ligne: Control Data <http://www.cdc.com>

DATATILSYNET, Information Security Guidelines for the processing of personal information, TR-100E: 1998, Data Inspectorate (Datatilsynet), avril 1999

HUTTON, Nick; Security and the Internet; Fairfax, UUNET Technologies Inc., 1999

Entreprise Management Associates, «An Introduction to Network Security: Ensuring the Safety of Your Network»; mai 2000

POLIVEC, Security Policy Development Process, Polivec, Colorado Springs, 2002

SUN MicroSystems, Protection From Within: A Look at Intranet Security Policy and Management; Paulo Alto, SUN MicroSystems, 1999

ZoneLabs, Small Business Internet Security; San Francisco, ZoneLabs, 1999