

## La protection de l'information

Hélène Dorion

Volume 23, Number 2, June 1992

URI: <https://id.erudit.org/iderudit/1057470ar>

DOI: <https://doi.org/10.7202/1057470ar>

[See table of contents](#)

Publisher(s)

Éditions Wilson & Lafleur, inc.

ISSN

0035-3086 (print)

2292-2512 (digital)

[Explore this journal](#)

Cite this article

Dorion, H. (1992). La protection de l'information. *Revue générale de droit*, 23(2), 197–234. <https://doi.org/10.7202/1057470ar>

Article abstract

After the *Stewart* case, the question of the protection of information was raised again. This issue is not new, but automation of data processing gives to it another dimension.

The evolution of such new automated technological processes disrupts the framework and management of the post-industrial society. Although it represents unexpected potential to generate, to store and to process whatever information, these new technologies are alarmingly vulnerable. These new devices, which are increasingly prevalent, control all the spheres of human activity; from the most sophisticated scientific businesses, to the diverse administrative actions, to miscellaneous daily operations. Information is disclosed by institutions and individuals to these vulnerable systems without too much suspicion.

The debate is not reduced to simple oppositions of moral, political, social or economical interests. For it is the management of all the framework of our civilization which is transformed, and without any technical progress to control this evolution, it is the balance of that framework which is jeopardized. In addition to having important impacts on the functioning of business and the States, these changes raise new problems as to the traditional rules of law.

The law is therefore challenged. This phenomenon raises up several questions. In the present stage of this astonishing evolution, what tasks can be performed by the traditional rules of law? What status, what protection must be granted to information? From which concepts, which theories, the reflection must be initiated to reform the law in this field?

---

## La protection de l'information\*

HÉLÈNE DORION

Avocate, Ottawa

### RÉSUMÉ

*Suite à l'arrêt Stewart, la question de la protection de l'information fut relancée. Cette question n'est pas nouvelle mais l'informatisation lui donne une tout autre dimension. L'évolution des nouvelles technologies informatiques bouleversent l'infrastructure et la gestion de la société post-industrielle. Bien que représentant des potentiels inespérés de générer, d'entreposer et de traiter l'information quelle qu'elle soit, ces nouvelles technologies sont d'une vulnérabilité inquiétante. Ces nouveaux dispositifs, dont la présence se fait de plus en plus envahissante, contrôlent pourtant toutes les sphères de l'activité humaine, des entreprises scientifiques les plus sophistiquées, en passant par les diverses actions administratives, jusqu'aux opérations quotidiennes les plus variées. À ces systèmes vulnérables, institutions et individus confient sans trop de méfiance toute sorte d'information. Le débat ne se réduit pas à de simples oppositions d'intérêts*

### ABSTRACT

*After the Stewart case, the question of the protection of information was raised again. This issue is not new, but automation of data processing gives to it another dimension. The evolution of such new automated technological processes disrupts the framework and management of the post-industrial society. Although it represents unexpected potential to generate, to store and to process whatever information, these new technologies are alarmingly vulnerable. These new devices, which are increasingly prevalent, control all the spheres of human activity; from the most sophisticated scientific businesses, to the diverse administrative actions, to miscellaneous daily operations. Information is disclosed by institutions and individuals to these vulnerable systems without too much suspicion. The debate is not reduced to simple oppositions of moral, political, social or economical interests. For it is the management of all the framework of our civilization which is transformed, and without any*

---

\* Ce texte est une version légèrement modifiée d'un rapport de recherche présenté à la Commission de réforme du droit du Canada. L'auteure désire remercier la Commission, plus particulièrement M<sup>e</sup> François Handfield, secrétaire de la Commission, de lui avoir permis de réaliser cette recherche.

*moraux, politiques, sociaux, ou économiques car c'est la gestion de toute l'infrastructure de notre civilisation qui est transformée et sans progrès techniques pour contrôler cette évolution, c'est l'équilibre de cette infrastructure qui est mis en péril. En plus d'avoir des impacts importants sur le fonctionnement des entreprises et des États, ces changements soulèvent de nouveaux problèmes quant aux règles traditionnelles de droit.*

*Le droit est donc interpellé, ce phénomène suscitant de nombreuses interrogations. Dans la phase actuelle de cette évolution stupéfiante, de quelle tâche les règles de droit traditionnelles peuvent-elles s'acquitter? Quel statut, quelle protection faut-il accorder à l'information? À partir de quels concepts, de quelles théories, la réflexion peut-elle s'amorcer pour réformer le droit dans ce domaine?*

*technical progress to control this evolution, it is the balance of that framework which is jeopardized. In addition to having important impacts on the functioning of business and the States, these changes raise new problems as to the traditional rules of law.*

*The law is therefore challenged. This phenomenon raises up several questions. In the present stage of this astonishing evolution, what tasks can be performed by the traditional rules of law? What status, what protection must be granted to information? From which concepts, which theories, the reflection must be initiated to reform the law in this field?*

---

## TABLE DES MATIÈRES

Introduction .....	199
I. Le droit actuel .....	200
A. Historique .....	200
B. La conception classique du droit de propriété et de la protection pénale contre le vol .....	202
1. Pays d'Europe continentale .....	203
2. Pays du Commonwealth .....	205
3. États-Unis .....	208
4. Canada .....	211
II. La nécessité d'une réforme .....	216
A. L'importance du rôle de l'information .....	217
B. La nature de l'information .....	218
1. Les diverses approches .....	218
2. Le caractère confidentiel .....	222
C. La protection de l'information .....	223
1. Quelle information faut-il protéger? .....	223
2. Quel droit devrait assurer la protection de l'information? .....	224

III. L'information et le droit criminel .....	227
A. Les objets du droit pénal .....	227
1. Le préjudice à autrui .....	228
2. Le tort à la société .....	228
B. La mise en œuvre du droit pénal et le respect de nos valeurs fondamentales...	229
C. La contribution du droit criminel .....	230
D. La création d'infractions .....	231
1. Les infractions relatives à des espèces particulières de biens .....	232
2. Le statut des nouvelles incriminations .....	232
Conclusion .....	233

## INTRODUCTION

La technologie évolue à un rythme effarant, elle a bouleversé les sociétés modernes en envahissant tous leurs secteurs. Cet envahissement ne se fait pas sans heurts. Le développement des technologies révèle des inadéquations des règles de droit traditionnelles face aux problèmes de droit que soulève l'informatisation. Entre autres incidences juridiques, les technologies modernes relancent la question de la protection de l'information. Si désormais la protection de l'information soulève autant de questions, c'est qu'elle échappe de plus en plus à notre contrôle. Les nouvelles technologies se traduisent d'un point de vue technique, par un accroissement du volume et surtout, de la fluidité de l'information, qui a pour conséquence une multiplication des risques d'atteintes. En effet, bien qu'elles présentent des potentiels inespérés de traitement, d'entreposage, voire même de création d'informations, ces technologies s'avèrent d'une vulnérabilité inquiétante. L'ampleur de ce nouveau phénomène interpelle le législateur. Le droit doit s'adapter à cette nouvelle réalité.

Si la plupart des pays ont réagi à ce phénomène en légiférant en matière d'informatique, les lois destinées à réprimer l'utilisation non autorisée d'ordinateurs, le détournement, l'interception, la falsification et la destruction des données, ne constituent pas une protection toujours adéquate et cohérente contre ces types d'atteinte. Les législateurs ont créé un régime juridique spécial en encadrant le domaine de l'informatique pour tenter de contenir les proportions alarmantes que prennent les crimes reliés à l'informatique. C'est un droit spécial qui s'est composé au gré des circonstances, sans distinction entre les questions ayant trait à l'information en général et celles qui traitent des données informatiques.

La décision de la Cour suprême du Canada dans l'affaire *Stewart* a relancé la question du statut juridique de l'information. L'affaire *Stewart* posait le problème du vol d'information, sans soustraction d'un support matériel quelconque. La Cour suprême a établi que l'information ne pouvait faire l'objet du crime de vol tel que défini à l'article 322 du *Code criminel*. Bien que la Cour suprême ait tranché la question au niveau judiciaire, il n'en demeure pas moins que la question n'est pas réglée pour autant. Dans l'arrêt *Stewart*, le juge Lamer a d'ailleurs formulé plusieurs questions sur lesquelles il invite le législateur à réfléchir : quelle définition précise devrait être attribuée aux termes « renseignements confidentiels »? La confidentialité est-elle fonction de l'intention du prétendu

propriétaire ou dépend-elle de certains critères objectifs? À quels moments les renseignements perdent-ils leur caractère confidentiel de sorte qu'ils échappent au droit criminel? La protection du droit criminel doit-elle être accordée seulement aux renseignements qui sont censés avoir une valeur commerciale quelconque?

## I. LE DROIT ACTUEL

### A. HISTORIQUE

Les codes criminels de tous les pays protègent de façon prédominante les objets corporels et visibles. La protection de l'information et des objets incorporels bien qu'existant autrefois (secrets d'État, secrets professionnels, brevets, droits d'auteur et secrets commerciaux) n'a pas joué un rôle prédominant avant le milieu du XX<sup>e</sup> siècle.

Pour les secrets commerciaux, le champ de protection a évolué au gré des changements de philosophie politique et économique. Durant la période de mercantilisme qui dominait l'économie anglaise au cours de la période de 1500 à 1760, il existait des lois protégeant les secrets commerciaux, dont certaines très sévères. Par la suite, le déclin du mercantilisme et l'émergence du laissez-faire expliqueraient l'absence de lois criminelles spécifiquement reliées aux secrets commerciaux et le développement de solutions de droits civils aux États-Unis comme en Angleterre. Le laissez-faire favorisait une diminution de l'intervention de l'État au profit de solutions privées.

Bien que dans une position dominante depuis la Première Guerre mondiale, les États-Unis ont adopté leurs premières lois criminelles protégeant les secrets commerciaux dans les années 1960 à cause de la présence de nations industrielles rivales comme l'Allemagne et le Japon<sup>1</sup>.

Au cours des dernières décennies, la situation a évolué rapidement. Le passage d'une société industrielle à une société post-industrielle, l'importance croissante de l'information pour les domaines de l'économie, la culture et la politique, ainsi que l'évolution de la technologie informatique, ont suscité des remises en question et des nouvelles attentes à l'endroit du « droit de l'information ». On parle de « changement de paradigme » des objets corporels aux objets incorporels qui a atteint le droit criminel substantif dans le cadre de diverses vagues de législation concernant l'informatique<sup>2</sup>.

Une première vague de réforme du droit dans la plupart des systèmes judiciaires occidentaux est apparue dans le domaine de la protection de la vie privée dans les années 1970 et 1980. Cette législation arrivait en réaction à de nouvelles atteintes à la vie privée que causaient les possibilités grandissantes de collecte, de storage et de transmission des données grâce aux nouvelles technologies. De nouvelles lois pour protéger les données concernant la vie privée des citoyens furent adoptées et de nouvelles réglementations administratives, civiles et pénales furent mises en place.

1. F. FETTERLY, « Historical Perspectives on Criminal Laws Relating to the Theft of Trade Secrets », (1979) 25 *Bus. Lawyer* 1535, pp. 1538 et s.

2. U. SIEBER, *General Report on « Computer Crime »*, International Academy of Comparative Law — XIIIth International Congress-Montréal, 1990, p. 11.

Au début des années 1980, une seconde vague de réforme des lois visait la répression des crimes économiques au moyen d'ordinateur. De nouvelles législations devenaient nécessaires puisque les dispositions criminelles qu'on leur appliquait protégeaient exclusivement les objets physiques, tangibles et visibles contre les crimes classiques. Pourtant, les nouvelles formes de crime au moyen d'ordinateur ne portaient pas atteinte uniquement aux objets au sens traditionnel du terme sous la forme d'un nouveau medium (comme un dépôt d'argent consolidé dans des relevés informatiques), mais aussi à des objets intangibles (comme des programmes d'ordinateur) et créaient de nouvelles méthodes de commission (manipuler un ordinateur plutôt que tromper une personne). La plupart des pays ont adopté des lois pour lutter contre les crimes économiques reliés à l'ordinateur.

On relève les premiers cas de « crime informatique » dans les années 1960. Ces cas étaient reliés principalement à la manipulation, au sabotage, à l'espionnage et à l'utilisation des systèmes d'ordinateur. Au cours des années 1970, on assiste à des crimes informatiques spectaculaires tels que les affaires *American Equity Funding*, *German Hersatt*, *Swedish Volvo*<sup>3</sup>.

Au cours des années 1980, il est apparu que le crime informatique n'était plus uniquement limité au crime économique, mais prenait aussi d'autres formes telles que le truquage d'ordinateurs d'hôpitaux ou autres ordinateurs contenant des renseignements confidentiels, ces dernières violations et le crime informatique étant à l'origine traités de façon distincte. À ces violations vinrent s'ajouter le piratage de programmes, le truquage de guichets automatiques et l'emploi abusif de systèmes de télécommunication.

Présentement, on craint surtout le *hacking*<sup>4</sup>, les virus informatiques et la *desktop forgery*<sup>5</sup>. Le danger que représente le *hacking* devint particulièrement éminent en 1989 quand des poursuites criminelles en République Fédérale Allemande permirent d'identifier des *hackers* allemands qui utilisaient des réseaux de données internationaux pour obtenir de l'information dans des systèmes d'ordinateurs américains, anglais et d'autres pays étrangers, dans le but de vendre le fruit de leurs « récoltes » aux services secrets soviétiques. De même, en novembre 1988, la menace des virus informatiques devint évidente lorsqu'un étudiant américain introduisit un virus informatique dans le réseau « Internet » qui, en l'espace de quelques jours affecta et paralysa environ 6 000 ordinateurs de ce réseau.

Ces affaires d'envergure transnationale illustrent les dimensions internationales du crime informatique et justifient les activités d'organisations internationales dans ce domaine<sup>6</sup>.

En l'absence de législation d'ensemble, jusqu'aux lois ou amendements législatifs relatifs à l'informatique, on était obligé de se rabattre sur les incriminations traditionnelles du droit pénal (vol, escroquerie, méfait, fraude, fabrication de faux, etc.) pour tenter de lutter contre un fléau qui prenait des proportions alarmantes et qui devenait très coûteux pour les personnes et entreprises qui exploitent un système informatique et pour la collectivité en général. Or, ce droit pénal

3. Voir *id.*, p. 5.

4. Le *hacking* est une intrusion audacieuse, pas toujours malicieuse, dans des systèmes et des réseaux d'ordinateurs dont l'accès est interdit. Ce genre d'intrusion a souvent pour but de commettre différentes formes de crimes informatiques et peut avoir des conséquences fâcheuses comme le déclenchement d'une guerre nucléaire...

5. Falsification sophistiquée de documents comme les certificats de valeurs, passeports et factures de cartes de crédit.

6. U. SIEBER, *op. cit.*, note 2, p. 6.

traditionnel a vite montré ses limites et s'est montré impuissant à assurer la répression des agissements frauduleux en matière de technique informatique. La nécessité et l'urgence de la protection systématique contre la fraude informatique devenaient de plus en plus évidentes. Des mesures législatives s'imposaient donc de manière impérative, mais leur mise en place soulevait de délicats problèmes qui faisaient hésiter nombre de pays : fallait-il axer la protection sur le contenant (le système informatique) ou le contenu (l'information traitée par le système) ou plutôt adopter une conception mixte qui consiste à traiter la protection du système seulement, comme le moyen d'assurer celle des produits de celui-ci, de sorte que les incriminations supposent toutes, la réunion de l'atteinte aux produits en même temps qu'au système<sup>7</sup>?

On parle maintenant d'un « droit criminel de l'information ». Cette nouvelle approche nous force à constater que l'analyse juridique des objets corporels et des objets incorporels (information) diffèrent considérablement : premièrement, les objets corporels sont des biens susceptibles d'une exclusivité de fait, d'un droit privatif réservé à un ou des individus alors que l'information serait plutôt un bien public qui, dans une société libre devrait nécessairement circuler de façon libre et ne devrait donc pas faire l'objet d'un droit d'exclusivité de la même manière que les objets corporels. Ce principe de base de libre circulation de l'information n'est pas seulement nécessaire pour le système économique et politique mais est indispensable aussi pour la transmission et le progrès de l'informatique dans les pays en voie de développement; deuxièmement, la protection des objets corporels vise à préserver les intérêts économiques de leur propriétaire tandis que la protection de l'information vise non seulement à préserver les intérêts économiques de son détenteur, mais doit aussi préserver les intérêts des personnes concernées par le contenu de l'information — de nouvelles questions surgissent sur cet aspect de la protection de la vie privée<sup>8</sup>. En conséquence de ces particularités spécifiques, il est évident qu'un régime juridique de l'information ne peut dériver d'une analogie avec les principes s'appliquant aux objets corporels, mais que l'on doive plutôt l'élaborer séparément.

L'historique et l'analyse comparative de la protection des biens corporels et de certains biens incorporels permettent de démontrer que les dispositions légales conçues en fonction du droit de propriété des objets corporels ne peuvent pas être appliquées simplement à la protection de l'information.

## **B. LA CONCEPTION CLASSIQUE DU DROIT DE PROPRIÉTÉ ET DE LA PROTECTION PÉNALE CONTRE LE VOL**

On peut suggérer que la question fondamentale qui se pose est : L'information, indéniablement de valeur patrimoniale (au moins potentiellement), mais de nature immatérielle, est-elle susceptible d'une des atteintes juridiques au patrimoine et notamment de la plus fondamentale d'entre elles : le vol?<sup>9</sup>

7. Comme on l'a fait aux États-Unis dans le *Counterfeit Access Device and Computer Fraud and Abuse*, 18 U.S.C.A. 1030 et au Canada dans le *Code criminel* (articles 342(1) et 430(1.1)).

8. Voir M. VENNE, « À la défense de la vie privée contre Big Brother » dans *Le Devoir*, mardi le 10 février 1992, p. 11.

9. B. BERGMANS, « Le vol d'information en droit comparé », (1988) 68 *R.D.P.C.*, p. 905.

Jusqu'à quel point l'acquisition d'information incorporelle (celle qui est prélevée sans son contenant) peut-elle être couverte par les dispositions pénales traditionnelles de vol, vol simple (*larceny*) et de détournement (*embezzlement*) qui s'appliquent de façon relativement facile à l'appropriation de l'information corporelle (celle qui est enlevée avec son contenant)?

La plupart des pays hésitent à appliquer les dispositions traditionnelles de vol et de détournement à la soustraction d'information parce que ces lois requièrent généralement que la propriété corporelle soit prise avec l'intention d'en priver la victime de façon permanente<sup>10</sup>. Cependant, dans certains pays, l'application des dispositions traditionnelles de vol et de détournement semblent possibles, du moins dans certains cas<sup>11</sup>.

Si la Cour suprême du Canada a refusé d'étendre à l'information la protection criminelle contre le vol, d'autres hauts tribunaux sont arrivés à des décisions différentes sur cette question. Avant de traiter de façon plus exhaustive de l'état du droit qui prévaut au Canada dans ce domaine, il nous a semblé utile d'examiner d'abord, brièvement, certaines dispositions législatives étrangères, des décisions relatives à cette question ainsi que des observations qu'elles ont suscitées qui nous ont semblé particulièrement intéressantes.

## 1. Pays d'Europe continentale

En France, la Cour de cassation n'a jamais retenu le vol relativement à l'information elle-même. Cette cour retient seulement le vol du support de l'information. Ainsi, selon elle, constitue un vol de document le fait de s'« approprier » celui-ci pendant le temps nécessaire pour en faire une photocopie<sup>12</sup>. Dans le même ordre d'idée, la même juridiction a qualifié par ailleurs de recel la détention de la photocopie d'un document volé<sup>13</sup>. La doctrine dominante soutient une opinion conforme à la position de la Cour de cassation : le texte d'incrimination français<sup>14</sup> ne permet pas d'admettre le vol d'information<sup>15</sup>.

À l'instar de la plupart des autres pays, le législateur français a légiféré dans le domaine de l'informatique en accordant d'abord une protection pénale aux renseignements personnels contenus sur des fichiers informatiques en adoptant les articles 41 à 44 de la *Loi n. 78-17* qui prévoient une peine maximale de cinq années d'emprisonnement. En 1988, la *Loi n. 88-19* prévoyait des dispositions relatives à la fraude informatique modifiant le Code pénal (articles 462-2 à 462-9). Cette loi couvre de façon plus vaste les agissements frauduleux imputables à l'informatique.

10. Voir, pour la Belgique, article 461 du Code pénal; pour l'Allemagne, articles 242, 246 du Code pénal; pour la Grèce, articles 372 et 375 du Code pénal; pour Israël, article 383 du Code pénal, pour l'Italie, articles 624 et 646 du Code pénal.

11. Voir, pour les Pays-Bas, article 321 du *Code pénal*.

12. Cass. Ch. Crim., 8 janvier 1979, D.1979, p. 509.

13. Cass. Ch. Crim., 12 janvier 1981, *Bull. Crim.*, n° 15.

14. Art. 379 du Code pénal français : « Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol »; Encyclopédie Dalloz, *Éléments constitutifs du vol simple*, Droit pénal, Vol. V, art. 1 et 2 : le concept de vol implique « la soustraction de la chose d'autrui ».

15. Voir J. DEVEZE, « Le vol de biens informatiques », *Sem. jur.* (Doc.) 1985, I, 3210, n°s 11 et s.; R. GASSIN, « Le droit pénal de l'informatique », *D.* 1986, *Ch.*, p. 35.



Aux Pays-Bas, le concept de « bien susceptible d'appropriation » dans les articles 310 (vol) et 321 (détournement) du Code pénal ne vise pas seulement les biens matériels mais a été étendu à tout élément patrimonial. Le bien ne doit pas nécessairement avoir une valeur économique, il suffit qu'il ait une valeur subjective<sup>16</sup>.

Les droits et les œuvres de l'esprit (droit d'auteur, brevet) ne sont pas considérés comme « biens »<sup>17</sup>.

Le 27 novembre 1983, la Cour d'Arnhem a jugé que les données informatiques sont un bien au sens de l'article 321 et condamné l'inculpé pour détournement. La Cour a estimé que les données informatiques constituent un bien parce qu'elles sont cessibles, reproductibles et disponibles, et qu'en outre, elles possèdent une valeur économique: qu'il y a appropriation parce que le copiage a entraîné un accroissement du patrimoine de l'inculpé au détriment de la société et parce que l'inculpé pouvait disposer des données en tant que maître absolu<sup>18</sup>.

La jurisprudence belge a admis le vol de données informatiques<sup>19</sup> mais le raisonnement qu'elle a adopté et la solution qu'il implique sont loin d'avoir épuisé la problématique. Par exemple, la reproduction de références contenues dans un catalogue, sans soustraction d'un objet corporel, ne constitue pas un vol<sup>20</sup>.

Par ailleurs, la Cour de cassation avait affirmé dans une décision du 25 janvier 1956 :

S'il est permis au juge répressif d'appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de pressentir à l'époque de la promulgation de la disposition légale, c'est à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de l'infraction.<sup>21</sup>

La volonté du législateur de considérer le copiage de données comme un vol est-elle manifeste? Selon l'auteur Vandenberghe, cette volonté n'est pas manifeste car autrement, les droits de propriété intellectuelle n'auraient pas été introduits. Pour cet auteur, c'est qu'une valeur économique qui est atteinte, une valeur économique que l'on s'attribue ou que l'on emporte. « Le vol d'une valeur économique, voilà qui ouvre d'intéressantes perspectives »<sup>22</sup>.

En Allemagne, comme l'information (y compris les données informatiques) n'est pas une chose corporelle, elle ne peut donner lieu à une condamnation pour vol ou détournement<sup>23</sup>. Ainsi, lorsqu'on reproduit ou copie un document, il n'y aurait que vol d'usage non punissable, puisqu'on laisse la chose au propriétaire même si on l'enlève, parce qu'on la remet ultérieurement<sup>24</sup>. Et

16. HR 6 janvier 1908, W 8648; HR 28 avril 1930, N.J., 1930, p. 1105; HR 27 novembre 1939, N.J., 1940, n° 219 dans B. BERGMANS, *loc. cit.*, note 9, p. 912.

17. HR 9 novembre 1931, N.J., 1932, p. 270 dans B. BERGMANS, *ibid.*

18. Hof Arnhem, 27 octobre 1983, N.J. 1984, n° 80. Version française dans B. BERGMANS, *ibid.*

19. Appel Anvers, 13 décembre 1984, *Droit de l'informatique*, 1986/2; p. 93, note de G. VANDERBERGHE.

20. Trib. corr. Liège, 26 juin 1987, *J.L.M.B.*, 1987, p. 1196.

21. Cass., 25 janvier 1956, *R.P.D.B.*, 1955-56, 668-669, cité dans G. VANDERBERGHE, *op. cit.*, note 19, pp. 94-95.

22. G. VANDERBERGHE, *id.*, p. 95.

23. K. TIEDEMANN, « Fraude et autres délits commis à l'aide d'ordinateurs électroniques », (1984) *Rev. dr. pén. crim.*, pp. 611 et ss.

24. Leipziger Kommentar, 8 Aufl. (de Gruyter, Berlin 1958), p. 302: « un secret de commerce n'est pas une chose », dans B. BERGMANS, *loc. cit.*, note 9, p. 907.

celui qui enlève un dossier uniquement pour le consulter n'est pas punissable parce qu'il n'agit pas avec une intention d'appropriation<sup>25</sup>.

Un tribunal aurait admis, dans un cas où des bandes magnétiques contenant des listes d'adresses ont été soustraites, copiées et revendues, l'appropriation de la valeur incorporée dans ces bandes au sens des articles 242 (vol) et 246 (détournement) du Code pénal<sup>26</sup>.

D'autres dispositions pénales existent en la matière. Ainsi, en matière d'espionnage informatique, le Code pénal réprime la violation et l'exploitation des secrets privés d'autrui (relatifs notamment à sa vie privée, à son industrie ou à son commerce)<sup>27</sup>. Certaines dispositions traitent aussi des secrets d'État, mais ces dispositions ne visent que les membres de certaines professions ou les titulaires de certaines fonctions ou charges auxquels un secret aurait été confié<sup>28</sup>.

Le Code pénal allemand réprime la violation du caractère confidentiel des paroles par enregistrement, et son utilisation, la violation du caractère confidentiel d'une lettre close, de tout autre document, ou de tout autre support destiné à la transmission de la pensée, clos ou protégé par un contenant clos, et l'espionnage informatique<sup>29</sup>.

Le Code pénal autrichien contient de nombreuses dispositions relatives à la protection du secret, certaines sanctionnant la trahison, la divulgation, l'espionnage et le service de renseignements de secrets d'État<sup>30</sup>, d'autres, la violation de secrets professionnels, du secret de la correspondance et la suppression de lettres, la violation du secret des télécommunications et l'emploi abusif d'appareils d'enregistrement ou d'écoute<sup>31</sup>.

Enfin, les secrets commerciaux et de fabrication sont protégés par des dispositions du Code pénal en matière de secret commercial et d'espionnage<sup>32</sup>.

## 2. Pays du Commonwealth

Même si l'article 4 du *Theft Act*<sup>33</sup> de 1968 inclut les biens intangibles dans les objets pouvant être volés, les commentateurs ont reconnu que la définition du vol s'y applique difficilement : ainsi, même si, par exemple, des secrets de commerce forment un bien intangible, et peuvent être appropriés de manière malhonnête, cela n'a pas pour effet d'en priver le titulaire : il ne perd qu'un avantage attaché au secret, c'est-à-dire son exclusivité, de sorte que, sauf circonstances exceptionnelles, des secrets ou de l'information ne peuvent être volés<sup>34</sup>.

25. *Ibid.*

26. U. SIEBER, *Computerkriminalität und Strafrecht* (2. Aufl.) (Heymann, Köln), p. 190 note 13 and B. BERGMANS, *ibid.*

27. Articles 203 et 204 du Code pénal.

28. Articles 93 et suivants.

29. Articles 201, 202 et 202a.

30. Articles 252 à 256 du Code pénal.

31. Articles 118-120 du Code pénal.

32. Articles 122, 123 et 124.

33. *Theft Act*, 1968 (U.K.), c. 60.

34. E. GRIEW, *The Theft Act 1968*, 2<sup>e</sup> éd., London, Sweet & Maxwell, 1974, n<sup>o</sup> 2-04, 2-42; W.R. CORNISH, *Protection of Confidential Information in English Law*, 611C43 (56 note 52) 1975 et J.C. SMITH, *The Law of Theft*, 3<sup>e</sup> éd., London, Butterworths, 1976, n<sup>o</sup> 277.

La jurisprudence a confirmé cette opinion : dans un premier cas, un étudiant avait « emprunté » et copié un questionnaire d'examen avant que celui-ci n'ait lieu<sup>35</sup>; dans un deuxième cas, un géologue travaillant pour Esso avait copié un document contenant des données géologiques et des renseignements sur les chances de trouver du pétrole et il l'avait proposé à des concurrents<sup>36</sup>. L'incrimination pour vol a été rejetée pour deux raisons : d'une part, l'information confidentielle n'est pas une forme de propriété intangible par opposition à la propriété du papier, car le titulaire jouissait seulement d'un droit (découlant de la confiance) de contrôle sur la publication du document (ce qui justifie une action civile basée sur l'« abus de confiance » en cas de violation de secret). Le fondement de cette action est normalement de nature contractuelle, mais peut également être trouvé dans la propriété de l'information et surtout dans un devoir de bonne foi<sup>37</sup> qui est un droit sur le document (*right over property*) plutôt qu'un droit en lui (*right in property*); d'autre part, le titulaire de l'information n'en était pas privé de manière permanente.

Similairement, il a été jugé que le piratage de film protégé par le droit d'auteur et la vente non autorisée de cassettes vidéo ne constitue pas un vol parce que la définition de bien du *Theft Act* n'inclut pas le droit d'auteur<sup>38</sup>.

Selon l'article 6(1) une personne qui s'approprie des biens appartenant à autrui dans l'intention de lui faire perdre la chose elle-même de manière permanente doit néanmoins être considérée comme ayant l'intention d'en priver autrui de manière permanente si elle a l'intention d'en disposer quels que soient les droits d'autrui; et son emprunt ou prêt peut aboutir au même résultat si l'emprunt ou le prêt est fait pour une période ou dans des circonstances qui le rendent équivalent à une soustraction ou une disposition pure et simple<sup>39</sup>.

Le dernier cas se présente, par exemple, quand la chose rendue (même dans son intégralité matérielle) a perdu sa valeur parce qu'elle ne peut plus remplir sa fonction (par exemple un abonnement de théâtre rendu quand la saison est terminée). On pourrait ainsi punir le vol d'information par la sanction de l'« emprunt » du document qui lui sert de support s'il a perdu toute utilité quand l'information est connue par l'« emprunteur » ou communiquée à des tiers. Cela est possible dans certains cas, par exemple dans le cas des questions d'examen<sup>40</sup>, mais pas applicable si l'information garde sa valeur pour son titulaire<sup>41</sup>.

L'article 1<sup>er</sup> du *Theft Act*<sup>42</sup> de 1978 punit le « vol de services », c'est-à-dire l'obtention frauduleuse et malhonnête de services de quelqu'un, quand ce

35. *Oxford c. Moss*, (1978) 68 Cr. App. R. 183.

36. « Absolon Case », *The Times*, 14 September 1983, p. 2.

37. Voir W.R. CORNISH, *Intellectual Property: Patents, Copyright, Trade Marks and allied rights*, London, Sweet & Maxwell, 1981, chap. 8.

38. *Rank Film Distributors Ltd. et al v. Vidéo Information Centre et al.*, 2 All. E.R., 76 (8183) 1981 (Chambre des lords).

39. *Theft Act, supra*, note 33, section 6(1): « A person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other's rights; and a borrowing or lending of it may amount to so treating it if, but only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal ».

40. Voir note dans *Oxford v. Moss*, (1979) *Crim. L.R.* 119, p. 121.

41. Voir T. EISENSCHITZ, « Theft of Trade Secrets », (1984) *Eur. Intell. Prop. Rev.*, pp. 91 et s.

42. Adopté pour remplacer l'article 16(2)(b) du *Theft Act* de 1968.

dernier est induit à conférer un bénéfice en faisant un acte, en le causant ou en permettant qu'il soit fait, en lui faisant croire qu'il a été ou sera payé pour ce bénéfice.

Le « vol de services » pourrait être appliqué en matière d'information mais cette disposition ne s'applique pas si l'information n'est pas fournie contre paiement (ce qui est normalement le cas en matière d'espionnage) et si l'information est obtenue directement d'un ordinateur, puisqu'on ne peut tromper une machine<sup>43</sup>.

Étant donné les difficultés d'appliquer les normes existantes à des comportements perçus comme répréhensibles, on a suggéré soit de créer une disposition légale expresse sanctionnant le vol d'information<sup>44</sup>, soit de considérer la confidentialité comme un droit de propriété<sup>45</sup>.

En 1981, la Law Commission proposait une nouvelle disposition sanctionnant l'abus de confiance, proposition qui ne fut pas adoptée<sup>46</sup>.

Il existe pour le Commonwealth une décision d'un tribunal d'appel concernant la nature de l'information et la protection à y accorder. Dans la décision australienne *The Federal Commissioner of Taxation v. United Aircraft Corporation*, le juge Latham a statué que l'information ne pouvait faire l'objet ni d'un droit de propriété réelle, ni d'un droit de propriété personnelle et ce, dans aucune circonstance<sup>47</sup>.

En 1972, le Younger Committee on Privacy in the United Kingdom reconnaissait que la protection civile contre l'utilisation non autorisée de renseignements confidentiels pourrait être indiquée, mais rejetait la création de toute nouvelle infraction de vol d'information, même dans des circonstances restreintes. Le Comité déclarait que faire une infraction du vol d'information soulevait de nombreuses difficultés : en premier lieu, bien que l'information devienne pour son propriétaire moins utile ou totalement inutile lorsqu'elle est volée, ce dernier n'en est pas privé, ce qui, selon le comité constitue un élément essentiel du crime de vol; en second lieu, il faudrait définir très soigneusement le genre d'informations qui serait reconnu en droit comme susceptible de vol, de même que les circonstances du vol. Autrement, selon le comité, on pourrait mettre en danger la liberté de communication<sup>48</sup>.

Par ailleurs, en 1973, le Torts and General Law Reform Committee de Nouvelle-Zélande évoquait les difficultés que posait la formulation d'une telle infraction. Selon le comité, il faudrait définir l'information visée et les circonstances qui constituent le vol ou le détournement, avec la précision qui convient à la création d'une infraction pénale assez grave. Il faudrait, toujours selon le comité,

43. A. TETTENBORN, « Stealing Information », (1979) *New Law Journal*, p. 967.

44. *Id.*, p. 968.

45. T. EISENSCHITZ, *loc. cit.*, note 41, pp. 91-92.

46. LAW COMMISSION, *Breach of Confidence*, Report no. 110, Cmnd 8388.

47. (1943-44) 68 C.L.R. 525, (High Ct. Aust.). Le juge Latham a énoncé : « Knowledge is valuable, but knowledge is neither real nor personal property. A man with a richly stored mind is not for that reason a man of property. Authorities which relate to property in compositions belong to the law of copyright and have no bearing upon the question whether knowledge or information, as such, is property. It is only a loose metaphorical sense that any knowledge as such can be said to be property [...]. But it cannot in my opinion be described as the property either of the persons who originally had it or other persons to whom it has been communicated, whether under and in pursuance of a contract or otherwise ». (pp. 534-535).

48. *Report of the Younger Committee on Privacy in the United Kingdom*, Cmnd 5012, p. 149.

éviter d'assurer une protection trop large qui chevaucherait le système de brevets et encouragerait les inventeurs à garder leurs informations secrètes. Il faudrait également tenir compte du principe de la liberté de communication dans une société ouverte. Dans l'hypothèse que l'on puisse surmonter les difficultés mentionnées, le comité croit toutefois que la création d'une telle infraction pourrait bien constituer un enforcement souhaitable du droit<sup>49</sup>.

Aucune infraction pénale de ce genre n'a encore été adoptée en Nouvelle-Zélande.

### 3. États-Unis

Aux États-Unis, il existe une forte tendance à appliquer la théorie du droit de propriété aux valeurs intellectuelles. Par exemple, certaines cours américaines ont considéré des données informatiques comme des « biens » ou « choses de valeur » en vue d'habiliter l'application des dispositions de vol simple ou de nouvelles dispositions générales au crime informatique.

Un cas célèbre illustre bien cette tendance à appliquer les droits de propriété aux intangibles. Dans l'affaire *International News Services v. The Associated Press*<sup>50</sup>, la Cour suprême des États-Unis avait décidé que des nouvelles devaient être considérées comme des « quasi-propriétés » (*quasi-property*). La cour avait énoncé un large principe selon lequel nul ne devrait récolter ce qu'il n'a pas semé à la suite duquel une doctrine de détournement (*misappropriation*) s'est développée en droit américain<sup>51</sup>. Sur la base de ce principe, la cour avait accordé une injonction interdisant au défendeur le copiage et la vente des nouvelles recueillies par le plaignant, jusqu'à ce que la valeur commerciale de l'information n'existe plus.

Le vol d'information est poursuivi essentiellement en tant que vol de secrets commerciaux, définis traditionnellement comme :

toute formule, tout modèle, tout appareil ou toute compilation d'informations que quelqu'un utilise dans ses affaires, et qui lui donne la possibilité d'obtenir un avantage par rapport à des concurrents qui ne connaissent ou n'utilisent pas ce secret. Il peut s'agir d'une formule pour une substance chimique, d'un procédé de fabrication, de traitement ou de conservation de matériaux, d'un modèle pour une machine ou autre appareil, ou d'une liste de clients.<sup>52</sup>

Cette définition fut récemment modifiée, le secret commercial se définit maintenant en ces termes :

information, y compris une formule, un modèle, une compilation, un programme, un dispositif, une méthode, une technique ou un procédé qui

- (i) tire une valeur économique indépendante, actuelle ou potentielle, du fait qu'elle n'est pas généralement connue par d'autres personnes qui ne peuvent

49. Department of Justice, Wellington, New Zealand (1973), p. 18.

50. (1918) 248 U.S. 215.

51. A.S. WEINRIB, « Information and Property », (1988) 38 *University of Toronto Law Journal*, p. 123 et s.

52. Commentaire b au §757 du *Restatement of Torts (1939)*, version française dans B. BERGMANS, *loc. cit.*, note 9, p. 915 note 70 approuvé par la Cour suprême dans une affaire civile, *Kewanee Oil Co. v. Bicron Corp.*, (1974) 416 U.S. 470, pp. 474-75 et utilisé également en matière pénale (par ex. *People v. Serrata*, 1976, 62 Cal. App. 3d 9(23)).

pas s'en assurer rapidement par des moyens propres, et qui tirent un profit économique de sa divulgation ou de son utilisation, et  
 (ii) est l'objet d'efforts raisonnables — selon les circonstances — en vue de la maintenir secrète.<sup>53</sup>

Les poursuites pénales se font normalement en vertu des législations des États, qui ont pour la plupart adopté des définitions semblables à celles du *Restatement*<sup>54</sup>, mais il existe également des lois fédérales dans certaines matières spécifiques. Par exemple, le *Theft of Government Property Statute*<sup>55</sup> permet de sanctionner le vol de « choses » de valeur appartenant à l'État ce qui comprend le vol d'informations secrètes.

Au niveau fédéral, la plupart des poursuites pour vol de secrets commerciaux se font en vertu du *National Stolen Property Act* qui incrimine le fait de transporter, dans le commerce interétatique ou extérieur, tous biens, articles ou marchandises d'une valeur de 5 000 \$ ou plus, dont on sait qu'ils ont été volés, détournés ou pris frauduleusement<sup>56</sup>.

La Cour suprême a estimé que des copies et notes constituent des biens ou marchandises pouvant être transportés dans le commerce interétatique ou extérieur, puisqu'il y a un marché pour les vendre. Mais l'information doit être matérialisée dans un objet, et le § 2314 ne serait pas applicable si l'information a seulement été mémorisée dans l'esprit du voleur et transcrite<sup>57</sup>.

Dans le domaine des secrets commerciaux, la réforme du droit a débuté dans les années 1960 à cause de l'insuffisance des sanctions civiles contre l'espionnage économique, notamment par des étrangers<sup>58</sup>, et d'autre part, à cause des difficultés d'application du droit pénal général.

La plupart des États ont modifié leur droit pénal. Certains États ont défini le secret commercial comme un bien aux fins de leurs lois pénales et d'autres ont créé une infraction spécifique de vols de secrets commerciaux, avec des formulations diverses<sup>59</sup>, et d'autres encore ont déterminé les objets pouvant être volés de manière générale comme les choses de valeur, tangibles ou intangibles. On refuse généralement de sanctionner une simple mémorisation quand l'information n'est pas incorporée dans un objet. Les tribunaux admettent que la valeur de ce qui a été volé ne se détermine pas sur la base de l'objet matériel soustrait, mais en vertu de la perte de l'exclusivité de l'information, c'est-à-dire du secret et du

53. §1(4) du *Uniform Trade Secrets Act* de 1984 version française dans B. BERGMANS, *id.*, p. 915.

54. Voir INSTITUTE OF LAW RESEARCH AND REFORM OF ALBERTA (ci-après A.I.L.R.R.), *Les secrets commerciaux*, rapport n° 46, 1986, pp. 267 et ss.

55. 18 U.S.C. § 641.

56. 18 U.S.C. § 2314: « [...] transports in interstate or foreign commerce any goods, wares, merchandise, securities or money [...] knowing the same to have been stolen, converted or taken by fraud ».

57. *U.S. v. Bottone, Salb and Sharf*, 365 F. 2d 389 (2d Circ., 1966).

58. Il y eut différents scandales suite à une série de vols de secrets commerciaux pharmaceutiques en Italie entre autres, où les substances pharmaceutiques n'étaient pas brevetables, à ce sujet: F. FETTERLEY, *loc. cit.*, note 1, p. 1536.

59. La plupart de ces lois exigent cependant que le secret soit incorporé dans un objet tangible, même s'il s'agit seulement d'une copie et s'il n'appartient pas au titulaire de l'information.

contrôle de fait qu'il permet. Les tribunaux sont cependant stricts dans l'appréciation du caractère secret de l'information<sup>60</sup>.

Le droit de la propriété intellectuelle résistait en général à considérer l'information comme une chose pour laquelle son détenteur pouvait revendiquer un droit de propriété. Le droit des secrets commerciaux offre aux détenteurs d'information secrète des recours contre l'usage non autorisé d'information secrète et contre ceux qui révèlent le secret en violant une relation de confidentialité. Cependant, le droit en général résistait à considérer le secret comme un objet de propriété.

Récemment, cette tendance a connu un revirement. La Cour suprême des États-Unis a ouvert un nouveau chapitre du droit des secrets commerciaux en décidant dans l'affaire *Ruckelshaus v. Mosanto Co.*<sup>61</sup> que les secrets commerciaux constituaient une propriété selon les termes du cinquième amendement. Avant cet arrêt, il semblait invraisemblable que l'on puisse en venir à un tel résultat parce que la plupart des tribunaux étaient réticents à considérer les secrets commerciaux comme pouvant être l'objet d'un droit de propriété<sup>62</sup>. Les tribunaux trouvaient des façons de protéger les détenteurs de secrets commerciaux contre les personnes qui utilisaient de façon malhonnête ces secrets. Les tribunaux appliquaient alors les théories de concurrence déloyale, d'abus de confiance ou de bris de contrat pour punir l'utilisation malhonnête des secrets commerciaux.

La Cour suprême des États-Unis devait répondre pour la première fois à la question de savoir si les secrets commerciaux pouvaient faire l'objet d'un droit de propriété. La Cour a décidé de façon unanime que les secrets commerciaux sont des objets de propriété protégés par le cinquième amendement et qu'ils ne peuvent pas être enlevés à leur propriétaire sans une compensation équitable. La Cour souligne que les droits de propriété du cinquième amendement ne sont pas créés par la Constitution. Ils sont plutôt créés, et leurs dimensions sont définies, par les règles et conventions issues de sources indépendantes comme le droit des États. La Cour soutient que les données de Monsanto étaient des biens faisant l'objet d'un droit de propriété pour les fins du droit du Missouri « which recognizes trade secrets, as defined in § 757, Comment d, of the Restatement of Torts, as property »<sup>63</sup>.

Dans *Carpenter v. United States*<sup>64</sup>, la Cour, citant l'arrêt *Mosanto*, a décidé que des informations reliées aux affaires d'un employeur faisaient l'objet d'un droit de propriété par cet employeur.

60. B. BERGMANS, *loc. cit.*, note 9, p. 919; A.I.L.R.R., *op. cit.*, note 54, pp. 267 et s. et R. G. HAMMOND, « Quantum Physics, Econometric Models and Property Rights to Information » (1981) 27 *McGill L.J.* 47, pp. 57 et s.

61. 467 U.S. 986 (1984). La Cour a décidé que des données de recherche soumises à une agence fédérale documentant la sécurité du produit des demandeurs pouvaient être considérées comme une « propriété » au sens du cinquième amendement. La Cour soutient que l'utilisation des données par l'agence, pour des fins d'évaluation du produit d'une autre firme, ou qu'une révélation publique de ces données pouvait, dans d'autres circonstances, constituer l'enlèvement d'un droit de propriété (*taking of « property »*) pour lequel le gouvernement doit payer une juste compensation.

62. Voir SAMUELSON, « Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law? », (1989) 38 *Cath. U. L. Rev.* 365, commentant les décisions de la Cour suprême qui ont considéré les secrets commerciaux comme l'objet d'un droit de « propriété ».

63. *Ruckelshaus v. Mosanto Co.*, *supra*, note 61, p. 1001.

64. (1987) 484 U.S. 19.

Ces décisions de la Cour suprême amèneront inévitablement d'autres questions complexes. La prochaine étape consistera en la difficile tâche de définir l'information, d'articuler les circonstances au sein desquelles l'information est ou n'est pas une propriété et de déterminer pourquoi dans certaines circonstances la désignation d'un droit de propriété sur l'information est justifiée et dans d'autres pas.

Ces deux décisions sont des signes d'un changement d'attitude envers la libre circulation de l'information et ils ne sont pas les seuls signes de cette nouvelle tendance. Les lois américaines contrôlant l'exportation considèrent que l'échange d'information technique et scientifique — même dans le cadre d'une conversation avec un étranger en sol américain — est une exportation de données techniques qui requiert une autorisation grâce à un permis de contrôle de l'importation<sup>65</sup>. De la même façon, le système de brevet permet l'émission d'ordres de garder le silence afin de prévenir la révélation d'inventions impliquant la sécurité nationale, incluant celles qui ne sont pas désignées « classées secrètes »<sup>66</sup>. Le ministère du Commerce des États-Unis s'engage de plus en plus dans les politiques concernant la propriété intellectuelle parce que les exportations de propriété intellectuelle constituent un des rares domaines dans lesquels les États-Unis profitent d'une balance de commerce positive. Un respect accru des droits américains dans le domaine de la propriété intellectuelle aurait comme résultat une croissance de cette balance positive. En conséquence, le domaine de la propriété intellectuelle fait maintenant l'objet de discussions dans le cadre des négociations du General Agreement on Tariffs and Trade (GATT).

Les arrêts *Ruckelshaus* et *Carpenter* s'inscrivent dans une tendance vers une protection accrue de droits de propriété sur l'information aux dépens de la libre circulation de l'information, ce qui n'a rien d'étonnant si on considère l'importance du rôle de l'information dans le développement de l'économie<sup>67</sup>.

#### 4. Canada

Au Canada, les décisions *Stewart*<sup>68</sup> et *Offley*<sup>69</sup> ont démontré une sérieuse différence d'opinion parmi les juristes sur la question du détournement ou de l'appropriation d'information confidentielle. Dans ces deux affaires, la question à décider était de savoir si l'information confidentielle constituait une « propriété » pour les fins d'application des dispositions du *Code criminel* sur le vol.

La Cour d'appel de l'Ontario a admis le vol d'information et sa décision fut loin de faire l'unanimité<sup>70</sup>. La Cour d'appel de l'Alberta a refusé de suivre le précédent de l'Ontario. Enfin, la Cour suprême a renversé la décision de la Cour d'appel de l'Ontario dans sa décision de mai 1988 concernant l'arrêt *Stewart*<sup>71</sup>.

65. Voir 15 C.F.R. § 379 1(b)2( ) (1988) et LETTERMAN, « United States Regulation of High Technology Exports », (1986) 20 *Int'l Law* 1147.

66. Voir 35 U.S.C. § 181 (1982).

67. OFFICE OF TECHNOLOGY ASSESSMENT, U.S. Congress, *Intellectual Property Rights in an Age of Electronics and Information*, 1986, pp. 40-41.

68. R. c. *Stewart*, (1983) 5 C.C.C. (3d) 481 (C.A. Ont.).

69. R. c. *Offley*, (1986) 51 C.R. (3d) 378 (C.A. Alb.).

70. Voir R.G. HAMMOND, « Theft of Information », (1984) 100 *L.Q.R.* 252 et F.R. MOSKOFF, Q.C. « The Theft of Thoughts: The Realities of 1984 », 27 *C.L.Q.* 226.

71. R. c. *Stewart*, [1988] 1 R.C.S. 963.



Toute la question selon la Cour suprême était de savoir si les renseignements confidentiels pouvaient faire l'objet d'un vol au sens de l'article 283 du *Code criminel* (maintenant l'article 322).

En première instance<sup>72</sup>, le juge Krever avait écarté cette thèse en affirmant que si la « chose » visée par l'article 283(1) pouvait être intangible, encore fallait-il, conformément à l'arrêt *R. c. Scallen*<sup>73</sup>, qu'elle puisse être considérée comme un bien, ce qui, en l'état du droit positif, ne pouvait être admis pour des renseignements confidentiels.

En appel, le juge Houlden avait décidé que la qualification de vol pourrait être retenue. D'une part, il a estimé que des renseignements confidentiels réunis au prix de temps, de travail et d'argent doivent être considérés comme des biens. D'autre part, en l'espèce, si Stewart avait réussi à se procurer les renseignements, ces renseignements auraient perdu leur caractère confidentiel et n'auraient pu de ce fait être restitués dans l'état où ils étaient antérieurement, ce qui suffisait à justifier la condamnation pour vol sur le fondement de l'alinéa d) de l'article 283(1).

Ces deux propositions furent réfutées en Cour suprême. Le juge Lamer affirma qu'une information en tant que telle ne peut être considérée comme un bien, au moins en droit criminel. Quant à la privation du caractère confidentiel des renseignements, elle ne suffisait pas à constituer l'*actus reus* requis pour qu'il y ait infraction au sens de l'article 283(1), c'est-à-dire le fait de prendre ou de détourner. Selon le juge, on ne peut être privé de la confidentialité parce qu'on ne peut pas en être propriétaire.

Ainsi, si l'information ne peut être considérée comme un bien, c'est parce qu'elle n'est pas un objet de propriété, et c'est cette particularité qui explique que son détenteur ne puisse se prévaloir d'un véritable détournement : il n'en est pas « propriétaire ».

Le droit donne aux entreprises un moyen spécifique de monopolisation de leurs créations techniques : le brevet d'invention. La *Loi sur les brevets d'invention*<sup>74</sup> ne s'applique que s'il s'agit d'une « invention » et celle-ci est définie dans la Loi comme : toute réalisation, tout procédé, toute machine, fabrication ou composition de matières, ainsi que tout perfectionnement de l'un d'eux, présentant le caractère de la nouveauté et de l'utilité<sup>75</sup>.

La société confère un droit exclusif d'exploitation, pour une période limitée, à l'inventeur qui accepte de rendre publique sa création. Le brevet d'invention n'accorde pas une protection pratique à l'information. En droit, l'information ne pourrait pas constituer une invention brevetable, par défaut de caractère industriel, de nouveauté ou d'activité inventive.

La *Loi sur le droit d'auteur*<sup>76</sup> vise plutôt la forme ; elle protège la forme d'expression d'une œuvre mais non les idées, le concept ou le sujet. Le droit d'auteur existe dès la création de l'œuvre mais sa protection se limite à son expression. L'auteur n'a pas de monopole sur les idées qui sont dans son œuvre.

72. (1982) 68 C.C.C. (2d) 305 (Ont.H.C.J.).

73. (1974) 15 C.C.C. (2d) 441 (C.A.C.-B.).

74. S.R.C. 1985, c. P-4.

75. *Id.*, art. 2.

76. S.R.C. 1970, chap. C-30 [mod. 1974-75-76, chap. 50].

Cette loi s'est adaptée aux technologies modernes mais elle n'accorde pas plus de protection générale à l'information elle-même<sup>77</sup>.

La *Loi fédérale sur les marques de commerce*<sup>78</sup> vise les comportements concurrentiels impliquant l'information mais elle ne touche pas à tous les cas possibles de prise d'information. Cette loi n'a pas pour objectif de protéger l'information mais elle vise plutôt à empêcher la concurrence déloyale. Depuis la décision de la Cour suprême dans l'affaire *Vapor c. MacDonald*<sup>79</sup>, les juges sont privés du texte fédéral puisque la Cour suprême a neutralisé les dispositions sur la concurrence déloyale contenues dans l'article 7 de la Loi. Cet arrêt, précisément rendu dans une affaire d'utilisation illégale d'information confidentielle, a déclaré inconstitutionnel l'alinéa e) de l'article 7 de la *Loi sur les marques de commerce*. Les motifs généraux de l'arrêt rendent précaire, désormais, le recours à l'article 7 en son entier. La Cour fédérale et la Cour supérieure ont d'ailleurs déjà considéré respectivement que l'alinéa b) de l'article 7 et l'article 7 en entier étaient *ultra vires* de la compétence fédérale. Les tribunaux canadiens appliquent la loi provinciale pour faire face aux actes de concurrence déloyale.

Ces lois ont donc une application plutôt limitée et ne couvrent pas l'utilisation non autorisée d'information. Bien qu'un certain mouvement d'opinions soit en faveur d'une protection par le droit des biens, après l'arrêt *Stewart*, en droit pénal, cette protection est écartée pour le moment, du moins au plan judiciaire.

À défaut de protection adéquate de l'information, la confidentialité constitue un moyen pratique de réservation qui est largement utilisé pour empêcher autrui d'exploiter l'information ou de façon plus radicale, pour priver autrui de la connaissance même de l'information. Ainsi envisagée, la confidentialité apparaît comme le seul mode adéquat de réservation des connaissances. L'information confidentielle est actuellement protégée en l'absence de règles spécifiques, par le droit des obligations ou *tort* en common law.

La plupart des situations d'abus d'information confidentielle portées devant les tribunaux sont des situations contractuelles. Il s'agit généralement de contrat de travail, le cas typique de litige étant celui de l'employé qui a acquis une information confidentielle dans l'exercice de son emploi et qui, celui-ci terminé, dispose de cette information à des fins personnelles ou au profit d'un tiers.

Le plus souvent le contrat stipule expressément l'interdiction de révéler ou d'user de l'information confidentielle. La violation de cette clause dont l'effet se poursuit normalement après la fin du contrat, est sanctionnée en tant que telle que la juridiction soit civile ou de common law.

Il existe des différences dans les solutions lorsque l'obligation n'est pas expresse mais tacite, impliquée, par exemple par une obligation de non-concurrence ou une obligation de loyauté, qui peuvent être elles-mêmes tacites, à l'instar de l'obligation de loyauté dans le contrat de travail. Le juge québécois recherchera en principe l'existence d'une telle clause. Lorsqu'elle existe, cette clause lui permet de statuer sur le fondement de la violation d'une obligation contractuelle. « La clause implicite de loyauté qui peut être lue dans tout contrat

---

77. *Loi modifiant la loi sur le droit d'auteur et apportant des modifications connexes et corrélatives*, adoptée le 3 fév. 1988 et entrée en vigueur le 8 juin 1988 (P.L. C-60).

78. S.R.C. 1985, c. T-13.

79. (1976) 22 C.P.R. (2d) 1 (S.C.).

d'engagement » explique « qu'un employé n'ait pas le droit de se servir d'informations confidentielles obtenues par et dans son emploi pour solliciter les clients de son employeur »<sup>80</sup>.

En l'absence de clause expresse relative à l'information, les tribunaux québécois suivent parfois les tribunaux de common law qui utilisent l'obligation fiduciaire par préférence à l'application du contrat<sup>81</sup>. La règle traditionnelle selon laquelle en common law la sanction du contrat ne peut consister que dans des dommages et intérêts (*damages*) expliquerait cette préférence des tribunaux de common law. En effet, la sanction de l'obligation fiduciaire, qui relève de l'équité (*equity*), peut mener à l'interdiction ou la prescription d'un acte.

En droit civil, le respect du contrat ne se heurte pas au même obstacle puisque l'article 1065 du *Code civil du Bas-Canada* permet d'ordonner l'exécution forcée. Afin de faire respecter une obligation de discrétion et de non-concurrence, la Cour supérieure du Québec se référant à l'article 1065 du Code civil affirmait que « l'exécution particulière de l'obligation constitue la principale et essentielle réparation et le recours du demandeur contre qui la violation du contrat a été commise »<sup>82</sup>. Néanmoins, malgré cette facilité et celle que lui donne l'article 1024 du Code civil, de jouer sur le contenu du contrat, les tribunaux québécois subissent l'influence de la common law. Ainsi, pour les cas des dirigeants de compagnies et des employés supérieurs, les juges québécois se rallient à l'analyse des juridictions de common law, en une relation fiduciaire, comme en témoignent des décisions de la Cour supérieure du Québec<sup>83</sup> dans lesquelles on réfère à l'arrêt de principe *Canadian Aero*, rendu par la Cour suprême<sup>84</sup>.

Dans les situations de relations extra-contractuelles, les juridictions de common law suivent les décisions anglaises *Saltman*<sup>85</sup> et *Seager Copydex*<sup>86</sup> fondées sur l'abus de confiance (*breach of confidence*)<sup>87</sup>. Le contenu de ce devoir

80. *Arcon Canada Inc. et al. c. Arcobec Aluminium Inc. et al.*, (1984) 7 C.P.R. (3d) 382.

81. À ce sujet, voir J.N. LANDRY, « The Protection of Trade Secrets in Canada. Patent and Trademark Institute of Canada », (1982) 12 *P.T.I.C. Bull.* 712 et des décisions de la Haute Cour de l'Ontario: *House of Faces Inc. et al. c. Leblanc*, (1984) 2 C.P.R. (3d) 177; *E.J. Personnel Services Inc. carrying on business as Ej Peel Placement Services c. Quality Personnel Inc. et al.*, (1985) 6 C.P.R. (3d) 173; *Drake International Inc. c. Tennenbaum et al.*, (1986) 10 C.P.R. (3d) 119 (dans laquelle on peut lire qu'existe « Tout à fait à part du contrat d'emploi [...] un devoir de droit commun d'agir de bonne foi et de ne pas faire usage de secrets et d'information confidentielle ») et *Promotivate International Inc. c. Toronto Star Newspapers Ltd. et al.*, (1986) 8 C.P.R. (3d) 546.

82. *Nedco Cooling — Semis Conductors Ltd. c. Mester and General Instruments F.W. Sicckles of Canada Ltd.*, (1961) C.P.R. 115 C.S., p. 120.

83. *Banque fédérale de Développement et al. c. Dandenault et al.*, Cour supérieure, n° 460-05-000464-81, 19 mars 1982; *Brimarriere Inc. c. Laplante*, Cour supérieure, n° 05-000323-81, 24 novembre 1983; *Resfab Manufacturier de Ressort Inc. et al. c. Archambault et al.*, (1985) 10 C.P.R. (3d) 102; *NFBC National Financial et al. c. Investors Syndicate Ltd.*, Cour d'appel, n° 09-000463-851, 24 janvier 1986.

84. *Canadian Aero Services Ltd. c. O'Malley et al.*, (1973) 11 C.P.R. (2d) 206.

85. *Saltman Engineering Co. Ltd. et al. c. Campbell Engineering Co. Ltd.*, [1984] 3 All E.R. (C.A.).

86. *Seager c. Copydex Ltd.*, [1967] 2 All E.R. 415 (C.A.).

87. À ce sujet, voir R.G. HAMMOND, « Is Breach of Confidence Properly Analysed in Fiduciary Terms? » (1979) 25 *McGill Law Journal* 224; du même auteur: « Breach of Confidence: Assignability of Rights », (1986) 2 *I.P.J.* 247.

est de ne pas faire de l'information un usage qui nuise à celui dont on l'a obtenue. Il ne peut être question d'abus de confiance que si l'information est confidentielle, si elle a été donnée alors qu'on pouvait s'attendre au secret, si elle a été utilisée sans autorisation, et s'il n'existait pas de motif valable à son utilisation ou à sa divulgation.

Dans certains cas, il y aura aussi des poursuites sur la base de l'enrichissement sans cause, doctrine qui vise à empêcher quelqu'un de conserver injustement de l'argent ou un autre avantage. Dans le cadre d'une action de ce genre, il devra y avoir preuve, à la fois, de l'existence d'un avantage pour le défendeur, que cet avantage s'est développé aux dépens du demandeur et qu'il serait injuste que le défendeur puisse conserver cet avantage.

C'est donc la relation entre les parties et non la nature de l'information elle-même qui détermine le statut juridique et le degré de protection accordés à l'information.

En l'absence de relation entre les parties, la situation est régie par les principes généraux de la responsabilité civile. C'est le régime général de la responsabilité civile extra-contractuelle qui permet de sanctionner civilement les obligations légales de confidentialité. Ces obligations peuvent avoir une sanction pénale<sup>88</sup>.

C'est aussi la responsabilité civile délictuelle qui sanctionne le comportement du tiers qui se rend complice de la violation d'un contrat, comme celui par exemple qui soudoie le salarié d'une entreprise pour se procurer des informations. Le cas échéant cet acte tombera sous le coup de la loi criminelle<sup>89</sup>. Si ce tiers est un concurrent de l'entreprise, on pourra avoir un recours en concurrence déloyale.

Les juges de common law utilisent le *tort* de *passing off*. Au Québec, la jurisprudence se fonde sur l'article 1053 du *Code civil du Bas-Canada*. La concurrence déloyale est définie comme « l'acte pratiqué de mauvaise foi à l'effet de produire une confusion entre les produits de deux fabricants ou commerçants ou qui, sans produire une confusion jette le discrédit sur un établissement rival »<sup>90</sup>. On ne peut utiliser cette action lorsque l'information prise ne produit aucune confusion entre les produits ou ne jette aucun discrédit sur un établissement.

Il apparaît donc que les moyens de protection de l'information confidentielle tirés du droit civil sont nombreux mais ne répondent pas adéquatement à plusieurs cas d'utilisation non autorisée d'information. Ils permettent d'obtenir des dommages-intérêts alors que souvent, l'utilisation d'une information obtenue frauduleusement par les défendeurs leur a rapporté un montant beaucoup plus élevé que celui qu'ils devront payer à titre de dommages.

Les recours de droit civil n'offrent pas une protection complète et ils sont trop divers pour constituer un système de protection satisfaisant. La complexité de cette protection, la relative inefficacité de celle-ci, son caractère fragmentaire et aléatoire la rendent inadéquate.

L'exemple des États-Unis illustre comment la conjoncture économique et l'évolution technologique favorisent présentement une attitude protectionniste

88. Voir la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. 1979, c. A-2.1.

89. Délit de commissions secrètes : art. 383(1) *C.cr.*

90. *Corbeil c. Dufresne*, (1933) 71 C.S. 548.

dans le domaine de l'information. La protection des secrets commerciaux connaît déjà une tradition de plusieurs décennies aux États-Unis et l'expérience américaine pourrait être utile à cet égard. Si le droit des secrets commerciaux évolue vers un plus grand protectionnisme, il sera peut-être nécessaire que le Canada ajuste son droit à cette nouvelle réalité puisque l'information est particulièrement touchée par les échanges commerciaux et technologiques<sup>91</sup>.

Bien qu'aucun pays du Commonwealth n'ait adopté de dispositions spéciales portant sur le détournement des secrets commerciaux, il est difficile au Canada d'ignorer le droit américain. Puisque les États-Unis représentent notre principal partenaire commercial et qu'il existe un chevauchement des relations commerciales entre les deux pays, et puisque les technologies modernes abolissent les frontières au niveau de nombreux échanges, il faut à tout le moins se demander s'il y a lieu de s'inspirer de l'expérience américaine dans le domaine des secrets commerciaux. L'importance des échanges commerciaux entre les États-Unis et le Canada commande peut-être un ajustement de la législation canadienne à la législation américaine dans ce domaine.

## II. LA NÉCESSITÉ D'UNE RÉFORME

Si la plupart des pays ont légiféré en matière d'informatique, il faut bien reconnaître que les lois destinées à réprimer l'utilisation non autorisée d'ordinateurs, le détournement, l'interception, la falsification et la destruction des données, ne constituent pas une protection à toute épreuve. Comment le droit peut-il protéger efficacement des données contenues, compilées, traitées et transmises à travers un système aussi vulnérable à toute forme d'intrusion? Qu'elle soit astucieuse, audacieuse ou malicieuse, l'intrusion dans les systèmes de logiciels peut provoquer leur paralysie, la destruction et l'effacement des programmes en plus de servir à divers agissements frauduleux. Il faut bien admettre que dans l'état actuel de la technologie informatique, aucun système juridique ne saurait encadrer de façon satisfaisante une information dont l'exactitude et l'intégrité sont constamment menacées. « Les progrès sur ce point doivent être techniques avant d'être juridiques »<sup>92</sup>.

Cette constatation n'écarte pas cependant la nécessité immédiate de formuler les définitions et les idées essentielles pour élaborer une théorie générale relative à la protection des choses intangibles. En d'autres domaines, l'expérience montre que le droit s'est formé à partir d'une notion fondamentale et de quelques principes, autour desquels sont venus s'articuler des législations spécifiques. « Or l'informatique ayant pour fonction de traiter l'information et la télématique de la déplacer, ces deux disciplines opèrent sur un dénominateur commun; l'information,

---

91. Il faut souligner les nouveaux problèmes que soulève le développement de la technologie. L'efficacité des moyens techniques favorise entre autres les échanges de programmes par des systèmes de télécommunications entre deux pays, ce qui permet d'échapper aux contrôles douaniers alors que s'ils traversent les frontières par le biais des moyens de transport traditionnels, ils doivent se soumettre à certains contrôles des importations et exportations, droits d'auteur et frais douaniers.

92. E. MACKAAY, « Les biens informationnels, le droit de suite dans les idées » dans *L'appropriation de l'information*, Études présentées par J.P. CHAMOIX, Paris, Librairies Techniques, 1986, chap. 5.

qui devrait logiquement se retrouver au cœur de toutes les difficultés juridiques qu'elles suscitent »<sup>93</sup>.

La protection des logiciels remet en cause un certain nombre de principes sur lesquels reposent actuellement la plupart des systèmes de droit occidentaux et n'est qu'une illustration parmi d'autres d'une difficulté plus générale qui est celle de la réservation du savoir-faire, des renseignements confidentiels voire même « de l'utilisation non autorisée de l'investissement intellectuel d'autrui »<sup>94</sup>; par quelque biais que l'on aborde le problème, la difficulté ressurgit. À moins de renoncer à l'idée d'une protection juridique, il faut reprendre dans son entier le problème du statut de l'information.

#### A. L'IMPORTATION DU RÔLE DE L'INFORMATION

À une époque où la société est de plus en plus dépendante de la technologie de l'information, les intérêts en jeu sont de plus en plus importants. Dans le monde des affaires, la majorité des transactions monétaires est administrée par ordinateurs, l'entière production des compagnies est fréquemment dépendante du fonctionnement des terminaux et plusieurs compagnies gardent leurs plus importants secrets d'affaires dans un ordinateur. De la même façon, l'administration contemporaine est liée à la technologie informatique et aux banques de données. Les systèmes de contrôle de la mer, de l'air et de l'espace, la supervision médicale et les systèmes de défense dépendent aussi en grande partie de la technologie informatique. En conséquence, il n'y a pas de doute que la sécurité de la technologie de l'information et la prévention du crime informatique est d'une importance décisive pour notre société d'information et reposent sur un concept général en développement : le droit de l'information et le droit de la technologie de l'information. En accord avec la cybernétique et l'informatique modernes, le nouveau concept de « droit de l'information » reconnaît l'information comme un troisième élément de base après la matière et l'énergie. Élaboré à partir d'analyse empirique, ce concept traite l'information comme un bien culturel et un atout politique mais la considère aussi comme un potentiel de danger particulier. La nouvelle théorie du « droit de l'information » conçoit que la technologie moderne de l'information altère les caractéristiques de cette information, particulièrement parce qu'elle lui donne une importance accrue et la traite comme un élément actif qui fonctionne sans intervention humaine à travers les systèmes de traitement automatique<sup>95</sup>.

L'information représente souvent une valeur économique. Les observateurs parlent d'un nouveau phénomène et d'une nouvelle valeur économique. Pourtant ce phénomène n'est pas nouveau en soi. Si la demande de clarifier son statut se fait pressante, c'est que la fragilité de celle-ci croît en même temps que croît son rôle économique.

Malgré la multitude de ses nouvelles apparences, le problème de l'information n'est pas foncièrement nouveau en droit. Les corporations médiévales tentaient de garder leurs secrets à travers une hiérarchie familiale. Joshua Wedgwood a tenté de persuader le parlement anglais de permettre l'ouverture du courrier

---

93. P. CATALA, « Ébauche d'une théorie juridique de l'information », *D. 1984 Chr.*, p. 97.

94. P. GAUDRAT, « La protection des logiciels », (1988) *Revue internationale du droit d'auteur*, p. 77.

95. Voir U. SIEBER, *op. cit.*, note 2.

des artisans pour empêcher que les ouvriers ne soient embauchés ailleurs sur le continent et n'emportent avec eux des connaissances techniques uniques de l'industrie de la poterie. L'histoire rapporte des cas d'espionnage industriel remontant à l'empire romain<sup>96</sup>. N'a-t-on pas connu de tout temps des règles punissant les espions et les traîtres qui avaient passé de l'information secrète à l'ennemi? Des règles sanctionnant la reproduction non autorisée, ne serait-ce que le plagiat?

Dans le cadre d'un système économique capitaliste libéral, les entreprises, placées en situation de libre concurrence ne parviennent à maintenir leur compétitivité qu'en se distinguant par la mise en œuvre de nouvelles techniques de production et de gestion. Or, cette compétitivité peut se maintenir non seulement par la conception d'idées novatrices, mais encore par la sauvegarde de l'exclusivité de ces dernières. Les idées étant déjà, par nature, sujettes à propagation, devant le phénomène de l'évolution technologique rapide, il devient de plus en plus difficile d'assurer leur monopolisation. Le droit est appelé à la rescousse.

## B. LA NATURE DE L'INFORMATION

### 1. Les diverses approches

La Cour suprême a décidé qu'« une chose quelconque » au sens du paragraphe 283(1) du *Code criminel* (maintenant 322(1)), doit être de nature telle qu'elle peut faire l'objet d'un droit de propriété et que le bien en question soit susceptible d'être pris ou détourné d'une manière qui occasionne une privation à la victime. Selon le juge Lamer, les renseignements confidentiels ne relèvent pas de cette définition. Ils ne sont pas des biens aux fins de l'article 283 (maintenant 322) du *Code criminel*. Quant à la confidentialité, le juge estime qu'elle ne peut faire l'objet d'un vol parce qu'elle ne relève pas de l'expression « une chose quelconque » employée au paragraphe 283(1) (maintenant 322(1)) du *Code criminel*<sup>97</sup>.

Cette question du droit de propriété suscite beaucoup de controverse. Certains soutiennent que bien que l'information ne corresponde pas à la notion traditionnelle du droit de propriété, « il existe un intérêt économique associé à la confidentialité de l'information qui constitue le secret commercial, intérêt qui est par nature un droit de propriété » et qu'à ce moment, il n'est plus possible de l'ignorer en droit criminel<sup>98</sup>. Le vol ou des infractions évoquant le vol et la fraude seraient donc à privilégier pour assurer la protection de l'information confidentielle ayant une valeur économique.

Selon un courant de pensée, les renseignements confidentiels sont des biens au sens du droit civil parce qu'ils possèdent plusieurs des caractéristiques des autres types de biens : un secret industriel, qui est un genre particulier de renseignements confidentiels, peut être vendu; il peut faire l'objet d'une licence ou être légué; il peut faire l'objet d'une fiducie ou être transmis à un syndic de faillite. Ainsi, comme le terme « propriété » désigne simplement l'ensemble des

96. Voir D.F. FETTERLEY, *loc. cit.*, note 1, p. 1535.

97. R. c. Stewart, *supra*, note 71.

98. A.I.L.R.R., *op. cit.*, note 54 et R. GRONDIN, « Vol d'information dans la société canadienne », (1989) 20 R.G.D. 235, p. 254.

droits dont jouit le propriétaire, cette protection pourrait être accordée sous la forme de droit de propriété<sup>99</sup>.

Pour d'autres, une extension de l'incrimination pour faire de l'information une « chose » susceptible d'être volée, serait de nature à menacer la mobilité de la main d'œuvre. Ainsi, l'information ne devrait pas être considérée comme un bien, même sur le terrain du droit civil car il s'ensuivrait un complet bouleversement du droit de la propriété intellectuelle. Plutôt que de chercher à obtenir le brevet d'invention ou demander le bénéfice du droit d'auteur, on pourrait toujours faire condamner l'usurpateur en lui appliquant les peines du vol<sup>100</sup>.

À l'intérieur de la science économique s'est constituée une nouvelle branche appelée « économie de l'information » dans laquelle on traite l'information comme si elle était un bien ordinaire. Ce courant considère que lorsqu'il s'agit de secteurs restreints du domaine de l'information, comme celui des biens informationnels, l'information ressemble assez à un bien ordinaire. On entend par biens informationnels « les brevets, les licences, les modèles, les marques, les logiciels, les banques de données, les dépenses de recherche et développement, les productions culturelles et d'information de l'édition et de la presse [...] »<sup>101</sup>. Cette énumération — non exhaustive puisqu'on pourrait ajouter le droit d'auteur — démontre que la notion de bien informationnel ne coïncide pas avec celle de « bien incorporel » ou de « bien immatériel » par laquelle on entend un droit patrimonial autre que la propriété<sup>102</sup>. L'usufruit est un droit, un bien incorporel, mais non un bien informationnel. Un logiciel n'est pas en soi un droit, mais plutôt un objet immatériel (un ensemble structuré d'idées), dont le statut juridique est pluriforme. Ce qu'ont en commun les « biens informationnels » mentionnés, c'est « qu'ils constituent des structures d'information dont la création a exigé un investissement non nul et dont on espère tirer des revenus commerciaux par la suite. Selon le cas, ils sont désignés par leur régime juridique ou par leur forme, leur support matériel »<sup>103</sup>.

Dans le cadre d'une analyse économique du droit, certains conçoivent que l'information dans la plupart sinon l'ensemble de ses acceptations, paraît fondée sur la notion de pouvoir de sélection<sup>104</sup>. Ainsi « l'information ne peut être reçue que lorsqu'il y a un doute; et le doute implique l'existence de plusieurs options — là où doit s'effectuer un choix, une sélection, une discrimination »<sup>105</sup>. La notion d'information présente donc un intérêt fondamental : l'information est l'ingrédient essentiel de la science économique. Toute activité humaine exige un processus plus ou moins long de traitement d'information.

99. Voir R.B. POTTER, « Theft of a Secret : The Information Age Overtakes the Supreme Court of Canada », (1989) *R.I.B.L.* 115 et A.S. WEINRIB, *loc. cit.*, note 51.

100. Voir R.G. HAMMOND, *loc. cit.*, note 60 et A. LUCAS, « La propriété de l'information après l'arrêt Stewart », [1989] *C.P.D.I.*, vol. 2, n° 1, 115.

101. Henri DELAHAIE, « L'enregistrement des biens informationnels dans l'entreprise », *Revue française de comptabilité*, juin 1983, p. 335.

102. Voir CENTRE DE RECHERCHE EN DROIT PRIVÉ ET COMPARÉ DU QUÉBEC, *Dictionnaire de droit privé*, Montréal, édition provisoire 1984.

103. E. MACKAAY, *loc. cit.*, note 92, p. 27.

104. Colin CHERRY, *On Human Communication*, Cambridge, Mass., M.I.T. Press, 2<sup>e</sup> éd., 1966, p. 244; CONSEIL ÉCONOMIQUE DU CANADA, *Rapport sur la propriété intellectuelle et industrielle*, Ottawa, Information Canada, 1971, pp. 16 et s. et Ejan MACKAAY, *loc. cit.*, note 92.

105. C. CHERRY, *id.*, p. 170.



Le professeur Hammond ajoute que l'information a les caractéristiques d'un bien public à caractère économique<sup>106</sup>.

Ejan Mackaay précise que le principe de la libre circulation de l'information est donc justifiée dans un système capitaliste : mieux les acteurs sont informés, mieux ils prennent leurs décisions et mieux fonctionnera l'économie du marché. Dans le cas d'entraves à la libre circulation de l'information, celui qui détient certaines informations a un avantage par rapport à ceux qui ne les ont pas. L'information supérieure lui permet souvent d'améliorer sa situation par rapport à celle des autres. L'information confère alors des pouvoirs<sup>107</sup>.

Une autre observation s'impose, observation que soulèvent la plupart des auteurs qui élaborent des réflexions sur la nature de l'information : elle ne se confond pas avec son support, elle représente une entité distincte. Bien que les formes dans lesquelles elle est transmise varient, l'information de base reste identique et présente le même intérêt. On peut d'ailleurs en changer la forme sans en modifier le contenu. « Cette caractéristique rend l'information particulièrement rébarbative pour le juriste : il peut appréhender le support, qui est matériel; le contenu, immatériel, demeure fuyant »<sup>108</sup>. L'information est un produit autonome. Elle « ne se ramène ni à l'objet qui la porte ni au geste qui la communique, elle a une réalité intrinsèque. Indépendante à la fois de son support matériel et de la prestation qui la délivre, elle est un bien en soi [...] »<sup>109</sup>.

Le droit pénal confirme qu'il existe une distinction claire entre le produit et le service, c'est-à-dire entre le bien et la prestation puisqu'« en sanctionnant le vol d'une bande magnétique enregistrée, ce n'est pas la soustraction du support mais celle des données qu'il réprime, des données qui constituent la "chose" d'autrui [...] »<sup>110</sup>.

Les tribunaux ont pourtant adopté des raisonnements à l'effet contraire à l'égard de l'information. C'est la nature intangible de l'information elle-même qui mène à ces raisonnements. On sanctionne la prise d'une pièce de papier mais on refuse de sanctionner l'enlèvement ou le détournement de la valeur attribuée à la feuille de papier (élément tangible) par l'information (élément intangible) qui y est consolidée<sup>111</sup>. L'anomalie du résultat d'un tel raisonnement, qui fut celui de la Cour suprême du Canada dans l'arrêt *Stewart*<sup>112</sup> et celui de la Divisional Court d'Angleterre dans l'arrêt *Oxford v. Moss*<sup>113</sup>, mène à des aberrations. Suivant cette logique, seule la feuille de papier, de valeur négligeable en elle-même, représente un intérêt qui puisse faire l'objet d'un droit de propriété et ce qu'elle contient n'a aucune valeur. Un questionnaire d'examen qui a nécessité plusieurs heures de préparation n'aurait d'autre valeur que celle de la feuille de papier sur laquelle il est imprimé.

Un courant de pensée considère que l'information doit être analysée dans le cadre d'une relation et que l'on doive considérer toute la question des

106. R.G. HAMMOND, *loc. cit.*, note 60, p. 52.

107. E. MACKAAY, *loc. cit.*, note 92.

108. *Id.*, p. 39.

109. P. CATALA, « La protection juridique des productions matérielles » dans *L'appropriation de l'information*, *op. cit.*, note 92, p. 97.

110. *Ibid.*

111. Pour une analyse détaillée de cette question, voir A.S. WEINRIB, *loc. cit.*, note 51, pp. 139 et s.

112. *Ibid.*

113. *Supra*, note 35.

droits sur l'information dans l'optique de la relation entre le détenteur de l'information et la personne qui s'en sert effectivement. Ainsi, le devoir de ne pas détourner l'information découlerait non pas des qualités intrinsèques de l'information, mais de la relation entre les parties<sup>114</sup>. C'est d'ailleurs le fondement conceptuel qu'ont adopté la plupart des juges du Commonwealth et plusieurs juges américains à l'égard des causes civiles<sup>115</sup>. Cependant, cette démarche suppose une « relation préexistante » alors qu'il peut ne pas exister une telle relation pour encadrer certains faits. « En outre, cette démarche conceptuelle ne conviendrait nullement au droit pénal, qui ne jouit pas d'un éventail de relations éventuelles »<sup>116</sup>.

Certains font allusion à un droit *sui generis* en parlant du droit de l'information<sup>117</sup>. Selon le professeur Hammond<sup>118</sup>, il est naïf de croire que l'information puisse servir de concept de base à une quelconque théorie juridique. Les bouleversements qu'ont suscités le développement technologique amèneront des mutations profondes de l'infrastructure de notre société. Les juristes, les économistes et les décideurs politiques doivent conjuguer leurs efforts pour amorcer la réflexion rendue nécessaire par ces transformations et créer de nouveaux modèles en cette période de transition vers une économie basée sur l'information. Il faut aménager des nouveaux concepts et de nouvelles théories qui amèneront à considérer que l'information est une ressource, un bien public à caractère économique<sup>119</sup> qui doit principalement, dans une société libre, circuler librement<sup>120</sup>.

Dans cette optique, on peut envisager l'information comme objet de droit (*entitlement-theory*)<sup>121</sup>. Cette théorie moderne de l'information rejette la théorie du droit de propriété qui est statique pour se tourner vers une approche procédurale. Dans le cadre d'une telle démarche, on se penche sur diverses questions à savoir les motifs qui permettent de décider que les personnes précises ont ou n'ont pas accès à certaines catégories d'information. Parmi ces motifs, on retrouve divers facteurs tels que l'organisation économique, les valeurs morales, les priorités de répartition dans une société donnée, ainsi que divers motifs à

114. Voir Jennifer E. STUCKEY, « The Equitable Action for Breach of Confidence: Is Information ever Property? », (1980) *Sydney Law Review*, vol. 9, p. 402.

115. À ce sujet, il y a toute la question de la distinction à faire ou ne pas faire sur la nature de l'information selon que les causes soient civiles ou criminelles. Cette question a été abordée dans l'affaire *Stewart* et les différentes instances ne sont pas arrivées à la même conclusion sur cette question. Ainsi, alors que la Cour d'appel de l'Ontario avait considéré que si une chose est un bien aux fins du droit civil (la Cour s'était appuyée sur des décisions civiles américaines et anglaises reconnaissant que les renseignements confidentiels sont des biens), il s'ensuit qu'elle l'est également en droit criminel. La Cour suprême a décidé que si les renseignements confidentiels devaient être assimilés à des biens aux fins du droit civil, il ne s'ensuit pas nécessairement qu'ils seraient des biens en droit criminel. Cet aspect de la question devrait donc faire l'objet d'une étude particulière.

116. A.I.L.R.R., *op. cit.*, note 54, pp. 196-197.

117. Voir entre autres M. BOURGEOIS, « La protection juridique de l'information confidentielle économique, Étude de droit québécois et français », *Les cahiers de propriété intellectuelle*, octobre 1988, p. 19 et J. STUCKEY, *loc. cit.*, note 114.

118. R.G. HAMMOND, *loc. cit.*, notes 60 et 70.

119. *Id.*, note 60, p. 109.

120. U. SIEBER, *op. cit.*, note 2, p. 16.

121. Voir CALABRESI, « Property Rules, Liability Rules and Inalienability Rules: One view of the Cathedral », (1972) 85 *Harv. L. Rev.* 1089.

caractère humaniste<sup>122</sup>. Ces facteurs permettant d'identifier les personnes qui ont droit à certaines catégories d'informations, il faut ensuite répondre à la question de l'application de ce droit, puis doter ce droit des recours jugés appropriés.

C'est cette approche qu'a retenue l'A.I.L.R.R. pour proposer des mesures législatives destinées à la protection des secrets commerciaux. Cette démarche, selon l'Institut, permet d'identifier les intérêts à protéger et de trouver un équilibre entre les droits des uns à l'information et les droits des autres à garder secrète une certaine information.

## 2. Le caractère confidentiel

Des critères ont déjà été énoncés pour déterminer le caractère confidentiel de l'information. Selon le vice-chancelier Megarry de la Chancery Division en Angleterre, le caractère confidentiel de l'information se détermine par la connaissance du possesseur, selon un fondement raisonnable et selon l'usage du marché<sup>123</sup>.

Le mot « confidentiel » signifie que l'information conçue n'est pas librement accessible à tous ceux, fussent-ils peu nombreux, qui la convoitent. La confidentialité implique l'utilité technique de l'information, dont elle est le facteur : l'information est gardée par celui qui la met au point parce qu'elle est techniquement utile; réservée, elle est recherchée par des tiers potentiellement disposés à payer un prix pour l'acquérir, prix qui est la contrepartie, au minimum, d'un gain de temps et souvent la certitude d'un résultat<sup>124</sup>.

La valeur commerciale de l'information se détermine par sa valeur marchande. Ce n'est pas la nature de la chose qui lui donne un caractère commercial mais la valeur qu'elle a sur le marché. De la même manière que le « critère des choses appropriables, c'est-à-dire des biens au sens juridique du terme, n'est plus leur nature, mais leur valeur économique »<sup>125</sup>. L'évaluation de la valeur marchande est directement reliée à la confidentialité. En effet, l'information qui n'est pas confidentielle, qui a un caractère public n'a aucune valeur économique parce que toute personne peut l'obtenir gratuitement. La confidentialité apparaît donc comme le moyen d'assurer à l'information sa valeur. « La valeur, condition du droit, présuppose ainsi une exclusivité de fait. [...] Il apparaît que la possibilité d'appliquer le droit de propriété à une information est étroitement dépendant de la valeur et du caractère confidentiel de celle-ci »<sup>126</sup>.

122. A.I.L.R.R., *op. cit.*, note 54, pp. 197 et s.

123. *Thomas Marshall (Exports) Ltd. v. Guinle*, [1978] 3 All.E.R. 193, pp. 209-210 : « First, I think that the information must be information the release of which the owner believes would be injurious to him or advantageous to his rival or others. Second, I think the owner must believe that the information is confidential or secret, i.e. that it is not already in the public domain. It may be that some or all of his rival already have the information : but as long as the owner believes it to be confidential I think he is entitled to try and protect it. Third, I think that the owner's belief under the two previous headings must be reasonable. Fourth, I think that the information must be judged in the light of the usage and practices of the particular industry of trade concerned ».

124. M. BOURGEOIS, *loc. cit.*, note 117, p. 7.

125. *Id.*, p. 21. Sur la qualification de bien appliquée à l'information en raison de sa valeur, voir M. VIVANT, « La notion de "biens informationnels" », (1984) 1 *J.C.P.*, p. 3132 et D.B. LIBLING, « The Concept of Property : Property in Intangibles », (1984) 94 *L.Q.R.* 103.

126. M. BOURGEOIS, *loc. cit.*, note 117, p. 22.

### C. LA PROTECTION DE L'INFORMATION

D'autant que l'on considère qu'il y a une information qui relève du domaine public et une autre information qui n'est pas du domaine public, il faut alors déterminer quelle information aurait avantage à être protégée et comment elle devrait être protégée.

#### 1. Quelle information faut-il protéger?

Certains soutiennent que l'on devrait protéger l'information confidentielle à valeur commerciale, tel les secrets commerciaux, d'autres estiment que c'est toute l'information confidentielle qui devrait être protégée.

Dans l'état actuel du droit, l'information confidentielle n'est protégée en l'absence de dispositions législatives<sup>127</sup>, que par le droit des contrats ou dans le cadre de relations entre individus. Un régime légal de l'information devrait d'abord considérer qu'il y a deux sortes d'information : celle pour laquelle aucune protection n'est nécessaire, celle qui est de libre parcours et l'autre, celle pour laquelle une protection pourrait être nécessaire parce qu'elle ne devrait pas être accessible à tous, parce qu'elle est confidentielle. On devrait retrouver certains critères pour qu'une information puisse être qualifiée de confidentielle<sup>128</sup>. L'information ne doit pas être connue du public, elle ne doit pas être insignifiante, elle doit avoir été communiquée dans des circonstances impliquant une obligation de confiance comme par exemple, durant des relations d'affaires. De façon évidente, la nouveauté et l'originalité ne sont pas nécessaires, ce qui illustre la distinction principale entre la nature de l'information protégée par les lois sur les brevets et droits d'auteur et le droit des secrets commerciaux. Une chose n'est pas claire cependant, la qualité de confidentialité requiert-elle un élément de valeur commerciale? Dans l'affaire *Argyll v. Argyll*<sup>129</sup>, en *obiter dicta*, on a suggéré que l'élément de valeur commerciale ne soit pas nécessaire.

Il est clairement établi que l'information doit être secrète, elle pourrait être imparfaitement secrète (*imperfectly secret*)<sup>130</sup>. L'information imparfaitement secrète peut aussi être protégée, comme dans le cas d'une nouvelle qui est connue par quelques personnes mais que la majorité des gens ignorent. « By the expenditure of labour and money the plaintiffs acquired this information and in their hands it was valuable property [...] that is, that those who did not know it were willing to pay to find out about it »<sup>131</sup>.

On pourrait déterminer un quelconque statut juridique à l'information à partir de la confidentialité car tout comme il y a de nombreux avantages à divulguer certains types d'information, il existe plusieurs sortes d'information, d'œuvres, d'inventions, de nouvelles pour lesquelles on a de bonnes raisons de vouloir en assurer l'exclusivité à son possesseur et d'en limiter la circulation<sup>132</sup>.

127. Sauf pour certains types d'information confidentielle qui touchent les personnes et qui bénéficient d'une certaine protection législative. Ce sujet devrait faire l'objet d'une étude particulière.

128. Voir *infra*, II. B.2.

129. (1967) Ch. 302

130. E. TURNER, *The Law of Trade Secret*, (1962), pp. 81 et s.

131. *Exchange Telegraph v. Central News*, (1897) 2 Ch. 48, p. 53.

132. *American Flange Case* dans George FORRAI, « Confidential Information — A General Survey », (1971) 6 *Syd.L.R.*, p. 383.

Les rédacteurs du rapport *Les secrets commerciaux* estiment qu'« il existe un intérêt économique associé à la confidentialité de l'information qui constitue le secret commercial, intérêt qui est par nature un droit de propriété et que ce droit à la confidentialité de l'information mérite d'être protégé, tant en droit civil qu'en droit pénal »<sup>133</sup>.

Dans son ensemble, le problème ne se limite pas au secret commercial et peut exiger des mesures à l'égard de plusieurs points du droit<sup>134</sup>. Le secret commercial est toutefois un sous-ensemble important de ce problème et selon l'A.I.L.R.R., ce sous-ensemble est maniable aux fins de la réforme du droit.

L'A.I.L.R.R. définit le « secret commercial » comme étant une « information commerciale ou technique identifiable tenue secrète en vue d'un bénéfice économique ». Cette information est créée au prix d'efforts et dépenses souvent considérables « en vue d'obtenir un avantage sur un concurrent à l'égard des produits ou des services. Si l'information était rendue publique, cet avantage concurrentiel serait perdu »<sup>135</sup>.

L'Institut classe les secrets commerciaux en quatre catégories : 1- les secrets liés à un produit technologique (par exemple, une formule chimique); 2- les secrets technologiques (c'est-à-dire la connaissance d'un procédé ou d'une technique que personne d'autre n'a encore mis au point); 3- l'information commerciale stratégique (renseignements secrets sur les marchés ou listes secrètes de clients) et 4- les compilations spécialisées d'information qui ne sont pas connues comme telles du public et qui ont une valeur unique pour cette raison<sup>136</sup>. Le secret commercial devrait être ainsi défini :

informations, y compris entre autres une formule, un patron, une compilation, un programme, une méthode, une technique ou un procédé, ou une information contenue dans un dispositif ou mécanisme qui, à la fois

- i) est ou peut être utilisée dans un commerce ou une entreprise
- ii) n'est pas généralement connue dans ce commerce ou cette entreprise,
- iii) a une valeur économique du fait qu'elle n'est pas généralement connue,
- iv) fait l'objet d'efforts raisonnables vu les circonstances pour en préserver le secret.<sup>137</sup>

## 2. Quel droit devrait assurer la protection de l'information?

L'importance économique prise par les fichiers, l'informatique, la création et la diffusion des images, ou même les seules idées, n'est pas à établir. Ces nouvelles richesses ne correspondent pas toujours aux conditions fixées pour la reconnaissance d'une propriété intellectuelle, de sorte qu'elles ne sont naturellement couvertes par aucune protection spécifique, alors pourtant que leur valeur économique est indéniable. Il n'est donc pas étonnant que le droit pénal des atteintes juridiques aux biens se trouve sollicité de prendre en considération l'information entendue dans son sens le plus large. Comme toute richesse, l'information suscite la convoitise et son appréhension frauduleuse est ressentie comme un délit : vol, escroquerie ou abus de confiance selon le cas.

En l'état actuel du droit, le droit des propriétés intellectuelles entend assurer la protection de la mise en forme de l'information. Comme l'information

133. A.I.L.R.R., *op. cit.*, note 54, p. 304.

134. *Id.*, pp. 37 et ss.

135. *Id.*, p. 2.

136. *Id.*, p. 3.

137. *Id.*, p. 366.

elle-même ne fait pas l'objet d'un droit précis, certain et défini, on cherche souvent à assurer sa protection dans le droit des atteintes juridiques aux biens. Si les adversaires de cette tendance tentent de démontrer qu'une telle recherche est anachronique<sup>138</sup>, ses tenants sont convaincus que le concept de propriété ne doit pas être statique et qu'il doit s'adapter aux nouvelles réalités, évoluer avec le développement du droit<sup>139</sup>, puisque le droit de propriété est « l'une des notions les plus perméables aux influences économiques, politiques et sociologiques du milieu dans lequel il s'exerce »<sup>140</sup>.

La notion de chose ou de bien « est une représentation intellectuelle et nous admettons que la qualité d'objet de droit peut être attribuée à un bien immatériel, pourvu que ce bien soit considéré comme tel économiquement et qu'il soit digne de protection juridique »<sup>141</sup>. Ainsi, les propriétés intellectuelles que connaît notre droit reposeraient sur la reconnaissance du bien-information. « Le créateur révèle, fait connaître quelque chose à la collectivité (forme ou idée, peu importe) et celle-ci est traitée comme un bien et devient objet de droit. Il n'y a pas de propriété intellectuelle sans reconnaissance du bien-information »<sup>142</sup>.

L'information est souvent le fruit de durs labeurs. Elle est compilée et consolidée au prix d'efforts et d'argent et sur elle repose la réussite économique de nombreuses entreprises. Elle assure aux entreprises la concurrence économique quand ce n'est pas le monopole. « To deny that anyone has the ability to "free ride" by using, without payment, information that has been gathered or discovered by the labours of another is to deny the very foundation of human progress »<sup>143</sup>.

C'est d'ailleurs cet argument découlant de la pensée libérale moderne sur la propriété<sup>144</sup> et sur lequel se fonde la conception moderne occidentale du droit de propriété, qui semble amener certains tribunaux et commentateurs à déduire que l'information est un bien. La dépense de temps et d'argent implique un droit de propriété pour celui qui a dépensé ce temps et cet argent<sup>145</sup>.

138. Voir entre autres J.E. STUCKEY, *loc. cit.*, note 114 et R.G. HAMMOND, *loc. cit.*, note 60.

139. Voir entre autres A.S. WEINRIB, *loc. cit.*, note 51 et R. GRONDIN, *loc. cit.*, note 98.

140. J.-L. BAUDOIN, « Les aspects modernes de la propriété privée en droit québécois », (1964) I *Revue de droit comparé de l'Association québécoise pour l'étude comparative en droit*, p. 123.

141. PLANIOL et RIPERT, *Droit civil français*, t. 3, Les biens, n° 50.

142. M. VIVANT, « À propos des biens informationnels », (1984) I *J.C.P.* 3132.

143. A.S. WEINRIB, *loc. cit.*, note 51, p. 126.

144. On acquiert des droits de propriété sur une chose qui, n'appartenant à personne, est le fruit de notre travail, de nos efforts. « [...] mixing one's labour with the land or with raw materials [...] » (JOHN LOCKE, *Two Treatises of Government*, §§ 27-28, Cambridge, Ed. P. Laslett, 1960).

145. Voir D.F. LIBLING, *loc. cit.*, note 125, p. 118 : « [...] it is the expenditure of time and money which is protected by the law of property. Therefore, an entity, whether corporeal or not is property if its commercial value was brought about by the expenditure of time and money »; voir aussi P.L. BIRO and M. CHROMECEK, « Is Confidential Property? — One more Time: a critical look at the Supreme Court of Canada Decision in *R. v. Stewart* », (1988) 5 *Can. Intel. Property Review* 233, p. 237 : « In fact, it can be argued that the *Exchange Telegraph* and other such cases are not property at all, but instead a "species" of unfair competition jurisprudence. What is being protected in those cases is not the property interest in information *per se*, but rather, as Libling says, the "time and money" expended by the party seeking the protection of the law ».

On a souvent envisagé la possibilité de recourir au droit de propriété pour établir un régime juridique de l'information et en assurer la protection. Certains assurent que l'information est susceptible d'être appropriée et que l'on devrait recourir au droit de propriété pour assurer la préservation de l'information, que ce soit en reconnaissant un droit de propriété sur l'information ou en mettant plutôt l'accent sur la personne. Cependant, la doctrine classique réserve le droit de propriété aux choses corporelles pour lesquelles il a été conçu et le considère comme inapplicable aux choses incorporelles<sup>146</sup>.

Dans cette optique, plusieurs commentateurs et tribunaux prônent une dématérialisation du droit de propriété considérant que le critère des choses appropriables n'est plus leur nature, mais leur valeur économique<sup>147</sup>. Ainsi serait « objet de vol selon cette interprétation tout bien corporel ou incorporel ayant une valeur économique »<sup>148</sup>. Cette interprétation amène cependant des incohérences. Si l'on suit cette interprétation, qu'advierait-il du domaine de la propriété intellectuelle? Plutôt que de chercher à obtenir un brevet d'invention ou demander le bénéfice du droit d'auteur, on pourrait toujours faire condamner l'usurpateur en lui appliquant les peines de vol puisque dans le cas des brevets et des droits d'auteur, il s'agit aussi de valeur économique. Dans l'hypothèse où on exclurait expressément la création littéraire et l'invention brevetable de la notion de « bien » pour faciliter l'application du crime de vol à la valeur économique, comment le justifier au niveau des concepts? On pourrait dire qu'une œuvre, une formule ou une nouvelle sont aussi des informations qui ont une valeur économique.

Une conception purement économique ou quantitative de l'information exclut les indispensables distinctions. Le terme même d'information suscite alors l'équivoque. Puisqu'une telle analyse est trop globalisante pour être opératoire, il faut donc en rester à des conceptions plus rigoureuses.

En droit civil, il y a toujours le contrat qui peut être mis à contribution. On assure une certaine protection à l'information en limitant la diffusion par des clauses appropriées. Parfois, il n'est pas besoin de clause spécifique. L'employé est, même dans le silence du contrat, tenu d'une obligation de confidentialité, corrolaire d'une obligation de confiance, de loyauté, *breach of trust* en common law. En dehors de tout contrat, on peut même décider que dans certaines circonstances déterminées, l'utilisation non autorisée de l'information constitue une faute engageant la responsabilité de l'utilisateur.

Il existe aussi la théorie des agissements parasites selon laquelle tout emprunt permettant de détourner des investissements faits par un concurrent ou plus généralement par un tiers devrait être considéré comme fautif. Cette théorie permet une réaction juridique à une sorte d'enrichissement sans cause, sans avoir à respecter les règles strictes dans lesquelles le droit civil enferme ce quasi-contrat : appauvrissement et enrichissement sans cause, corrélation entre les deux, absence de cause, caractère subsidiaire de l'action, effet consistant dans une compensation limitée au terme le plus faible<sup>149</sup>.

146. M. BOURGEOIS, *loc. cit.*, note 117, p. 19.

147. Voir *id.*, p. 22; R. GRONDIN, *loc. cit.*, note 98, p. 253; D.F. LIBLING, note 145, p. 119.

148. Le crédit bancaire, à cause de sa valeur économique, a été considéré comme objet de vol même s'il n'est pas tangible dans *R. v. Scallen*, (1974) 15 C.C.C. (2d) 441.

149. J.-L. BAUDOIN, *Les obligations*, Cowansville, Éd. Yvon Blais Inc. 1983, n<sup>os</sup> 547 et s.

Au point de vue civil, l'A.I.L.R.R. propose une législation qui se caractérise par la création à titre supplétif, de deux *torts*, pour sanctionner, respectivement, l'acquisition d'une information par des moyens dits impropres, et la révélation ou l'usage de l'information par une personne tenue de ne pas agir ainsi, que ce soit ou non en vertu d'un contrat. La définition des moyens impropres, comme la définition des cas d'existence d'une relation relative à l'information confidentielle, est, pour l'essentiel, laissée à l'appréciation de la jurisprudence afin de préserver l'adaptabilité nécessaire d'un secteur en évolution. La création de sanctions très variées est également recommandée<sup>150</sup>. On perçoit aisément l'utilité de la réforme proposée pour les provinces de common law qui connaissent avec les *torts*, un système de fautes et de sanctions prédéfinies. En revanche, on perçoit moins bien l'utilité d'une telle réforme pour le Québec en raison de l'adaptabilité de son système de responsabilité civile, délictuelle et contractuelle.

Par ailleurs, l'expérience étrangère, surtout américaine, nous démontre que les secrets commerciaux représentent une catégorie d'information qui peut accéder au statut de « bien » pénalement protégé.

### III. L'INFORMATION ET LE DROIT CRIMINEL

Peut-être que l'importance croissante de l'information dans notre société et sa nouvelle vulnérabilité apportent de si profondes mutations que de nouveaux concepts juridiques fondamentaux s'imposent. Pour l'instant, le droit criminel est sollicité et il faut vérifier l'opportunité et la nécessité de s'en remettre à lui. Le droit criminel requiert des textes précis destinés à appréhender des comportements socialement nocifs bien définis; il en va de la liberté des individus. Le droit criminel n'intervient pas à chaque fois qu'il est nécessaire d'assurer une certaine protection. Avant de prévoir des mesures pénales sur une question quelconque, des moyens autres que la création de crimes doivent s'avérer insuffisants et une conduite doit causer ou menacer de causer un préjudice sérieux aux individus ou à la société. Le droit pénal doit être un outil de dernier recours qui « suppose la violation grave de valeurs importantes dans notre société »<sup>151</sup>. Il est évident que le choix d'une intervention législative dans ce domaine comme dans les autres domaines relève d'un choix politique qui devrait refléter les valeurs fondamentales qui composent une société. Le choix de protéger une quelconque forme d'information sera déterminé à partir de demandes ou de besoins existant dans une société. « À sa manière, le droit pénal réaffirme nos valeurs sociales, impose leur respect et condamne leur violation »<sup>152</sup>.

#### A. LES OBJETS DU DROIT PÉNAL

Il faut donc aborder la question de la protection pénale en examinant les objets du droit pénal et les lignes directrices qui permettent de décider si un comportement donné peut relever d'autres institutions sociales ou s'il exige une intervention du droit pénal.

150. Voir A.I.L.R.R., *op. cit.*, note 54, chapitre 10.

151. COMMISSION DE RÉFORME DU DROIT DU CANADA (ci-après C.R.D.C.), *Pour une nouvelle codification du droit pénal*, Rapport 30, 1986, p. 1.

152. C.R.D.C., *Notre droit pénal*, 1976, p. 6.



Le Comité canadien de la réforme pénale et correctionnelle a fait dans son rapport (rapport Ouimet) la recommandation suivante : « aucune conduite ne doit être décrite comme criminelle, sauf si elle constitue une grave menace pour la société et s'il est impossible de la redresser par d'autres moyens légaux »<sup>153</sup>.

La Commission de réforme du droit a proposé dans *notre droit pénal* une série de critères pour déterminer ce qui constitue et ce qui ne constitue pas un crime. Il faut se demander :

- si l'action cause un préjudice grave à autrui;
- si elle viole de quelque façon nos valeurs fondamentales, à tel point qu'elle cause un tort à la société;
- si nous sommes sûrs que les mesures nécessaires pour mettre en œuvre le droit pénal contre cette action ne violeront pas elles-mêmes nos valeurs fondamentales;
- si après réponse affirmative à ces trois questions, nous croyons que le droit pénal peut contribuer de façon substantielle à résoudre le problème.

## 1. Le préjudice à autrui

Les porte-parole de l'industrie font valoir que les pertes de secrets commerciaux sont graves. Selon certaines études empiriques, le crime informatique entraîne des pertes importantes pour les entreprises et les gouvernements et il est rare que les entreprises et les gouvernements divulguent ces pertes car cela pourrait laisser entendre qu'il existe des failles dans leur sécurité. De plus, les poursuites les obligent à révéler certains éléments du secret en public devant la cour<sup>154</sup>. La technologie facilite l'espionnage et l'espionnage représente maintenant une menace réelle même pour les entreprises bien administrées. C'est bel et bien de causer un préjudice à autrui que de détourner à son avantage le résultat du labeur et des dépenses d'autrui et de le priver de l'avantage relié à ce travail et à ces coûts.

## 2. Le tort à la société

C'est indéniablement un comportement inacceptable dans notre société de « voler » de l'information. Le jugement rendu dans l'affaire *Stewart* démontre que c'est une faiblesse de notre droit criminel de ne pas lui accorder une protection particulière. Le juge Lamer a d'ailleurs incité le législateur à intervenir dans ce domaine suggérant que « les renseignements confidentiels, et en fait toute information ayant une valeur commerciale, ont besoin d'une certaine protection en vertu de notre droit criminel »<sup>155</sup>. À cause de l'importance du rôle de l'information dans l'économie, il semble que les législateurs soient forcés d'admettre qu'il est indispensable de porter une grande attention à sa protection. « *Stealing information exceeds the limits of acceptable behaviour in a modern society* »<sup>156</sup>. « [...] a legal

153. CANADA, Ministère de la Justice, *Le droit pénal dans la société canadienne*, Ottawa, 1982.

154. Voir A.I.L.R.R., *op. cit.*, note 54, p. 55.

155. *R. v. Stewart*, *supra*, note 71, p. 978.

156. Richard B. POTTER, « Theft of a Secret: The Information Age Overtakes the Supreme Court of Canada — *R. v. Stewart* », (1989) 3 *Review of International Business Law*, p. 120.

system that fails to recognize that information itself can be stolen is simply out of touch with the role of information in modern commercial practice »<sup>157</sup>. La valeur de l'information augmente avec le développement de la technologie parce qu'elle est au cœur de cette technologie et qu'elle représente un atout majeur pour les industries, entreprises et institutions, qu'elles soient privées ou publiques.

Tandis que les juges du Commonwealth considèrent plutôt le domaine du détournement d'information en termes de comportement, les juristes américains tentent d'exposer et de justifier les raisons économiques d'une protection juridique du secret commercial en s'appuyant sur la diffusion de la technologie, la récompense de la créativité et l'intérêt personnel des employés à une mobilité de la main-d'œuvre<sup>158</sup>. Les justifications sont liées à la reconnaissance de l'importance de la production et de la diffusion d'une « bonne information » dans toute la société et sur le fait qu'il est souhaitable sur le plan économique que le comportement novateur reçoive une récompense économique quelconque<sup>159</sup>.

Compte tenu que le droit devrait viser « l'expérience organisée selon un ordre économique »<sup>160</sup> et que c'est cet ordre économique qui commande la majorité des choix politiques et législatifs, il faut tenir compte de l'importance et de la valeur de l'information confidentielle à valeur économique dans la structure et le fonctionnement de notre économie<sup>161</sup>.

D'une façon générale, on peut affirmer que le détournement d'un secret commercial est contraire à l'éthique commerciale et que « notre système socio-économique ne pourrait probablement pas survivre s'il n'y avait pas au moins certaines limites au comportement prédateur »<sup>162</sup>.

Sans une protection adéquate de l'information, il y aura peut-être moins d'incitations à l'investissement et au développement. Une intervention du droit pénal semble nécessaire pour assurer cette protection. « Resort to the criminal law power to proscribe undesirable commercial practices is today as characteristic of its exercise as has been resort thereto to curb violence or immoral conduct »<sup>163</sup>.

## B. LA MISE EN OEUVRE DU DROIT PÉNAL ET LE RESPECT DE NOS VALEURS FONDAMENTALES

Il faut bien sûr « adopter à l'égard du domaine de l'information une vue d'ensemble qui tient compte du conflit entre la libre circulation de l'information et le droit à la confidentialité »<sup>164</sup>. Ainsi, il pourrait exister des cas où le droit de propriété d'un individu à l'égard de la confidentialité d'un secret commercial devrait

157. A.S. WEINRIB, *loc. cit.*, note 51, p. 142.

158. Voir *Ruckelshaus c. Monsanto*, (1984) 81 L. Ed. (2d) 815; E. KITCH, « The Law and Economics of Rights in Valuable Information », (1980) 9 *J. Legal Studies* 683. et T. ROBISON, « The Confidence Game : An Approach to the Law about Trade Secrets », (1983) 25 *Arizona Law Rev.* 347.

159. Voir A.I.L.R.R., *op. cit.*, note 54, pp. 156 et s.

160. Ernst MACH, cité dans C.R.D.C., *Le vol et la fraude*, 1977, n° 19, p. 67.

161. E. MACKAY, *Economics of Information and Law*, Hingham Mass., U.S.A., Kluwer Nijhoff Publishing, 1982 et A.S. WEINRIB, *loc. cit.*, note 51.

162. A.I.L.R.R., *op. cit.*, note 54, pp. 152-153.

163. B. LASKIN, *Canadian Constitutional Law*, 4th ed., Toronto, Carswell, 1975, p. 824.

164. R. c. Stewart, *supra*, note 71, p. 979.

céder la préséance au droit du public au libre accès à certaines sortes d'information<sup>165</sup>.

Quant à la mobilité de la main-d'œuvre, l'expérience américaine démontre que la protection de l'information confidentielle à valeur commerciale ne semble pas trop avoir perturbé la libre circulation entre les entreprises même si un grand nombre d'États ont adopté des lois pénales, très peu de poursuites sont intentées en vertu de ces lois. L'existence de lois pénales pourrait bien avoir un effet dissuasif sur les employés.

### C. LA CONTRIBUTION DU DROIT CRIMINEL

Il nous apparaît que bien qu'une protection pénale soit utile pour assurer une certaine information, une grande part des comportements parasitaires qui affectent l'information ne sera pas réglée pour autant. Sa vulnérabilité est technique, et à bien des égards, l'intervention du droit criminel sera inutile. Des dispositions pénales peuvent exister sans que l'on puisse les appliquer. Une information peut être détruite, détournée, enlevée ou falsifiée sans que l'on sache par qui l'acte répréhensible ait été commis et comment. La pratique d'espionnage ou de vol industriel est en recrudescence et atteint même, semble-t-il, des proportions alarmantes mais, il nous semble que ce fléau est principalement relié à une perte de contrôle technique et des progrès doivent être réalisés dans ce domaine. Toutefois, le droit criminel pourrait contribuer de façon substantielle à résoudre le problème d'abord par son effet dissuasif et ensuite pour pallier à l'insuffisance du droit civil à cet égard.

Punir les actes de piraterie d'une sanction pénale démontre qu'il existe une réprobation sociale envers ces gestes et découragerait le comportement malhonnête. Devant la possibilité de se voir appliquer des peines de prison, les membres de la haute direction des entreprises ne pourraient plus considérer que prendre la décision de détourner un secret commercial est uniquement une décision comptable à prendre en fonction d'un calcul financier. Aussi, parce que les voleurs sont rarement pris, de lourdes sanctions imposées à ceux qui le sont peuvent être le seul moyen efficace de dissuasion<sup>166</sup>.

La portée restreinte des recours civils est aussi un argument en faveur d'une protection pénale. Les recours civils peuvent s'avérer vains à l'égard des sociétés qui sont à l'abri des jugements d'origine étrangère. Par exemple, une injonction civile est inefficace contre l'espion industriel qui est mobile et qui agit pour le compte du voleur ou de l'entreprise qui commande le détournement. Dans de tels cas, le droit pénal pourrait être la seule réaction efficace. Les lois pénales facilitent l'extradition des voleurs internationaux et permettent aux tribunaux de juger non la personne morale, mais la personne responsable<sup>167</sup>.

Enfin, une poursuite pénale peut soulager une entreprise du fardeau financier que représentent l'enquête et les procédures lors d'actions civiles. L'État devra alors supporter le coût des poursuites pénales mais cette protection est particulièrement importante pour les entreprises dont les ressources sont limitées.

165. Voir A.I.L.R.R., *op. cit.*, note 53, pp. 343 et ss.

166. Voir GLASBEEK. « Why Corporate Deviance is not Treated as a Crime — The need to make Profits A Dirty Word », (1984) 22 *Osgoode Hall L.J.* 393 et A.I.L.R.R., *op. cit.*, note 53, p. 184.

167. A.I.L.R.R., *id.*, p. 186.

#### D. LA CRÉATION D'INFRACTIONS

Certaines informations confidentielles pourraient faire l'objet d'un droit d'auteur. Les informations confidentielles à valeur commerciale (secrets commerciaux) devraient bénéficier d'une protection en vertu du droit criminel tandis que l'obtention malhonnête de toute autre information confidentielle pourrait dépendre du droit civil seulement.

Il faudrait donc que, pour bénéficier de la protection du *Code criminel*, l'information confidentielle ait une valeur commerciale (répondre à certains critères) et que sa prise ou son détournement soit malhonnête et entraîne ou aurait entraîné une privation ou un préjudice.

« Il faut prendre soin, dans la rédaction des lois pénales, d'éviter les infractions liées aux faits »<sup>168</sup>. Aussi, afin d'éviter de n'interdire qu'un certain sous-ensemble de comportements aberrants, l'A.I.L.R.R. propose une définition pénale qui vise la généralité : l'acquisition, la divulgation et l'utilisation représenteraient des méthodes par lesquelles on peut porter atteinte à l'avantage économique lié à un secret commercial<sup>169</sup>.

L'Institut propose en premier lieu la création de deux infractions essentielles, l'une réprimant l'acquisition, la révélation ou l'utilisation frauduleuse d'un secret commercial au préjudice de son détenteur légitime (*misappropriation*), l'autre les manœuvres incitant une personne à révéler ou utiliser un secret commercial (*fraudulent misappropriation*). En second lieu, il propose la modification de nombreux articles du *Code criminel*, ayant pour objet la protection des biens, afin d'y intégrer ou d'en soustraire le secret commercial. Les infractions proposées visent l'ingérence illicite à l'égard de l'avantage économique que procure la connaissance d'un secret commercial. Selon l'Institut, l'élément supplémentaire qui justifie le recours au droit pénal pour punir les cas de détournement est le caractère répréhensible de la conduite et non une quelconque caractéristique de la classe d'information protégée. L'emploi de dispositions pénales viserait donc non pas un ensemble défini d'informations qui justifient une protection plus considérable, mais bien les cas de détournements qui sont particulièrement répréhensibles. Ce ne serait pas le droit de possession de l'information qui serait protégé par le droit pénal mais bien « le droit économique à la confidentialité de cette information ».

On peut suggérer qu'une définition du « vol » plus générale et plus étendue serait préférable à une infraction particulière relative à certaines informations sous prétexte qu'une seule infraction pour couvrir toute appropriation malhonnête diminuerait le nombre d'interdictions prévues au *Code criminel*<sup>170</sup>. Le droit devrait certes s'en tenir à des généralités, mis à part, cependant, certains éléments particuliers<sup>171</sup>. En l'occurrence, l'application des notions de droit de propriété et des dispositions traditionnelles de vol à l'information n'est pas souhaitable puisque ces notions ont été développées pour s'adapter à des objets matériels. Néanmoins, la spécificité de l'information n'est pas un obstacle à une reconnaissance par le droit pénal. Sa spécificité requiert toutefois la création de dispositions spéciales.

168. *Id.*, p. 313.

169. *Id.*, p. 314.

170. Voir R. GRONDIN, *loc. cit.*, note 98, p. 261.

171. C.R.D.C., *op. cit.*, note 152, p. 67.

## 1. Les infractions relatives à des espèces particulières de biens

L'article 2 du *Code criminel* définit « biens » comme désignant « les biens meubles et immeubles de tous genres » et l'article 322 définit le vol comme la prise de possession « d'une chose quelconque, animée ou inanimée ». Il en résulte un très grand champ d'application du vol, les biens pouvant faire l'objet d'un vol étant très nombreux. En vertu du Code, les biens incorporels tels que le crédit ou les fonds déposés dans une banque peuvent aussi faire l'objet d'un vol<sup>172</sup>. L'infraction générale de vol a donc un vaste domaine d'application. Certains biens cependant peuvent justifier des dispositions spéciales. Il en est ainsi de l'électricité (article 326), des cartes de crédit (article 342), du courrier (article 356), des mines (article 396) et de la monnaie (article 459). Ces objets peuvent justifier des articles pour différentes raisons<sup>173</sup>. Par exemple, l'article 326 prévoit des dispositions spéciales pour assurer que l'usage frauduleux de l'électricité et des télécommunications constitue un crime. Ces dispositions spéciales sont nécessaires puisque « l'électricité et les télécommunications ne constituent pas, dans le langage ordinaire, des objets et on ne peut non plus les prendre ou les détourner au même titre que des objets matériels ordinaires »<sup>174</sup>. On peut également mentionner à cet égard l'article 327 qui concerne la possession de dispositifs permettant de détourner des installations ou un service de télécommunications, et l'article 342.1 concernant l'utilisation non autorisée d'ordinateur.

L'information ne constitue pas, dans le langage ordinaire, un objet et on ne peut non plus la prendre et la détourner au même titre que des objets matériels ordinaires. Tout comme pour l'électricité et les télécommunications, à cause de sa spécificité, pour s'assurer que l'usage frauduleux de l'information constitue un crime, il faut recourir à certaines dispositions spéciales. L'information constitue une valeur particulière qui peut nécessiter une protection spéciale.

## 2. Le statut des nouvelles incriminations

Quel statut doit-on donner aux nouvelles incriminations touchant à l'information? Il s'agit de savoir s'il faut légiférer au moyen d'une loi spéciale ou s'il y a lieu, au contraire d'intégrer des textes nouveaux dans le *Code criminel*.

Faut-il utiliser et aménager les incriminations existantes : vol, escroquerie, fraude, méfait, abus de confiance, falsification, etc. ou convient-il de créer des délits nouveaux? Il peut être utile de considérer certains actes répréhensibles concernant l'information comme des infractions distinctes, non pas sous la rubrique générale du vol mais plutôt sous une rubrique distincte d'infractions concernant l'information.

En ce qui concerne la protection de l'intégrité de l'information, tout comme pour la protection de l'usage exclusif de l'information, le droit criminel a un caractère fragmentaire et on ne devrait y avoir recours qu'en ultime recours. Par conséquent, il est impossible de protéger l'intégrité de l'information grâce à une disposition criminelle générale de la même façon que la propriété corporelle est protégée par des lois sur les dommages à la propriété. Néanmoins, en protégeant

---

172. R. v. Scallen, *supra*, note 128.

173. Voir C.R.D.C., *op. cit.*, note 152, pp. 66 et s.

174. *Ibid.*

l'intégrité de données spécifiques, le droit criminel peut jouer un rôle important. Ceci serait particulièrement applicable aux données entreposées et transmises dans des systèmes informatiques.

Il conviendrait de créer un chapitre distinct du *Code criminel* se rapportant à la protection de l'information. Il serait ainsi possible d'en arriver à une systématisation nette et à une différenciation entre des règles générales pour la protection de l'information et des règles spécifiques pour les données informatisées. Un tel chapitre aurait également l'avantage de pouvoir intégrer d'éventuelles dispositions visant d'autres sortes d'agissements répréhensibles touchant à d'autres types d'information. Ce concept de « droit criminel de l'information » est donc souhaitable pour l'aménagement de nouvelles dispositions criminelles touchant à un secteur de droit en développement.

### CONCLUSION

Une protection des secrets commerciaux ne règlera pas toute la question mais le besoin pour une telle protection existe au Canada et les secrets commerciaux représentent un ensemble maniable dans ce domaine du droit. Au plan international, il existe une tendance vers la protection des secrets commerciaux. Afin de parvenir à un consensus international dans ce domaine, on pourrait souhaiter que tous les systèmes juridiques prévoient une protection pénale des secrets commerciaux — soit par le biais du *Code criminel* ou de lois sur la concurrence déloyale — appuyée de dispositions de droit civil appropriées touchant la concurrence déloyale<sup>175</sup>. Ces dispositions pénales et civiles devraient s'appliquer de façon générale aux secrets commerciaux et non pas se limiter à l'ordinateur et aux données informatisées. Cependant afin d'éviter une monopolisation de l'information, la protection des secrets commerciaux devrait se limiter à certaines façons intolérables d'obtenir l'information et ne pas s'étendre à l'information *per se*<sup>176</sup>.

Les infractions spécifiques, du type de celles que suggère le rapport de l'A.I.L.R.R., sont orientées vers l'information. Le secret commercial est défini en fonction de l'information. Les infractions proposées pourraient donc avoir leur place au sein de ce nouveau chapitre réservé à l'information avec les dispositions sur l'utilisation non autorisée d'ordinateur qui, bien que de façon plus équivoque, font aussi référence à l'information. Ainsi, si de nouveaux sous-ensembles d'information viennent à accéder au statut d'éléments maniables et protégeables pour les fins du droit pénal, ils pourront trouver leur place au sein d'une rubrique du *Code criminel* réservé à l'information.

Devant de phénomène de l'émergence du droit criminel de l'information, il faudra certes proposer de nouvelles définitions dont l'élaboration conduira sans doute à reconsidérer le droit de la propriété intellectuelle et la hiérarchie de la protection des différents types d'informations qui font l'objet de protection. De nouveaux paradigmes juridiques s'imposent avec comme fondement la liberté de l'information et la protection des intérêts particuliers du détenteur d'information.

175. Voir U. SIEBER, *op. cit.*, note 2, chapitre V A 2.

176. Voir U. SIEBER, « Legal Protection of Computer Data, Programs, and Semiconductor Products — A Comparative Analysis with Suggestions for Legal Policy » dans : ICC, INTERNATIONAL CHAMBER OF COMMERCE (ed.), *International Contracts for Sale of Information Services*, 1988; R.G. HAMMOND, *loc. cit.*, note 70 et A.I.L.R.R., *Protection of Trade Secrets*, Report for Discussion No 1, 1984.

ainsi que les intérêts du « sujet » concerné par l'information personnelle. Toutes dispositions interdisant le détournement d'information doivent s'interpréter sous réserve des dispositions de la *Charte canadienne des droits et libertés*, notamment la garantie de la vie, de la liberté et de la sécurité de la personne (article 7), la protection contre les fouilles, les perquisitions ou les saisies (article 8), le droit à un procès public (alinéa 11d)) et l'interdiction d'utiliser les témoignages incriminants (article 13). Ces droits et libertés ne peuvent être restreints que dans les limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique (article 1).

L'utilisation croissante des systèmes électroniques pour compiler l'information pose aussi de nouveaux problèmes procéduraux<sup>177</sup>. De plus, la mobilité des données à travers les systèmes automatisés, rend nécessaire une harmonisation du droit tant criminel que non criminel, au niveau international. Par exemple, un crime peut être commis à l'aide d'un ordinateur dans un pays et ses résultats peuvent faire surface dans un autre pays. Une protection internationale est aussi importante pour les systèmes de télécommunication qui traversent les frontières de plusieurs pays. Il existe également un besoin d'harmonisation internationale en ce qui concerne l'utilisation de programmes importés de pays étrangers et la protection des programmes exportés vers d'autres pays.

Sur ces questions, plusieurs organismes internationaux réalisent des études et tentent de dégager des consensus et d'intégrer le plus grand nombre de pays possible aux divers travaux dans ce domaine. Des recherches devraient donc être réalisées à l'échelle nationale sur ces diverses questions.

---

177. Voir U. SIEBER, *op. cit.*, note 2, chapitre IV. Ces problèmes touchent notamment l'obtention et l'utilisation de données dans un procès criminel particulièrement celles qui sont obtenues à l'étranger, l'admissibilité de la preuve, la saisie. Voir aussi pour la définition d'objets de saisie, C.R.D.C., rapport N° 24, *Search and Seizure*, 1984, p. 11 (« objects of seizure » means « things, funds, and information ») et C.R.D.C. Document de travail n° 30, *Les pouvoirs de la police les fouilles, les perquisitions et les saisies en droit pénal*, 1983, pp. 155 et s.