Université de Montréal

Les infractions portant atteinte à la sécurité du système informatique d'une entreprise

par
Ibtissem Maalaoui

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maîtrise en droit (L.L.M.)
option droit des affaires

Septembre, 2011

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

Les infractions portant atteinte à la sécurité du système informatique d'une entreprise

Présenté par:
Ibtissem Maalaoui

a été évalué par un jury composé des personnes suivantes:

Geneviève DUFOUR
président-rapporteur

Vincent GAUTRAIS
directeur de recherche

Diane LABRÈCHE
membre du jury
(dissidence)

RÉSUMÉ

Les nouvelles technologies de l'information et des communications occupent aujourd'hui une place importante dans les entreprises, quelle que soit la taille ou le(s) domaine(s) d'activité de ces dernières. Elles participent de manière positive au développement de la vie économique. Elles sont toutefois à l'origine d'une nouvelle forme de criminalité qui menace la sécurité et l'intégrité des systèmes informatiques dans l'entreprise. Celle-ci est d'une ampleur difficile à évaluer, mais surtout difficile à maîtriser avec les dispositions législatives déjà en place, laissant par là même apparaître qu'une adaptation au niveau juridique est inévitable. Certains pays industrialisés ont ainsi décidé de mettre en place un cadre juridique adéquat pour garantir aux entreprises la sécurité de leurs systèmes informatiques. Notre étude va justement porter sur les dispositifs mis en place par deux systèmes juridiques différents. Forcés de prendre en compte une réalité nouvelle – qui n'existait pas nécessairement il y a plusieurs années –, la France et le Canada ont décidé de modifier respectivement leurs codes pénal et criminel en leur ajoutant des dispositions qui répriment de nouvelles infractions.

À travers cet exposé, nous allons analyser les infractions qui portent atteinte à la sécurité du système informatique de l'entreprise à la lumière des outils juridiques mis en place. Nous allons mesurer leur degré d'efficacité face à la réalité informatique. En d'autres termes, il s'agit pour nous de déterminer si le droit va répondre ou non aux besoins de l'informatique.

Mots clefs : nouvelles technologies de l'information et des communications - atteintes - sécurité - système informatique - entreprise - droit pénal.

SUMMARY

The new information and communication technologies (NICT) currently play an important role in companies, regardless of their size or field of activity; in addition they contribute positively to the economy. However, their use has led to NICT-related criminality, which threatens the security and integrity of the companies' computer systems. NICT-related criminality has grown exponentially; its increase is hard to assess, and especially hard to control using the existing legislative provisions. Hence, legal adaptations appear unavoidable. Several First World countries have decided to set up, through different means, an adequate legal framework to guarantee the security of companies' computer systems.

Our study will focus precisely on the mechanisms that have been set by two different legal systems. France and Canada, which had to take into account a new reality–new to at least some extent–have decided to amend their respective penal and criminal codes by adding provisions that penalize further infringements. In this work, we will analyze the crimes that undermine the security of the companies' computer systems in light of the legal tools in place. We will asess how effectively they face today's computer world and will determine whether or not the law will meet or not the needs of this type of technology.

Key words: new information and communication technologies, security, computer system, breach, company, criminal law.

TABLE DES MATIÈRES

ABRÉVIATIONS

A.L.D.	Actualité Législative Dalloz
Alta. Prov. Ct	Alberta Provincial Court
Art.	Article
B-C. C.A.	British Columbia Court of Appeal
Bull. crim.	Bulletin des arrêts de la Cour de cassation en matière criminelle
C.A. Qué	Cour d'appel du Québec
C.C.C.	Canadian Criminal Cases
C.cr.	Code criminel canadien
C.F.	Cour fédérale du Canada
C.F.A.A.	Computer Fraud and Abuse Act
CLUSIF	Club de sécurité de l'information français
Comm.	Commentaire
Comm. com. élect	Communication commerce électronique
C.pén.	Code pénal français
C.R.	Criminal Reports
Crim.	Cour de cassation, Chambre criminelle
C.S.P.	Cour des sessions de la paix du Québec
D.	Recueil Dalloz (Paris)
D. I.	Droit de l'Informatique
Éd.	Édition, éditeur

Fasc.	Fascicule
Gaz. Pal.	Gazette du Palais
Ont. H.Ct.	Ontario Supreme Court, High Court of Justice
J.-Cl. Comm.	Juris-classeur Communication
J.-Cl. Pén.	Juris-classeur Pénal
J.C.P.	Semaine juridique (édition générale)
J.C.P. G	La Semaine juridique (édition générale)
J.C.P. E	Semaine juridique, entreprise et affaires
J.E.	Jurisprudence Express
J.O.	Journal Officiel de la République Française
J.O.C.E.	Journal Officiel de la Communauté Européenne
J.Q.	Jugements du Québec
Lamy Dt. de l'Inf.	Lamy Droit de l'Informatique
L.J.	Law Journal
LPA	Les Petites Affiches
L.R.C.	Lois refondues du Canada (depuis 1985)
Nfld. C.A.	Newfoundland Court of Appeal
NY. Ct. App.	Court of Appeals of New York
N.Y.Civ. Ct.	Civil Court, City of New York
Obs.	Observation
O.C.D.E.	Organisation de coopération et de developpement économiques
Ont. S.C.J.	Ontario Superior Court of Justice
Par.	Paragraphe

Préc.	Précité(e)
P.U. d'Aix-Marseille	Presses universitaires d'Aix-Marseille
P.U. d'Aix-en-Provence	Presses universitaires d'Aix-en-Provence
P.U.F.	Presses universitaires françaises
R.C.S.	Recueil de la Cour Suprême du Canada
R.D.P.	Revue de Droit Public
R.J.Q.	Recueils de jurisprudence du Québec
Sask. Prov. Ct.	Saskatchewan Provincial Court
Somm.	Sommaire
T.I.C.	Technologies de l'information et des communications
Tex. App.	Court of Appeals of Texas
TGI	Tribunal de Grande Instance
Trib. corr.	Tribunal correctionnel (France)
U.S.C.	United States Code
Vand. L. Rev.	Vanderbilt Law Review
Vt. L. Rev.	Vermont Law Review
Wash. Rev. Code Ann.	Washington Review Code Annotated
Wis. Ct. App.	Court of Appeals of Wisconsin

Je dédie ce travail à ma sœur Olfa et
à ma fille Mona.

REMERCIEMENTS

Je tiens à remercier Monsieur le professeur Vincent Gautrais pour avoir accepté d'être mon directeur de recherche et cela, malgré toutes ses préoccupations. Je le remercie aussi pour les judicieux conseils qu'il m'a prodigués tout au long de la rédaction de ce mémoire.

Je remercie également ma famille, particulièrement ma sœur, qui m'a permis de venir au Canada et m'a offert la possibilité de continuer mes études alors que j'avais perdu tout espoir. Je la remercie de m'avoir soutenue tout au long de la réalisation de mon mémoire de maîtrise; je la remercie également pour ses conseils, ses encouragements et surtout sa générosité.

« L'informatique, comme le droit, infiltre tous les capillaires de la vie sociale. Mais leurs réseaux de diffusion ne sont pas séparés comme ceux de la lymphe et du sang. Bien au contraire, l'informatique et le droit se mêlent chaque jour davantage dans les canaux communs. La première paraît désormais vouée à susciter de nouvelles règles dans toutes les branches du second : propriétés intellectuelles, contrats, preuve, dématérialisation des titres, traitements nominatifs, fraude et délinquance... »[1]

[1] Pierre CATALA, *Le droit à l'épreuve du numérique – Jus ex machina*, PUF, 1998, p. 9.

INTRODUCTION

Les nouvelles technologies de l'information et des communications (ci-après TIC) occupent une place très importante dans la stratégie des sociétés du monde entier et ce, quelles que soient leur taille ou la nature de leurs activités. En effet, l'entreprise, pour faire face à l'accroissement de la concurrence et à l'accélération du changement économique, doit apprendre à faire mieux, plus vite et moins cher. Et c'est justement à travers l'emploi de ces moyens que l'entreprise va réaliser cet objectif. Une étude portant sur la croissance réalisée par l'OCDE (Organisation de Coopération et de Développement Économiques) a démontré que les TIC constituaient un facteur déterminant dans la productivité et la croissance de l'entreprise[2].

L'évolution, l'optimisation et la banalisation de l'informatique ont même rendu les entreprises dépendantes des TIC tels que les logiciels, l'Internet, l'intranet et la messagerie électronique. Un exemple simple : imaginez ce qui se passerait dans l'entreprise si les employés devaient se passer d'Internet, du courriel ou même du téléphone pendant une journée de travail…[3] Une enquête, menée en 2010 par le

---

[2] « La diffusion des TIC dans les entreprises : examens collectifs par pays », OCDE, en ligne : <http://www.oecd.org/document/35/0,3343,fr_2649_33757_35223715_1_1_1_1,00.html>, (consulté le 26 Novembre 2009)
Sur le même sujet voir : *Une nouvelle économie? Transformation du rôle de l'innovation et des technologies de l'information dans la croissance*, OCDE, éd.2000, p.53. L'étude réalisée par l'OCDE a démontré que :

1. Les TIC est un facteur important de performance en matière de croissance;
2. Dans de nombreux cas, les TIC, particulièrement depuis l'émergence de l'Internet, du World Wide Web, des navigateurs et du commerce électronique, ont joué un rôle important en faveur de l'innovation dans l'entreprise;
3. L'utilisation des TIC dans l'entreprise lui permet d'améliorer sa productivité;
4. L'utilisation des TIC dans l'entreprise a permis a l'entreprise de développer de nouvelles façons de réduire les couts de la recherche de nouvelles idées.

Voir aussi, *Perspectives des technologies de l'information de l'OCDE,* éd. 2008

[3] Une enquête menée par PC World, en collaboration avec Computer Associates en 2005, a démontré que si la ligne d'internet n'est pas disponible pendant une heure, si le site Web est inaccessible pendant une heure ou encore si le système de courriels est paralysé pendant une heure par une attaque virale… pour une organisation de 10 a 20 collaborateurs, la perte de productivité dépasse

CLUSIF auprès de 350 entreprises françaises de plus de 200 salariés, a montré que 73% d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques (avec un maximum de 83% pour le secteur du commerce)[4].

La dépendance aux TIC n'est certainement pas sans revers. Elle constitue des risques potentiels pour l'entreprise[5]. Outre des incidents techniques, on assiste aujourd'hui à une forme de criminalité nouvelle et plus complexe. Quelques exemples méritent d'être cités afin de clarifier ce phénomène. En France, une stagiaire chinoise chez l'équipementier automobile Valeo a été accusée d'avoir volé des informations confidentielles. Les faits de cette affaire remontent à 2005, lorsque l'entreprise a constaté la disparition d'informations de l'ordinateur mis à la disposition de la stagiaire et le téléchargement de données confidentielles présentes sur le réseau interne. La stagiaire a toujours nié tout piratage en expliquant que l'ordinateur de la société étant saturé, elle l'avait vidé et transféré les données sur son disque dur personnel pour les sauvegarder. Elle affirmait ne pas avoir prêté attention en signant la charte de confidentialité et ignorer qu'il était interdit d'utiliser un disque externe ; elle niait en outre avoir transmis ces données à quiconque. L'entreprise a porté plainte contre la stagiaire pour vol de données informatiques en se fondant sur « un accès frauduleux dans un système de traitement automatisé de données et abus de confiance »[6]. En décembre 2010, le moteur de recherche Google

---

rapidement les 1000 euros, sans tenir compte du manque a gagner et du préjudice en terme d'image de marque. Voir Jan-Frans LEMMENS, *Les PME et la sécurité : « vers une approche intégrale ? »*, Best Of Publishing – IDG Belgium, 2007.

[4] « Menaces informatiques et pratiques de sécurité en France », CLUSIF – 2010, en ligne : <https://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf>, (consulté le 11 juin 2011), p.16.

[5] Exemple, selon l'association anglaise des moyens de paiement (APACS), la fraude bancaire en ligne a coûté 52,5 millions de livres, soit pratiquement 57 millions d'euros en 2008. Au-delà de la valeur du préjudice, l'association relève la forte croissance des fraudes sur Internet par rapport à l'année précédente. En 2007, l'association avait évalué le coût de la fraude à 22,6 millions de livres. En un an, la croissance a donc été de 132%. Une explosion qui peut s'expliquer en partie par la croissance du nombre d'utilisateurs de la banque sur Internet. En France, le préjudice est difficile à estimer. En ligne:
<http://www.zdnet.fr/actualites/internet/0,39020774,39388908,00.htm >
(consulté le 16 Novembre 2009)

[6] « Deux mois ferme pour la stagiaire chinoise de Valeo », TF1 NEWS, 18 déc. 2007, en ligne :

a affirmé avoir subi deux attaques. La première a ciblé un système qu'il a mis en place et visait à fournir aux autorités chinoises des informations sur ses utilisateurs dans le but d'accéder aux comptes Internet Gmail de militants chinois défenseurs des droits de l'Homme. La seconde attaque a aussi ciblé des militants des droits de l'Homme installés en Europe, en Chine et aux États-Unis. Leurs mots de passe de messagerie ont été récupérés et des logiciels malveillants ont été installés sur leurs ordinateurs portables. Cette attaque a également ciblé au moins vingt autres entreprises travaillant dans différents domaines (Internet, finance, technologies, médias, chimie...)[7]. En février 2011, l'entreprise de sécurité McAfee a annoncé que des pirates chinois s'étaient introduits illicitement dans les ordinateurs de cinq multinationales pétrolières. Pendant plus de deux ans, ils ont pu accéder aux données financières et à d'autres informations détaillées sur les stocks de pétrole. Le tout représenterait des renseignements d'une valeur de plusieurs « millions de dollars »[8]. À la mi-avril 2011, Sony a subi une série d'attaques informatiques. Un groupe de pirates informatiques, qui a revendiqué ces attaques, a prétendu vouloir s'amuser et lutter contre l'ennui qui pèse sur la cybercommunauté; il dénonçait également la vulnérabilité du système informatique de Sony. Ce groupe a affirmé que s'introduire dans ce système avait été un jeu d'enfant en exploitant simplement « de vulgaires et ordinaires » failles de sécurité. Bien entendu, les conséquences de telles intrusions sont très lourdes pour l'entreprise. Le 6 juin 2011,

---

<http://lci.tf1.fr/france/justice/2007-12/deux-mois-ferme-pour-stagiaire-chinoise-valeo-4866420.html>, (consulté le 21 juin 2011)

[7] « Comment Google a été attaqué depuis la Chine », Le Figaro. Fr, 24 février 2010, en ligne : < http://www.lefigaro.fr/web/2010/01/13/01022-20100113ARTFIG00819-comment-google-a-ete-attaque-depuis-la-chine-.php>, (consulté le 08 juin 2011)

[8] « Des espions chinois dans les ordinateurs des géants du pétrole », La Tribune.fr, 28 janvier 2011, en ligne :
<http://www.latribune.fr/entreprises-finance/industrie/energie environnement/20110210trib000600289/des-espions-chinois-dans-les-ordinateurs-des-geants-du-petrole-.html>, (consulté le 08 juin 2011)

Sony a signalé avoir été victime d'un autre accès illicite sur le site de sa filiale européenne[9].

À travers ces quelques exemples, nous constatons d'abord que le risque pour l'entreprise peut être interne – issu du comportement délictuel de certains employés – ou externe, provenant donc d'attaques extérieures. Nous constatons ensuite que la menace est bien réelle et qu'elle vise le patrimoine informationnel de l'entreprise et ce, quel que soit le domaine de son activité. Mais nous constatons surtout que les crimes liés à l'utilisation des TIC ont évolué. Aujourd'hui, on ne vole plus un ordinateur portable pour sa technologie, mais plutôt pour les informations qu'il contient. On pénètre un réseau non pas pour accéder à des bases de données mais par esprit « ludique »[10], comme l'ont d'ailleurs bien exprimé les pirates qui ont attaqué les sites de Sony. En effet, les cybercriminels se sont adaptés à l'évolution des technologies de l'information. Désormais, ils n'ont plus aucune limite pour perpétrer leurs actes.

Pour contourner ces risques, il est donc indispensable d'assurer la sécurité des systèmes informatiques de l'entreprise. À cet effet, les politiques et initiatives gouvernementales sont essentielles pour aider l'entreprise à atteindre cet objectif. Une étude réalisée par l'OCDE a démontré que le nombre de gouvernements qui accordent un degré élevé de priorité à la sécurité des systèmes et réseaux d'information a augmenté depuis 2008 ; par ailleurs, en 2010, dix priorités d'action à long terme dans le domaine des TIC ont été fixées, avec au premier rang la sécurité des systèmes informatiques et des réseaux[11]. En outre, les entreprises doivent aussi agir. Un bon nombre d'entre elles ayant compris l'importance cruciale d'une protection efficace des technologies de l'information, elles ont mis en place

---

[9] « Sony victime d'une nouvelle intrusion informatique », Le Monde.fr, 06, juin 2011, en ligne :<http://www.lemonde.fr/technologies/article/2011/06/06/sony-victime-d-une-nouvelle-intrusion-informatique_1532338_651865.html >, (consulté le 08 juin 2011)

[10] Daniel MARTIN, *La criminalité informatique*, Puf, 1997, p.23.

[11] «Perspectives des technologies de l'information de l'OCDE 2010, principales conclusions», OCDE, en ligne : <http://www.oecd.org/dataoecd/4/9/46478073.pdf>, (consulté le 08 juin 2011), p. 7.

des mesures de sécurité afin de lutter contre les imprudences des employés, et surtout contre les tentatives d'intrusions virtuelles et leurs conséquences graves sur les données se trouvant dans le système informatique de l'entreprise. On parle notamment de pare-feu, cryptage, mot de passe, etc.

Toutefois, les démarches entreprises pour mettre en place des techniques de sécurité, bien qu'efficaces pour maintenir la sécurité des systèmes informatiques dans l'entreprise, restent tout de même insuffisantes. Les malveillances et les incidents de sécurité sont toujours bien présents : intrusions, attaques virales, vols de matériel informatique, accroissement des problèmes de divulgation d'information et attaques logiques ciblées sont hélas toujours au menu! Une enquête réalisée en 2008 a démontré qu'à la suite de la mise en place des dispositifs de sécurité, une amélioration a été constatée notamment concernant les attaques virales. Par contre, la lutte contre les intrusions continue de préoccuper de plus en plus les entreprises[12]. D'où la nécessité de faire entrer en jeu des outils juridiques pour garantir cette sécurité. On parle notamment des dispositions pénales qui doivent sanctionner l'auteur de toute atteinte intentionnelle portée à l'égard d'un système informatique.

---

[12] Une enquête internationale réalisée en 2008 par Devoteam Consulting, portant sur la sécurité des systèmes d'informations, a démontré que :

1. La lutte contre les attaques virales est présente de façon régulière chez 44% des entreprises, alors que la lutte contre les intrusions préoccupe de plus en plus les entreprises : 35% en 2007 contre 12,5% en 2006.
2. Le pourcentage du budget informatique alloué à la sécurité au sein de l'entreprise en 2008 est soit constant, soit en augmentation par rapport à 2007.
3. Une amélioration concernant les attaques virales a été constatée suite à la mise en place des dispositifs de sécurité :
   - En 2007, 52% des entreprises interrogées ont été victimes d'attaques virales sans conséquences majeures contre 57% en 2006;
   - 7% des entreprises ont subi des conséquences significatives contre 8% en 2006;
   - 39% des entreprises n'ont pas constaté d'attaque contre 35% en 2006 ;
   - Parmi les entreprises victimes d'atteinte à la sécurité de leur système informatique (intrusion, vol de données, indisponibilité, virus, etc.) seules 12% ont pu identifier des pertes financières.

En ligne:
<http ://www.apogeecom.fr/images/File/marketing/Enquete_secu_2008_080606_BD.pdf>,
(consulté le 21 janvier 2009)

Désormais, les législateurs – notamment ceux des pays industrialisés – sont placés face à un défi énorme : assurer la sécurité des systèmes informatiques et des données contre une criminalité nouvelle qui ne cesse d'évoluer. Ils se sont alors interrogés sur l'efficacité de leurs dispositions pénales, prises à une époque où l'innovation technologique dont on bénéficie actuellement en était à ses balbutiements. Ainsi, il semble que l'introduction de nouvelles mesures législatives soit nécessaire dans ces pays étant donné que les dispositions en place sont devenues insuffisantes, et surtout dépassées.

De leur côté, les États-Unis ont fait le premier pas dans cette direction en adoptant, au niveau fédéral[13], le « Computer Fraud and Abuse Act »[14] en 1984[15]. Le Canada et la France ont quant à eux préféré modifier respectivement leurs codes criminel et pénal. Le Canada a alors adopté la loi de 1985 modifiant le droit

[13] Les 50 États Américains ont eux aussi adopté des lois pour interdire la fraude informatique. Florida a été le premier État à adopter en août 1978 une loi intitulée «Florida Computer Crimes Act ». Voir: A. H. SCOTT, *Computer and Intellectual Property Crime: Federal and state Law*, 639-1300 (2001). L'État de Vermont fût le dernier à adopter une loi en mai 1999. Pour une description détaillée de la loi et de ses origines, voir : J.A. TOWER, «Hacking Vermont's Computer Crimes Statute », 25 *VT. L. REV*. 945 (2001)

[14] 18 U.S.C. s. 1030, J.J. FALVEY, A.M. MCCALLEN, « General Legal Issues », 2 *INTER. L. and PRAC.* § 26:9(2009) (Wec) (Site consulté le 08 janvier 2010)

[15] Le « Computer Fraud and Abuse Act » est adopté en 1984 par le congrès américain suite à une tentative de régularisation d'internet. Cependant, la limitation de son champ d'application à la protection des intérêts du gouvernement fédéral a exposé le CFAA à beaucoup de critiques. L'adoption du CFAA était la première action mise en place pour contrôler les fraudes reliées aux ordinateurs. Toutefois, le congrès reconnaît que cette législation est incomplète et qu'elle renferme plusieurs lacunes. Pour limiter ces critiques, le « Computer Fraud and Abuse Act » a été amendé en 1986. L'amendement était majeur. D'une part il y a eu un ajout, que je juge très significatif, relatif à la création de trois nouvelles incriminations :

1. Accès avec intention de frauder à la sous section (a)(4)
2. Modifier, endommager ou détruire les données ou empêcher son utilisation à la sous section (a)(5)
3. Accès avec intention de trafic de mot de passe à la sous section (a)(6)

D'un autre côté, un ajout aussi important que le premier caractérise l'amendement de 1986. Il s'agit des définitions apportées pour les mots clefs à la sous section (e).

Voir: D. S. GRIFFITH, «The Computer Fraud and Abuse Act of 1986: A Measured Respond to a Growing Problem», 43 *VAND. L. REV*. 456 (1990)

D'autres amendements se sont ensuite succédés en 1988, 1989, 1990, 1994, 1996, 2001et 2002. Voir: J.A.-M. ADAMS, «Controlling cyberspace: Applying the computer fraud and abuse act to the internet», 12 *SANTA CLARA COMPUTER & HIGH TECH. L.J.* 403 (1996)

pénal[16] ; il fut suivi de la France avec la loi « Godfrain », adoptée le 5 janvier 1988[17]. Malgré qu'elles présentent certaines différences, les dispositions adoptées

[16]*Loi de 1985 modifiant le droit pénal*, S.C. 1985, C-18, c. 19, art. 46 et art. 58, a apporté des modifications législatives au Code Criminel. Ces modifications sont inspirées en grande partie des recommandations du sous-comité sur les infractions relatives aux ordinateurs, et elles sont entrées en vigueur le 4 décembre 1985. Elles concernent :

1. L'interdiction de l'utilisation non autorisée d'un ordinateur prévue dans l'article 342.1du C.cr.
2. Le méfait concernant des données prévues dans l'article 430 du C.cr

[17] Avant l'adoption de la loi «Godfrain », qui prend le nom de son initiateur, le droit pénal de l'informatique en France était «pratiquement inexistant » dans le domaine de la protection pénale des biens, à l'exception de la protection des logiciels à travers le droit d'auteur. Pour combler ce vide, une proposition de loi était présentée par M. Jacques Godfrain et un groupe de députés en août 1986 (Doc. AN 1985-1986, 3e session extraordinaire, n° 352). Elle contient deux dispositions :

1 La création de deux nouvelles incriminations :
   a- L'entrée, sans apparence de droit, dans un système de traitement de l'information (article 2 et 3 de la proposition)
   b- La captation illicite de données ou de programmes enregistrés (article 4 de la proposition).

2 La modification des textes relatifs aux incriminations traditionnelles à savoir le faux, le vol, l'escroquerie, l'abus de confiance, la dégradation et la destruction pour les adapter à la protection contre les nouveaux risques informatiques.

La proposition a fait l'objet, dans cette époque, de diverses critiques. Selon le professeur Devèze, cette proposition présentait le défaut de s'attacher principalement à la défense des biens qui sont déjà assurés. Mais surtout, elle comportait des lacunes graves quant à la protection des systèmes. Voir Jean DEVÈZE, «Commentaire de la proposition de loi relative à la fraude informatique présentée par M. J. Godfrain le 5 août 1986 », D.I. 1987.

Mais malgré toutes ces critiques, la proposition Godfrain est venue en première lecture devant l'assemblée nationale. Par ailleurs, le texte été très largement modifié (Rapport ANDRÉ, Doc. AN, 1986-1987, 2e session ordinaire, n° 744). L'assemblée nationale a créé de nouvelles incriminations regroupées dans un chapitre 3 intitulé « De certaines infractions en matière informatique) :

a- L'accès frauduleux à un système de traitement automatisé de données;
b- L'action d'entraver ou de fausser le fonctionnement d'un tel système;
c- L'introduction illicite d'informations dans le système de traitement automatisé de données et la suppression ou modification illicite des informations contenues dans un tel système;
d- L'altération de la vérité de nature à causer un préjudice à autrui par la suppression, la modification ou l'introduction illicite précitée;
e- L'usage intentionnel de documents ainsi altérés.

De son côté, le Sénat «partisan d'une pénalisation assez étroite, avait pensé que, pour faire une bonne loi pénale en la matière, il fallait, avant de définir les infractions elles-mêmes, définir les situations à protéger ». Par conséquent, il a modifié le titre de la proposition de loi qui, désormais, s'appelait proposition « relative à certaines infractions en matière de système de traitements automatisés de données »

De la sorte, le sénat a simplifié les incriminations contenues dans ce chapitre. Désormais, il n'y en a que 2 :

a- L'accès ou le maintien frauduleux dans un «système de traitement automatisé de données ». Ici, on remarque très bien que le sénat par l'ajout du maintien à l'accès, a étendu le champ de l'incrimination.
b- La substitution intentionnelle au « maître du système » en agissant sur l'un des éléments de celui-ci.

par le législateur canadien et le législateur français s'inscrivent autour de deux infractions principales, à savoir l'accès illicite à un système informatique et les atteintes que ce dernier ainsi que les données peuvent subir.

Notons à cet effet que la prise de conscience des risques liés aux crimes informatiques est assez récente en France, mais aussi au Canada. En effet, jusqu'en 1988, la France ne disposait que de deux textes en vue de faire face à ce genre de crimes. Il s'agit de la Loi informatique, fichiers et libertés de 1978[18], et de la Loi sur la protection du droit d'auteur datant de 1985 et qui tend à protéger les logiciels contre certaines formes de piratage[19]. Il a donc fallu attendre la loi Godfrain en 1988[20] pour que la France se dote d'un arsenal répressif allant jusqu'au pénal[21]. Par la suite, une panoplie de lois fut alors adoptée. On peut citer à titre d'exemple la Loi relative à la sécurité intérieure en 2003[22], la Loi pour la confiance dans l'économie

---

Le sénat a, toutefois, apporté une autre innovation. Il a inséré, au sein du texte même, les définitions relatives aux termes techniques clefs apparus dans le texte tel que le «système de traitement automatisé de donnée » (Rapport THYRAUD, Doc. Sénat, 1987-1988, 1re session, n° 3).
Mais, en deuxième lecture, cette idée était rejetée par l'assemblée nationale. Elle a préféré laisser cette tache à la jurisprudence (Rapport ANDRÉ, Doc. AN, 1987-1988, n° 1087). Ce n'est qu'en troisième lecture, que le texte fût adopté pour devenir la *Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique,* J.O. 6 janv. 1988, p.231. En ligne :
<http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19880106&numTexte=&pageDebut=00231&pageFin=>, (consulté le 12 mars 2011). (Ci-après Loi Godfrain de 1988)

[18] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* J.O. 7 janv. 1978, p.227, en ligne :
<http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19780107&numTexte=&pageDebut=00227&pageFin= >, (consulté le 08 juin 2011)

[19] *Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle,* J.O. 04 juil. 1985*,* en ligne :
<http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000693451>, (consulté le 08 juin 2011)

[20] *Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique,* préc., note 17.

[21] Éric FILIOL et Philippe RICHARD, *Cyber criminalité : enquête sur les mafias qui envahissent le web*, DUNOD, 2006, p. 187.

[22] *Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure,* J.O. n° 66 du 19 mars 2003, en ligne :
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199>, (consulté le 08 juin 2011)

numérique en 2004[23] et la Loi relative aux communications électroniques et aux services de communication audiovisuelle datant de la même année[24].

En droit canadien, il n'existait pas non plus de texte pénal visant spécifiquement le crime informatique jusqu'en 1985, date à laquelle on a apporté des modifications au Code criminel en adoptant de nouvelles infractions relatives à l'intégrité des systèmes informatiques. Par ailleurs, on a utilisé jusqu'en 1985 des dispositions générales se trouvant dans le Code criminel et s'appliquant au vol (art. 322 du C.cr.), à la fraude (art. 380 du C.cr) ou à l'extorsion (art. 346 du C.cr.) et ce, afin de tenter de combattre certains crimes liés à l'informatique. Après l'adoption de la loi modifiant le Code criminel[25], plusieurs autres lois ont été adoptées au Canada afin de renforcer le cadre juridique lié aux crimes informatiques. À titre d'exemple, on peut citer la Loi sur la preuve au Canada[26], la loi sur le droit d'auteur[27] et la loi sur l'entraide juridique en matière criminelle[28]. En 1997, le législateur a apporté diverses modifications à son code pénal par le biais de la Loi visant à améliorer la législation pénale, tel l'article 342.2 du C.cr. relatif à la possession de moyens permettant d'utiliser un service d'ordinateur[29].

---

[23] *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,* J.O. n° 143 du 22 Juin 2004, en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=>, (consulté le 08 juin 2011)

[24] *Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle,* J.O. 10 juil. 2004, en ligne : <http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399>, (consulté le 08 juin 2011)

[25] *Loi de 1985 modifiant le droit pénal*, préc., note 16.

[26] *Loi sur la preuve au Canada*, L.R., 1985, ch. C-5, en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-5/derniere/lrc-1985-c-c-5.html>, (consulté le 08 juin 2011)

[27] *Loi sur le droit d'auteur,* LRC 1985, c C-42, en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-42/derniere/lrc-1985-c-c-42.html>, (consulté le 08 juin 2011)

[28] *Loi sur l'entraide juridique en matière criminelle*, L.R. 1985, ch.30(4e Suppl), en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-30-4e-suppl/derniere/lrc-1985-c-30-4e-suppl.html>, (consulté le 08 juin 2011)

[29] *Loi de 1996 visant à améliorer la législation pénale*, L.C. 1997, ch. 18, art. 19.

L'objectif de notre travail est de nous poser la question suivante : quelles sont les principales infractions qui portent atteinte à la sécurité du système informatique dans une entreprise et quelle réponse le droit pénal a-t-il réservé à ces infractions ? Concrètement, on va analyser dans ce travail deux infractions. Dans un premier temps, notre analyse portera sur l'infraction relative à l'accès illicite aux systèmes informatiques et aux données. L'étude de cette infraction est importante pour deux raisons. La première est qu'il s'agit de l'incrimination principale de la loi française de 1988[30] et de la loi canadienne de 1985[31]. La deuxième est qu'il n'existait pas, en droit pénal français avant 1988 et en droit criminel canadien avant 1985, de texte qui pouvait appréhender cette infraction. Dans un second temps, lors de notre étude, nous allons traiter l'infraction qui est incontestablement la plus importante parce qu'elle organise la protection des systèmes informatiques et des données contre plusieurs atteintes dont ils peuvent faire l'objet.

Afin de mieux comprendre la portée de ces infractions, nous avons choisi de les analyser à la lumière de deux systèmes juridiques différents, à savoir un pays de conception civiliste, la France, et un autre d'approche régie par la *Common Law,* le Canada. Certaines précisions doivent être apportées. La *Common Law* est une conception d'origine anglaise, bâtie essentiellement sur la jurisprudence, par opposition au droit civiliste ou codifié dans les pays de tradition romaine. La particularité de la *Common Law* est qu'elle évolue sans arrêt et ne reste donc pas statique. Toutefois, elle respecte la règle du *stare decisis*, qui fait que le juge est lié par les décisions précédentes, ce qui assure une certaine stabilité. Contrairement à cela, le droit pénal de conception civiliste reste statique et n'évolue pas très vite du fait qu'il est codifié. Le juge doit respecter les principes dégagés par le législateur au sein du Code. Le juge peut décider d'un revirement de la jurisprudence.

L'apport de cette comparaison va être important car celle-ci va nous permettre de constater s'il y a des ressemblances, voire même des convergences,

[30] *Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique,* préc., note 17.
[31] *Loi de 1985 modifiant le droit pénal,* préc., note 16.

entre le droit pénal français et le droit criminel canadien. Rappelons que, de façon intéressante, la France et le Canada ont tous deux signé la *Convention sur la cybercriminalité*[32]. Celle-ci constitue le premier traité international qui, aux termes de son préambule, vise à poursuivre « une politique pénale commune, destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ». La convention s'emploie donc à harmoniser les législations nationales en matière de droit pénal. Outre les infractions informatiques (falsification et fraudes informatiques), la pornographie juvénile et les atteintes à la propriété intellectuelle, la *Convention sur la cybercriminalité* réprime l'accès illicite à tout ou partie d'un système informatique, l'interception illégale de données informatiques et l'atteinte à leur intégrité ou à celle du système. Les comportements incriminés doivent toujours être commis de façon intentionnelle et « sans droit » pour que la responsabilité pénale soit engagée.

Dans ce travail, nous allons voir comment ces deux pays, de conceptions juridiques différentes, ont évolué face à cette nouvelle criminalité liée à l'informatique. Nous allons examiner comment les objectifs de chacun des pays étudiés, malgré certaines différences, sont au final très semblables.

Notre travail se présentera alors en deux parties. La première traitera de l'infraction d'accès illicite aux systèmes et aux données informatiques. Dans cette partie, il s'agira de traiter le cas d'une personne qui, tout en étant dépourvue de droit, accède à un système informatique de l'entreprise ou à des données contenues dans celui-ci. L'accès illicite dans ce cas peut être une finalité en soi ou un moyen de réaliser d'autres objectifs (partie 1).

---

[32] La *Convention sur la cybercriminalité*, 23.XI.2001, Budapest, S.T.E n°185, en ligne : <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm>, (consulté le 11 juin 2011). La convention a été adoptée par la France par la *Loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* (J.O. 20 mai 2005) et par le Canada, qui l'a signé le 23 novembre 2001.

À la suite d'un accès, qu'il soit autorisé ou non, les systèmes informatiques peuvent subir des altérations réelles et très profondes qui affectent leur bon fonctionnement ou les données qu'ils peuvent contenir. C'est le cas par exemple d'une personne qui introduit un programme malicieux dans le système informatique de l'entreprise, ce qui peut entraîner la perte de données, voire même une perturbation dans le fonctionnement du système. Les atteintes aux systèmes et aux données informatiques feront l'objet de notre analyse dans une deuxième partie (partie 2).

PREMIÈRE PARTIE : L'accès illicite aux systèmes et aux données informatiques

L'accès illicite aux systèmes et aux données informatiques est une infraction plus complexe qu'elle n'y paraît. En effet, les objets de l'accès peuvent varier. On peut en distinguer trois : les systèmes informatiques et les données, les réseaux informatiques et, enfin, les communications informatiques[33]. Alors que dans les deux premiers cas, l'opération visée par l'infraction sera constituée par un accès, dans le dernier, l'opération visée par l'infraction sera constituée par une interception[34].

Notons que les trois cas d'accès coïncident, mais pas complètement. En effet, dans certains cas, l'accès à un réseau peut entraîner l'interception d'une communication. En revanche, une interception dépend toujours d'un accès à un réseau ou à un système connecté à celui-ci. De même, l'accès aux systèmes et aux données pourra conduire à l'accès à un réseau, par exemple dans le cas où les données seront appréhendées lors d'une communication[35].

En France, le législateur incrimine largement, au sein de l'article 323-1 du Code pénal[36], le fait d'accéder à « un système de traitement automatisé de données » en entendant celui-ci de manière large pour englober les réseaux informatiques et, par conséquent, les interceptions de communications effectuées à

---

[33] Par communications informatiques, on entend les communications entre deux systèmes informatiques appartenant à la même personne, deux ordinateurs communiquant entre eux, un système informatique communiquant avec lui-même, ou enfin les communications entre un ordinateur et une personne.

[34] Pascal VERGUCHT, *La répression des délits informatiques dans une perspective internationale*, thèse en droit, Université de Montpellier, 1996, par. 138.

[35] *Id.*

[36] *Code pénal français,* 108e édition, Paris, Dalloz, 2011, en ligne : <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110503>, (consulté le 03 mai 2011), (ci-après « C.pén. »)

la suite d'un tel accès. Il faut noter à cet effet qu'il n'existe pas au niveau du Code pénal français d'autre disposition traitant des interceptions de communications informatiques. Mais l'article 226-15 al. 2 du C.pén. reste pertinent parce qu'il interdit l'interception de communications privées (chapitre 1).

Au Canada, le législateur a adopté une approche juridique différente de son homologue français. Il a mis en place au sein de l'article 342-1(1) du Code criminel[37] l'infraction d'utilisation non autorisée d'ordinateur, en vertu de laquelle il réprime l'obtention frauduleuse d'un service d'ordinateur et l'interception d'une fonction d'ordinateur (chapitre 2).

[37] *Code criminel*, L.R.C. (1985), c. C-46, mod. par L.R.C. (1985), c.2 (1er supp.), en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-46/derniere/lrc-1985-c-c-46.html>, (consulté le 03 mai 2011), (ci-après « C.cr. »)

Chapitre 1 : L'accès illicite à « un système de traitement automatisé de données » en droit français

Un accès simple à « un système de traitement automatisé de données » peut être le but poursuivi par la personne ; il sera donc répréhensible dès lors qu'il n'est pas autorisé (I). Cependant, il est rare de voir une personne qui accède à un système informatique sans avoir un objectif bien précis. En effet, l'accès illicite à un système informatique et aux données constitue dans la plupart des cas un moyen de réaliser une autre opération interdite telle l'appréhension de données informatiques lors d'une interception des communications (si le système informatique est connecté à un réseau bien sûr) (II).

I) L'accès illicite à « un système de traitement automatisé de données »

En France, l'article 323-1 al.1 du C. pén. interdit « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ». Pour la constitution de cette infraction, on a pu constater l'exigence d'une « condition préalable »[38], à savoir l'existence d'un « système de traitement automatisé de données ». Aussi convient-il d'illustrer en quoi consiste cette notion(A), avant de passer à l'analyse des éléments constitutif de l'infraction relative à l'accès à « un système de traitement automatisé de données » ou au maintien dans celui-ci(B).

[38] Raymond GASSIN, « La protection pénale d'une nouvelle « universalité de fait » en droit français : les systèmes de traitement automatisé de données », (Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique), A.L.D. 1989, par. 51, p.14.

A) La définition de la notion de « système de traitement automatisé de données »

Pour tomber sous le coup des articles 323-1 à 323-3 du C.pén., les agissements prévus par ces textes doivent nécessairement être perpétrés à l'encontre d'un « système de traitement automatisé de données ». Malgré l'importance d'une telle notion pour l'application de la loi Godfrain de 1988[39], cette notion n'est pas définit par le législateur.

Par ailleurs, lors de sa première lecture du texte de loi, le Sénat a insisté sur la nécessité de définir, au sein même de la loi et de façon précise, les termes techniques du nouveau dispositif pénal[40], particulièrement la notion de « maître du système » et celle de « système de traitement automatisé de données ». Concernant cette dernière notion, le Sénat a proposé la définition suivante en procédant par énumération de ses composantes physiques :

> « On doit entendre par systèmes de traitements automatisés de données, tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, d'organes d'entrées-sorties, et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité. »[41]

Ultérieurement, lorsque le texte de loi fut transmis pour une seconde lecture devant l'Assemblée nationale, cette dernière a écarté la définition proposée par le Sénat, laissant à la jurisprudence le soin de définir cette notion[42]. En effet, la controverse entre l'Assemblée nationale et le Sénat, qui a entraîné l'absence d'une définition légale au sein du texte de loi, s'attache à l'exhaustivité de l'énumération des composantes de l'ensemble qui concourt à un résultat déterminé, de même qu'à

---

[39] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[40] Rapport J. THYRAUD, préc., note 17, p. 50.
[41] *Id*., p. 51.
[42] Rapport ANDRÉ, préc., note 17.

la question relative à l'exigence ou non d'un dispositif de sécurité[43]. De surcroît, on a aussi averti le législateur de ne pas contourner cette problématique en adoptant une définition très large, comme il l'a fait précédemment avec d'autres notions[44].

Par ailleurs, même si la définition proposée par le Sénat n'a pas été retenue dans le texte de loi de 1988[45], celle-ci va conserver un intérêt particulier pour guider la jurisprudence (1) et la doctrine (2) dans l'interprétation de cette notion.

1) L'interprétation de la notion de « système traitement automatisé de données » par la jurisprudence

Le 5 janvier 1994, la Cour de cassation a rendu un arrêt très important dans lequel elle a retenu une conception large de la notion de « système de traitement automatisé de données »[46]. En l'espèce, les faits ont débuté en 1988, lors de l'élaboration d'un système ayant pour objectif d'informatiser la gestion d'une entreprise. Une employée avait alors porté des mentions erronées sur des fiches manuscrites de saisie informatique – lesquelles fiches étaient créées afin d'administrer les produits de la société dans un seul fichier. En s'appuyant sur les anciens articles 462-5 et 462-6 du Code pénal, relatifs à la falsification de documents informatisés et à l'usage desdits documents, l'entreprise a porté plainte contre l'employée. Mais en raison de l'absence d'élément moral de l'infraction, l'employée a été acquittée par le Tribunal correctionnel.

Par la suite, la Cour d'appel de Versailles a disqualifié par un arrêt rendu le 17 janvier 1992 les faits poursuivis en délit d'altération volontaire de données dans

---

[43] J.O. A.N., 5 novembre 1987, p. 3654.
[44] Il s'agit particulièrement de la notion de « traitements automatisés d'informations nominatives », que l'on trouve dans la *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, préc.,* note 18, art 5.
[45] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[46] Crim. 5 janv. 1994, JCP E. 1994.I, étude n° 359, p. 252, par. 16, note Vivant et le Stanc.

un système de traitement automatisé de données prévu dans l'article 462-4 du Code pénal[47] ; elle a également condamné l'employée ayant porté préjudice à l'entreprise. Cette employée a ensuite formé un pourvoi en cassation qui s'est fondé sur le fait que les mentions inexactes qu'elle a portées sur les fiches manuscrites de saisie informatique ne peuvent constituer un délit d'introduction de données à l'intérieur d'un système de traitement automatisé de données. Mais la Chambre criminelle a rejeté le pourvoi et a jugé que l'article 462-4 du Code pénal s'applique lorsque des données inexactes ont été introduites dans un système de traitement automatisé en cours d'élaboration.

Bien qu'il ne faille pas lui attribuer une portée générale, cette solution peut être approuvée en l'espèce[48]. En effet, dans ce cas, les mentions inexactes ont été introduites dans le système alors que celui-ci été exploité dans le cadre de tests de validation opérés sur des données réelles. Donc, le système était en fonctionnement[49] même s'il était en cours d'élaboration. Bien entendu, la solution aurait été différente si les tests de validation avaient été opérés sur des données fictives. À ce moment-là, on n'aurait pas pu considérer que le système était en fonctionnement[50].

Selon la Cour de cassation, un système de traitement de données devrait donc s'entendre comme :

> « Tout ensemble composé d'une ou de plusieurs unités de traitement, de mémoire, de logiciels, de données, d'organes d'entrées-sorties et de liaisons qui, sans considération de l'existence d'un système de sécurité qui

[47] Aujourd'hui, c'est l'art 323-3 du C.pén.
[48] Raymond GASSIN, « Au sujet du délit d'atteinte volontaire aux données contenues dans un système de traitement de données (commentaire d'un arrêt de la chambre criminelle du 5 janvier 1994) », Lamy D.I. 1996, par.11, p. 3.
[49] *Id*., par.15, p. 3.
[50] *Id*.

> lui est rattaché, opère sur des données réelles et non fictives, qui concourent à un résultat déterminé. »[51]

À travers cet arrêt, la Cour de cassation a donc retenu un sens large de la notion de « système de traitement automatisé de données » et a considéré que les fiches manuscrites de saisie informatique faisaient partie de ce système.

De son côté, dans un arrêt rendu en avril 1994 se référant à la définition d'un « système de traitement automatisé de données » telle que proposée par le Sénat, la Cour d'appel de Paris a jugé qu'un service télématique (36-15) est un « système de traitement automatisé de données » :

> « Il convient de constater que les poursuites exercées visent en l'espèce des « systèmes de traitement automatisé de données », au sens de la loi du 5 janvier 1988, s'agissant d'atteintes alléguées à des ensembles, unités de traitement, organes entrées-sorties et liaisons concourant en principe, pour chacun des services télématiques concernés, à un résultat déterminé. »[52]

En octobre 1992, la Cour d'appel de Douai a jugé que le disque contenant le logiciel de comptabilité et les données d'un cabinet d'expertise comptable constituait aussi un système[53]. Cette décision, bien qu'elle respecte le choix des parlementaires, est largement critiquée par la doctrine qui soutient qu'un élément isolé, par exemple un logiciel non intégré à un ordinateur, ne saurait constituer un système[54].

---

[51] Jean-François CASILE, *Le Code pénal à l'épreuve de la délinquance informatique*, PU d'Aix-Marseille, 2002, par. 207, p. 85.
[52] Paris, 5 avril 1994 : Juris-Data n° 021093, en ligne : <http://www.lexisnexis.com> (consulté le 11 mai 2011), p.25. (Dans la base de données de Lexis Nexis, il y a un document PDF de toutes les décisions. Le numéro de page que l'on mentionne fait référence à ce document. Cela s'applique pour toutes les décisions répertoriées dans ce travail que l'on a trouvées sur ce site).
[53] Douai, 7 oct. 1992, Gaz. Pal. 1993, p. 236, note Latry-Bonnart.
[54] R. GASSIN, préc., note 48, par. 10, p. 3.

On relève aussi que le Tribunal de grande instance de Paris a jugé que le système électronique de cartes bancaires est un système de traitement automatisé de données au sens de l'article 323-1 du C.pén.:

> « Le système CB est, au sens des dispositions précitées, un système de traitement automatisé de données […] le terminal de paiement, parce qu'il vérifie lors d'une transaction l'authenticité de la carte en effectuant un calcul de données sur celle-ci, doit être considéré comme partie intégrante du système automatisé de données; que le fait que les travaux sont menés sur un terminal inerte sera sans conséquence sur la prévention, démonstration étant faite par le prévenu lui-même que le secret de la valeur d'authentification de la carte à puce sera percé via les informations contenues dans le terminal. »[55]

Il nous semble que le jugement du Tribunal correctionnel de Paris peut être défendu. Si l'on retient la définition d'un « système de traitement automatisé de données » telle que proposée par le Sénat, le terminal de paiement peut constituer en soi un système. Il est constitué d'éléments tels que le clavier, un écran, une unité centrale, des logiciels (précisément l'algorithme d'authentification des cartes bancaires introduites dans le terminal), etc., l'ensemble étant destiné à réaliser une transaction au moyen d'une carte bancaire[56].

Même si la définition sénatoriale de l'expression « système de traitement automatisé de données » n'a pas été retenue dans la loi de 1988 relative à la fraude informatique[57], on remarque à travers la jurisprudence citée ci-haut qu'elle a éclairé les juges pour cerner le sens de cette notion. Il en va tout autrement pour la doctrine qui, semble-t-il, n'a pas été convaincue par la définition sénatoriale. Dès lors, l'élaboration d'une autre définition relative au « système de traitement automatisé de données » est devenue une nécessité pour la doctrine.

---

[55] TGI Paris, 25 fév. 2000, D. 2000, n° 18, p. 220.
[56] Xavier DELPECH, « Fraude à la carte bancaire : aspects juridiques », D. 2000, p.222.
[57] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.

2) La conceptualisation de la notion de « système traitement automatisé des données » par la doctrine

Parmi les auteurs qui se sont particulièrement attachés à l'analyse juridique du « système de traitement automatisé de données » et qui ont le mieux approfondi cette question figure M. Gassin[58]. Néanmoins, son approche a fait l'objet de certaines critiques.

Pour mieux comprendre la notion de système de traitement automatisé de données, l'auteur propose de définir les trois termes « clefs » de cette expression, à savoir : les « données », le « traitement automatisé », et enfin le « système de traitement automatisé de données ».

a) Les données

La « donnée» est définie, selon l'arrêté relatif à l'enrichissement du vocabulaire de l'informatique, comme étant « la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement »[59]. Elle se caractérise par son caractère formel, et doit donc être distinguée de l'information. La seconde constituant « la substance intellectuelle » de la première[60]. Ce qui est visé par la loi de 1988[61], ce sont donc les données et non les informations.

---

[58] R. GASSIN, préc., note 38, p. 14.
[59] *Arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique*, J.O. 17 jan. 1982, p. 624, liste 1, p. 625. En ligne : <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19820117&numTexte=&pageDebut=50624&pageFin= > (site consulté le 12 mars 2011).
[60] R. GASSIN, préc., note 38, par. 59, p.15.
[61] *Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique,* préc., note 17.

Tel qu'employé dans le texte, le terme « donnée » englobe les « données brutes », non structurées, et il désigne les éléments d'informations qui sont traités par le système ainsi que les programmes qui servent à les traiter[62].

b) Le traitement automatisé

Pour tenter de trouver une définition à l'expression « traitement automatisé », l'auteur a essayé de savoir, en premier lieu, s'il existe une différence entre le « traitement automatisé » et le « traitement automatique », et en deuxième lieu, si les « traitements mixtes »[63] entrent dans la notion de « traitement automatisé ».

1- « Traitement automatisé » versus « traitement automatique »

Le « traitement automatique » est défini comme « l'ensemble des opérations réalisées par des moyens automatiques, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation »[64]. Si l'on s'appuie sur la loi relative à l'informatique, aux fichiers et aux libertés, qui définit « le traitement automatisé d'informations nominatives » comme « tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives… »[65], il apparaît que les notions de « traitement automatique » et de « traitement automatisé » sont synonymes[66]. En revanche, lorsqu'on se réfère à la Convention

---

[62] R. GASSIN, préc., note 38, par. 60, p.15.
[63] Traitements dont une partie consiste en un traitement informatique alors que l'autre partie consiste en un traitement manuel (appelé mécanographique).
[64] *Arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique,* préc., note 59.
[65] *Loi n°78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés,* préc., note 18, art. 5.
[66] R. GASSIN, préc., note 38, par. 62, p.15.

108 du Conseil de l'Europe, qui définit le « traitement automatisé » comme étant « des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion »[67], l'expression « traitement automatisé » semble avoir un sens plus large que celui de la notion de « traitement automatique »[68].

2- « Traitement automatisé » et « traitement mixte »

On relève ici deux conceptions. La première, restrictive, est défendue par le professeur Croze ; elle assimile le « traitement automatisé » au « traitement informatique »[69]. En vertu de cette approche, l' « ordinateur » reste au centre du champ d'application de la loi de 1988[70]. Bien que nous soyons d'accord avec cette dernière affirmation, nous pensons que cette approche est trop restrictive car elle exclut du champ d'application de la loi les fichiers manuels et les fichiers mécanographiques. Cela se remarque particulièrement lorsqu'on se réfère à la directive 95/46/CE du 24 octobre 1995, qui définit le traitement comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés »[71]. D'où l'idée de se pencher plutôt vers la deuxième conception, qui est plus large. Défendue par le professeur Gassin, cette approche permet de faire entrer dans le cadre du « traitement automatisé » les « traitements mixtes » « du

---

[67] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,* 28 janvier 1981, art 2)c). En ligne :
< http://www.conventions.coe.int/Treaty/FR/Treaties/Html/108.htm>, (consulté le 03 mars 2011.)
[68] R. GASSIN, préc., note 38, par. 63, p.16.
[69] Hervé CROZE, « L'apport du droit pénal à la théorie générale de l'informatique (à propos de la loi no 88-19 du 5 janvier 1988 relative à la fraude informatique) », JCP, 1988.I, étude n° 3333, par. 7.
[70] La *loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[71] *Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995, art 2)b), J.O. n° L 281 du 23.11.1995, p. 31–50 (ci- après Directive 95/46/CE)

moment qu'ils forment un système et que les éléments non automatiques auxquels il est porté illégalement atteinte font partie dudit système »[72].

c) Le « système de traitement automatisé de données »

D'un point de vue juridique, le professeur Gassin présente le « système de traitement automatisé de données » comme une « universalité de fait ». Pourquoi « universalité de fait » ? Il s'agit d'une universalité parce que les droits et les biens qui composent le système font partie d'un ensemble ayant un système juridique propre[73]. Il s'agit d'une universalité de fait parce que cet ensemble n'a pas de passif propre[74].

De la définition proposée par le professeur Gassin, il ressort essentiellement que les articles 323-1 à 323-3 du C.pén. ne s'appliquent que pour un seul système et ses éléments. Sont donc exclus du champ d'application de la loi de 1988[75] les agissements qui affectent un réseau assurant la communication entre systèmes distincts[76]. Nous pensons qu'une telle position n'est pas envisageable, surtout à une époque où tout se passe à travers les réseaux. À titre d'exemple, le mois de janvier 2011, des pirates auraient infiltré les réseaux internes des ministères canadiens, et ce afin d'obtenir les mots de passe confidentiels de certains administrateurs qui leur permettraient d'accéder aux systèmes informatiques, et ainsi d'obtenir des informations confidentielles[77]. En outre, nous pouvons nous référer au commentaire du sénateur Thyraud concernant la définition proposée relative au « système de traitement de données ». Ce dernier a en effet affirmé qu' « elle [la définition]

---

[72] R. GASSIN, préc., note 38, par. 69, p.17.
[73] *Id*., par.75, p. 18.
[74] *Id*.
[75] La *loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[76] R. GASSIN, préc., note 38, par.80, p. 19.
[77] « Les réseaux informatiques d'Ottawa attaqués. » En ligne : <http://www.radio-canada.ca/nouvelles/National/2011/02/16/002-cyber-attaque-informatique-federal.shtml>, (Consulté le 4 mars 2011)

couvre la situation la plus simple, l'ordinateur isolé, et la plus complexe, le réseau aux multiples ramifications qui fait le tour de la Terre… »[78].

Par conséquent, « dans l'esprit des législateurs, l'infraction devait donc clairement couvrir l'ordinateur comme le réseau mondial, l'ensemble du matériel et de l'immatériel, sans aucune différence entre les ordinateurs personnels ou les célèbres super-ordinateurs de calcul de la société Cray Research »[79]. Le fait d' « admettre l'idée selon laquelle la loi du 5.01.88 écarterait de son champ d'incrimination les réseaux reviendrait à lui « rogner les ailes » et à lui « ôter toute portée véritable »[80].

Nous pensons enfin que pour éviter toute ambiguïté liée à la notion de « système de traitement automatisé des données », il serait souhaitable qu'une intervention législative vienne en préciser le contenu.

À la lumière de la jurisprudence et de la doctrine, nous avons ainsi analysé la notion de « système de traitement automatisé des données » (ci-après « système »), perçue comme une condition nécessaire à l'application de la loi Godfrain de 1988[81]. Nous allons passer à l'étude de l'infraction prévue à l'article 321-1 al.1 du C.pén. en vertu duquel on incrimine toute « situation indue »[82] dans un « système ». Concrètement, on va analyser l'infraction qui réprime celui qui accède ou se maintient de façon frauduleuse dans un « système ».

---

[78] Rapport J. THYRAUD, préc., note 17, n° 3, p.52 et 53.
[79] P. VERGUCHT, préc., note 34, par. 140.
[80] Guillaume CHAMPY, *La fraude informatique*, t. 1, PU d'Aix-en-Provence, 1992, p.144.
[81] La *loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[82] Jean DEVÈZE, « Chronique Droit pénal des affaires », JCP E. 1988.II, étude n°15122. p. 125.

B) Les éléments constitutifs de l'infraction relative à l'accès ou au maintien frauduleux dans un « système »

Nous analyserons dans un premier temps l'élément matériel de l'infraction (1) pour ensuite tenter de relever l'élément moral (2).

1) L'élément matériel

À la lumière de l'article 323-1 al.1 du C.pén., nous constatons que le législateur incrimine non seulement celui qui accède mais aussi celui qui se maintient dans « tout ou partie » d'un « système » et ce, indépendamment du résultat auquel ces actions peuvent conduire.

a) L'accès

Le législateur lui-même ne définit pas l'accès. Le dictionnaire Larousse définit l'accès comme étant « la possibilité pour quelqu'un de pénétrer dans [quelque chose] »[83]. Justement, la Cour d'appel de Paris ne dit pas autre chose :

> « L'accès frauduleux, au sens de l'article 462-2 du Code pénal issu de la loi du 5 janvier 1988 et au sens de l'article 323-1 du Code pénal, vise tous les modes de pénétration irréguliers d'un système, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de télécommunication. »[84]

Par ailleurs, pour tomber sous le coup de la loi, la pénétration de la personne dans le « système » n'est pas suffisante. Ladite personne doit aussi être dépourvue

[83] Larousse.fr, en ligne <http://www.larousse.com> (Site visité le 2 mars 2011.)
[84] Paris, 5 avril 1994, préc., note 52, p. 27.

de droit pour le faire, comme l'a rappelé la Cour d'appel de Toulouse : « L'accès à un système informatisé de données tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'y accéder. »[85] Dans le même sens, la Cour d'appel de Douai, a considéré que l'accès à un système informatique d'une entreprise est sans droit lorsqu'il n'est pas autorisé[86].

C'est donc le simple fait de pénétrer, sans droit, dans un « système » qui est visé par l'article 323-1 al.1 du C.pén. Les modes ou les moyens utilisés pour le faire[87] importent donc peu. L'accédant peut profiter des faiblesses du système de sécurité pour y pénétrer[88]. Il peut également s'introduire par l'insertion d'un programme appelé « cheval de Troie » lui permettant de maîtriser totalement le système informatique de l'entreprise[89]. L'accès peut aussi résulter de la composition d'un code d'accès obtenu de façon frauduleuse. Selon le Tribunal de Grande Instance de Paris, l'accès tombe sous le coup de la loi pénale dans le cas d'une personne qui a utilisé le numéro et le code confidentiel d'une carte appartenant à une tierce personne pour s'introduire dans le réseau téléphonique de « France Télécom » et bénéficier de la sorte d'appels gratuits à l'étranger[90].

---

[85] Toulouse, 21 janv. 1999 : Juris-Data n° 040054, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.6.
[86] Douai, 7 oct. 1992, préc., note 53, p. 236.
[87] Michel VIVANT *et al*., *Droit de l'informatique et des réseaux*, Lamy, 2007, par. 3243, p.1903; J.-F. CASILE, préc., note 51, p. 95; Nidal El CHAER, *La Criminalité informatique devant la justice pénale*, Beyrouth, Liban, Éditions Sader, 2004, p. 113; Jean DEVÈZE, « Atteintes aux systèmes de traitement automatisé de données », *J.-Cl. Pén*., fasc. unique, par. 29, en ligne : <http://www.lexisnexis.com>, (consulté le 8 mars 2011.)
[88] Paris, 13 oct. 2010 : Juris-Data n°021727, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.4.
[89] Trib. corr. Limoges, 14 mars 1994, Expertises 1994, p. 238, obs. Teboul.
[90] TGI, Paris, 26 juin 1995, LPA, 1 Mars 1996, n°27, p.4, note Alvarez.

Le mobile poursuivi par l'accédant n'est pas non plus pris en considération pour l'application de l'article 323-1 al.1 du C.pén.[91] Comme l'a relevé la Cour d'appel de Rouen :

> « Que le mobile ayant animé les quartes prévenus, à savoir la récupération des données dont la société BONNA SABLA était restée propriétaire, ne les autorisait pas davantage à accéder, à l'insu des dirigeants habilités, au système informatique de la société SNM 3000. »[92]

Il en est de même pour les conséquences possibles de l'accès. Le Tribunal de grande instance de Vannes a ainsi jugé que l'article 321-1 du C.pén. s'applique « dès lors qu'une personne non habilitée pénètre dans le système. Il importe peu au tribunal que les données des comptes utilisateurs n'aient pas été modifiées. »[93]

En revanche, l'accès aux parties des sites Internet pouvant être atteintes par la simple utilisation d'un logiciel grand public de navigation ne peut être incriminé, selon la Cour d'appel de Paris[94]. Il en est de même pour la simple copie de fichiers par une personne habilitée par ses fonctions à accéder aux données sensibles du système informatique de l'entreprise[95].

L'article 323-1 al.1 du C.pén. réprime non seulement l'accès à un système, mais également le fait de s'y maintenir. Ainsi, le maintien, tout comme l'accès, caractérise-t-il l'élément matériel de l'infraction prévue dans cet article.

---

[91] Christian LE STANC et Pascale TRÉFIGNY, « Droit du numérique », D. 19 juil. 2007, n° 28, p. 1998.
[92] Rouen, 17 mars 2005 : Juris-Data n°291578, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.12.
[93] TGI, Vannes, 13 juillet 2005 : Juris-Data n° 294765, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.9.
[94] Paris, 30 octobre 2002, Expertises 2003, n° 266, p. 36.
[95] Grenoble, 4 mai 2000 : Juris-Data n°122622, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.3.

b) Le maintien

Il convient tout d'abord de préciser que le délit de maintien a été ajouté à celui d'accès par le Sénat au cours d'une discussion parlementaire. Le rapporteur Thyraud, faisant référence à l'article 462-2 du C.pén[96]., énonce :

> « Votre commission vous propose d'en modifier légèrement la rédaction afin d'étendre l'infraction au cas du fraudeur habilité à accéder à une partie du système qui, ayant eu frauduleusement accès à une partie non autorisée de ce système, s'y maintient en connaissance de cause, et au cas du fraudeur qui ayant eu par hasard accès à un système fermé, s'y maintient volontairement tout en sachant qu'il n'y a pas droit. »[97]

Ainsi, cette volonté d'élargir le champ d'application de l'article 323-1 du C.pén se traduit-elle par le fait que le maintien irrégulier est incriminé dans deux situations, détaillées ci-après.

La première est celle où la personne ayant une autorisation d'accès à une partie du système en profite pour accéder à une autre partie du système et s'y maintenir sans autorisation, La Cour de cassation a justement expliqué que :

> « À supposer que l'accès soit régulier, le maintien sans droit et en pleine connaissance de cause dans un système de traitement automatisé des données suffit à caractériser l'infraction dès lors que le « maître du système » a manifesté l'intention d'en restreindre le maintien aux seules personnes autorisées. »[98]

La deuxième situation s'applique à toute personne qui est entrée dans le système par erreur, ou par hasard – pour reprendre le mot utilisé par le sénateur

[96] Aujourd'hui, c'est l'article 323-1 du C.pén.
[97] Rapport J. THYRAUD, préc., note 17, p. 58.
[98] Crim. 3 oct. 2007, *Bull.crim*., n° 236, p. 995.

Thyraud – et qui s'y maintient en sachant pertinemment qu'elle n'a pas le droit de le faire. À cet effet, la Cour d'appel a rappelé dans un arrêt rendu en 1994 que « la loi incrimine également le maintien irrégulier dans un système de la part de celui qui y serait entré par inadvertance, ou par celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement »[99].

Par ailleurs, d'autres cas de maintien irrégulier peuvent être relevés. Il s'agit notamment de celui qui s'est prolongé au-delà du temps autorisé[100]. C'est le cas par exemple d'employés de l'ANPE qui ont utilisé des minitels, mis à leur disposition par leur employeur dans un but exclusivement professionnel, et ont abusivement prolongé leur maintien dans ces appareils pendant des heures, voire des nuits entières, à l'insu de leur entourage grâce aux systèmes d'inhibition et des écrans noirs. Cela avait pour but de multiplier le nombre de points leur donnant droit à des cadeaux et de l'argent sans que le prix des communications soit à leur charge. Après avoir rappelé que le maintien se définit comme étant « l'action de faire durer », la Cour d'appel de Paris a reconnu ces employés de l'ANPE coupables du délit de maintien frauduleux au motif qu'ils ont fait durer la connexion au-delà du temps permis[101].

Le délit de maintien frauduleux dans un système est aussi constitué dès lors que le prévenu, qui a accédé régulièrement à des serveurs minitels accessibles au public, s'y est maintenu de façon délibérée au moyen de l'envoi par ordinateur de messages incitant les utilisateurs de ces services à utiliser des services concurrents[102].

---

[99] Paris, 5 avril 1994, préc., note 52, p.27.
[100] R. GASSIN, préc., note 38, par. 112, p. 25.
[101] Paris, 15 décembre 1999 : Juris-Data n°106710 en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.19.
[102] Paris, 14 janvier 1997 : Juris-Data n°020128, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.16.

Notons aussi que pour tomber sous le coup de l'article 323-1 al.1 du C.pén., il importe peu de considérer les conséquences d'un maintien irrégulier. Que ce maintien soit « actif »[103] – comme dans le cas des prévenus qui se sont maintenus dans l'annuaire électronique de France Telecom et ont procédé à des manœuvres illégales pour bénéficier de téléchargements gratuits [104] –, ou qu'il soit « inoffensif » [105] – qu'il résulte d'une simple promenade dans le système et n'entraîne aucun dommage à celui-ci[106] –, il est dans les deux cas incriminable.

Notons enfin que le maintien peut être de plusieurs formes. Il y a le maintien dit « on line». L'intrus dans ce cas après avoir accéder frauduleusement au système, reste « sciemment branché au lieu de se déconnecter.»[107] Bien que le maintien dit « online » soit la catégorie de maintien la plus répandue, il existe une autre forme de maintien dit « offline ». Ce dernier se produit suite à la présence de l'intrus dans le système après la fin de la connexion, et il se matérialise selon plusieurs scénarios. Par exemple, l'installation dans le système d'une « boite aux lettres » permet à l'intrus de revenir dans ce système contre la volonté du « maître du système »[108].

c) L'accès ou le maintien dans « tout ou partie » du système

À la lecture de l'article 323-1 al.1 du C.pén., on constate que le législateur incrimine autant l'accès que le maintien dans « tout ou partie » d'un « système ». Cela implique que le prévenu n'a pas à accéder ou à se maintenir dans tout le système pour caractériser le délit prévu à l'article 323-1 al.1 du C.pén. L'accès ou le maintien dans certaines parties du système – comme l'accès à un simple logiciel ou

---

[103] R. GASSIN, préc., note 38, par.113, p. 25.
[104] Trib. Corr. Brest, 14 mars 1995, LPA. 28 juin1995, n°77, p. 4, note Choisy.
[105] R. GASSIN, préc., note 38, par.113, p. 25.
[106] Paris, 15 mai 2001 : Juris-Data n°148055, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.4.
[107] Jean Paul BUFFELAN, « La répression de la fraude informatique », Expertises, 1988, n° 103, p. 100
[108] G. CHAMPY, préc., note 80, p. 228.

l'accès aux données – suffisent donc pour commettre le délit[109]. D'ailleurs, la Cour d'appel de Douai a jugé que la copie du disque d'un système d'expert comptable faite sans autorisation caractérise le délit d'accès frauduleux à un système automatisé car ce n'est pas seulement au logiciel ou à des données isolées qu'a pu accéder le copiste mais à des données traitées par le système[110].

Ainsi, lorsqu'une personne pénètre dans une partie du système, elle est punie de la même façon que si elle pénètre dans tout le système[111]. Toutefois, la personne doit agir sans droit et de manière frauduleuse. Cela nous amène à étudier l'élément moral de l'infraction d'accès et de maintien.

2) L'élément moral

L'article 323-1 al.1 du C.pén. incrimine « le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie » d'un « système ». Ainsi, l'élément moral de l'infraction réside-t-il dans le caractère « frauduleux » de l'accès et du maintien. L'auteur de l'acte doit agir volontairement. Concrètement, il doit en toute connaissance de cause pénétrer et/ou se maintenir dans un système sans en avoir le droit. C'est justement ce qui a été affirmé par la Cour d'appel de Paris :

> « Pour être punissable, l'accès ou le maintien doit être fait sans droit et en pleine connaissance de cause […] pour que l'infraction existe, il suffit que le « maître du système ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées. »[112]

[109] J. DEVÈZE, préc., note 87, par. 28, p. 9.
[110] Douai, 7 oct. 1992, préc., note 53, p. 326.
[111] J-F CASILE, préc., note 51, par. 195, p.81.
[112] Paris, 5 avril 1994, préc., note 52, p. 27.

Ainsi, l'accès à un « système » ou le maintien conscient dans celui-ci, sans autorisation, caractérise un dol général[113] concrétisé par la conscience d'avoir violé la volonté du « maître du système »[114]. De ce fait, un accès autorisé ne pourra être qualifié de frauduleux qu'à la condition que l'autorisation donnée ait été dépassée[115]. En effet, le défaut d'annulation du code d'accès d'un employé licencié ne constitue pas une autorisation implicite de la part du « maître du système » d'accéder au système de l'entreprise, a affirmé la Cour d'appel de Toulouse. L'absence de droit, dans ce cas, qualifie l'entrée dans le « système » de frauduleuse[116].

Par ailleurs, l'accès à un système ouvert au public ou le maintien dans celui-ci ne pourra pas être qualifié de frauduleux dans la mesure où le « maître du système » a manifesté son intention de ne pas restreindre l'accès audit système. La Cour d'appel de Rennes a, justement, jugé que la connexion par minitel à l'annuaire électronique de France Télécom ne peut être qualifiée de frauduleuse dès lors que l'accès à cet annuaire dans le but d'en recopier les données n'est contraire ni à la loi pénale ni à la volonté de France Télécom – laquelle entreprise met à la disposition des consultants une liste destinée à l'information du public en temps réel et n'a pas manifesté l'intention d'en restreindre l'accès pas plus que la durée de consultation[117].

Notons aussi qu'un accès par erreur à un système ne peut tomber sous le coup de la loi pénale. Encore faut-il que l'auteur de l'acte sorte du « système » aussitôt qu'il a eu conscience de l'irrégularité de son acte. Dans le cas contraire,

---

[113] J.-F. CASILE, préc., note 51, par. 260, p.103.
[114] Le Sénat a proposé la définition suivante du « maître du système », mais l'Assemblée nationale n'a pas voulu la reprendre : « toute personne physique ou morale, toute autorité publique, tout service ou tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation ou de ses finalités », Rapport J. THYRAUD, préc., note 17, p.53.
[115] Crim., 10 déc. 1998, N° de pourvoi : 97-85867, en ligne:
http://www.lexinter.net/JPTXT2/intrusion_dans_un_systeme_automatise_de_traitement.htm
(Site consulté le 11 mars 2011.)
[116] Toulouse, 21 janv. 1999, préc., note 85, p. 6.
[117] Rennes, 6 févr. 1996 : Juris-Data n°042141, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011), p5-6.

l'élément moral de l'infraction est relevé suite à l'absence de « sortie » du système et au maintien dans celui-ci[118].

Notons également que la mise en place d'un dispositif de sécurité peut constituer un moyen de faire connaître à certaines personnes qu'elles n'ont pas le droit de pénétrer dans le système ou de s'y maintenir[119]. Par conséquent, lorsque la personne pénètre dans un « système » protégé, cela permet de prouver son intention frauduleuse[120].

Ainsi, les éléments constitutifs de l'infraction prévue à l'article 323-1 al.1 du C.pén. sont établis lorsqu'une personne accède à, ou se maintient dans, tout ou partie du « système » et ce, sans autorisation et avec la conscience de l'irrégularité de son acte. Par ailleurs, l'accusé peut échapper à sa responsabilité pénale en démontrant son état d'esprit innocent. Il peut démontrer sa bonne foi, l'erreur ou l'accident[121].

Enfin, en aucun cas le mobile de l'infraction ne peut être invoqué pour tenter d'échapper à la responsabilité pénale, comme l'a clairement dit le Tribunal de grande instance de Vannes en jugeant que :

> « [...] ne saurait en particulier être considéré comme exonératoire de responsabilité pénale la considération suivant laquelle l'intrusion sur des comptes utilisateurs protégés par des mots de passe cryptés a eu lieu dans un contexte prétendument pédagogique alors que cette intrusion, au mépris de la charte de bon usage des ressources informatiques, permettait d'accéder à des comptes utilisateurs sécurisés détenus par d'autres

[118] M. VIVANT *et al*., préc., note 87, par. 3244, p. 1905.
[119] R. GASSIN, préc., note 38, par. 128, p. 29.
[120] G. CHAMPY, préc., note 80, p. 250; M. VIVANT *et al*., préc., note 87, par. 3244, p. 1905; Virginie PRAT et Yann BRÉBAN, « Note sous la Cour d'appel de Paris, douzième Chambre, section A, Ministère public, Tati », Gaz. Pal. 2003, n° 205, p.23.
[121] J. DEVÈZE, préc., note 87, par. 40.

> étudiants ou membres du personnel comportant à la fois un espace universitaire et un espace personnel. »[122]

À travers l'article 323-1 al.1 du C.pén., le législateur français réprime donc celui qui accède à tout ou partie d'un « système » ou s'y maintient frauduleusement. Comme on a pu le constater, du fait de la notion de « système de traitement automatisé de données », l'infraction d'accès est assez large pour englober les réseaux informatiques et, par conséquent, les interceptions de communications informatiques qui peuvent être effectuées à la suite d'un tel accès et qui peuvent avoir comme conséquence la perte de données informatiques. Bien qu'il n'y ait pas d'autre disposition dans le Code pénal qui accorde une protection aux communications informatiques, le législateur traite au sein de l'article 226-15 al.2 du C.pén. de l'interception des communications privées. Cette infraction va faire l'objet de notre analyse dans ce qui suit.

II) L'interception des communications privées

L'article 226-15 al.2 du C.pén. interdit « le fait commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ». Avant de passer à l'analyse des éléments constitutifs de cette infraction, il convient de préciser en quoi consiste son objet.

A) La définition de l'objet de l'infraction

L'alinéa 2 de l'article 226-15 du C.pén. vise à protéger les correspondances qui sont transmises d'un point à un autre par la voie des télécommunications. La correspondance est définie comme étant un « échange de lettres ou d'autres

[122] TGI, Vannes, 13 juillet 2005, préc., note 93, p.9.

messages assimilés (télex, télégrammes) »[123]. On retrouve ainsi l'idée d'une relation entre deux ou plusieurs personnes qui communiquent entre elles à travers divers moyens tels que le téléphone, le fax, le courrier électronique, les lettres, etc. Le Tribunal de grande instance de Quimper définit le terme correspondance comme étant « toute relation par écrit établie entre deux personnes identifiables, qu'il s'agisse de lettres, messages ou plis fermés ou ouverts, un courrier électronique, dès lors qu'il est adressé par une personne nommément désignée à une personne elle aussi nommément désignée »[124]. La correspondance doit par ailleurs être transmise par voie de télécommunication. On entend par télécommunication « les émissions, transmissions ou réceptions, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique »[125]. Sont donc visées les communications téléphoniques, celles transmises à travers le réseau internet telles que les messages électroniques…[126] En outre, malgré que le Code pénal ne l'ait pas expressément exigé, la correspondance doit avoir un caractère privé[127]. À cet effet, il y a correspondance privée lorsque le message est « exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée »[128] ; citons par exemple le courrier électronique, qui permet l'envoi d'un message d'une adresse E-mail vers une autre adresse E-mail[129]. En revanche, le caractère privé de la correspondance tomberait lorsque le message est posté au sein d'une liste de diffusion[130].

L'objet de l'infraction d'interception de communications privées étant défini, on va analyser dans ce qui suit ses éléments constitutifs.

---

[123] Gérard CORNU, *Vocabulaire juridique*, Association Henry Capitant, PUF, p. 236 et p. 810.
[124] TGI. Quimper, 17 juillet 2008, en ligne :
< http://www.legalis.net/jurisprudence-decision.php3?id_article=2387> (consulté le 30 août 2009)
[125] Code des postes et des communications électroniques, En ligne:
<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987&dateTexte=20080505> (consulté le 04 mai 2011), art. L-32.
[126] TGI. Paris, 2 nov. 2000, Expertises. 2001, p.191, note X. Furst.
[127] Clotilde MORLOT-DEHAN, « Les évolutions du secret de la correspondance », R.D.P. 2005.II, p.369.
[128] Définition donnée par la circulaire du 17 janvier 1988 prise en application de la *Loi n° 86-1067 du 30 septembre 1986*, J.O. du 09 mars 1988.
[129] Florence BITAN, « Courrier électronique», *J.-Cl. Comm*., fasc. 4740, par. 62, en ligne : <http://www.lexisnexis.com>, (consulté le 08 mars 2011)
[130] Philippe BELLOIR, « L'application des règles de procédure pénale aux infractions commises sur le réseau internet », Legalis.net. 2002. II, p. 21.

B) Les éléments constitutifs de l'infraction d'interception de communications privées

L'examen des éléments constitutifs de l'infraction d'interception des communications privées s'attachera d'abord à la définition de l'élément matériel (1) puis à la définition de l'élément moral (2).

1) L'élément matériel

En vertu de l'article 226-15 al.2 du C.pén., plusieurs comportements caractérisent l'élément matériel de l'infraction d'atteinte aux correspondances. On note l'interception, le détournement, la divulgation ou l'utilisation de la correspondance. Par ailleurs, le domaine de notre étude consacré aux interceptions de communications nous conduit à ne considérer que le premier comportement, à savoir l'interception. En effet, d'un côté, le détournement de la correspondance est une atteinte à l'acheminement de la correspondance; d'un autre côté, la divulgation et l'utilisation sont des comportements qui se rattachent plutôt au contenu de la correspondance, constituant ainsi une atteinte à la confidentialité de cette dernière.

La notion d'interception n'a pas été définie par le législateur français. Si l'on se réfère au dictionnaire Larousse[131], le verbe intercepter désigne le fait d' « arrêter quelque chose au passage, [d'] en interrompre le cours direct ». Donc, pour constituer une interception aux termes de l'article 226-15 al.2 du C.pén., l'agent doit capter la correspondance pendant son acheminement de l'expéditeur vers le destinataire[132], ou lorsqu'elle est parvenue à destination sans avoir déjà été consultée par le destinataire. Une fois reçue et lue par le destinataire, elle ne constitue plus que des données informatiques. Par conséquent, elle n'est plus

[131] *Larousse.fr, Encyclopédie et dictionnaires Larousse*, en ligne : <http://www.larousse.fr/> (consulté le 30 août 2009)
[132] Crim.14 avr. 1999, JCP G 1999, II, étude n° 10312.

protégée par l'article 226-15 al.2 du C.pén. Cependant, elle peut être indirectement protégée à travers l'article 323-1 du C.pén., qui réprime l'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données[133].

Notons aussi que l'interception de correspondances suppose « une préméditation », la mise en place d'un stratagème et d'un branchement en vue de capter[134] celles-ci. C'est d'ailleurs ce qui a été confirmé par la Cour de cassation dans un arrêt rendu en 1999 :

> «Ne sauraient constituer une interception de correspondance émise par la voie des télécommunications, au sens de l'article 100 du Code de procédure pénale, les simples lectures et transcriptions par les policiers, sans artifice ni stratagème, des messages parvenus sur la bande d'un récepteur de messagerie unilatérale. »[135]

Enfin, il est à noter que pour être puni, il importe peu que celui qui a intercepté le message ait eu connaissance de son contenu même si, en pratique, le contenu du message est toujours l'objectif de l'interception[136]. Toutefois, une intention coupable est exigée pour retenir la responsabilité de l'auteur de l'interception. Cela nous conduit à examiner l'élément moral de l'infraction.

2) L'élément moral

En vertu de l'article 121-3 al.3 du C.pén., l'élément moral de l'infraction d'atteinte aux correspondances est constitué d'un dol général. Une intention coupable de l'agent qui a commis l'interception est par conséquent requise. Afin de

---

[133] Virginie PELTIER, «Atteintes au secret des correspondances commises par des particuliers», 2008, *J.-Cl. Pén*., art. 226-15, par. 51, en ligne : <http://www.lexisnexis.com>, (consulté le 08 mars 2011)
[134] Jean PRADEL, « La lecture d'un « Tatoo » n'est pas une écoute téléphonique », D.1999, p. 324.
[135] Crim. 14 avr. 1999, préc., note 132, étude n°10312.
[136] V. PELTIER, préc., note 133, par.57.

retenir la culpabilité de l'auteur de l'interception, il faut prouver que celui-ci avait la volonté d'intercepter la correspondance. Cette volonté est manifestée par son comportement : l'auteur, bien qu'ayant conscience que la correspondance ne lui est pas destinée, l'intercepte à l'insu de son destinataire[137]. En effet, il revient toujours aux juges de fond d'établir la preuve, en s'appuyant sur des faits, de l'intention coupable de l'auteur de l'acte interdit. Ainsi, l'intention coupable de l'employeur est caractérisée, selon la Cour d'appel de Pau, dès lors que celui-ci s'est introduit, sans autorisation, dans la messagerie personnelle de son ex-employé en employant diverses manœuvres pour intercepter ses messages. L'employeur avait nécessairement conscience de s'approprier les documents qu'il savait appartenir à son ex-employé à son insu et contre son gré[138]. Il faut aussi souligner que la Cour d'appel, en rendant sa décision, a expressément rappelé que le mobile étant indifférent, il importait peu que l'employeur ait voulu, en opérant de la sorte, se constituer une preuve dans le cadre d'un litige qui l'opposait à son employé[139].

En revanche, sont exclues du champ d'application de la loi pénale les personnes qui interceptent une correspondance d'autrui en vertu d'une autorisation spéciale de la loi ou du juge[140].

Enfin, il serait important de s'interroger sur l'éventualité d'un dol spécial pour caractériser l'élément intentionnel de l'infraction d'atteinte aux correspondances transmises par voie électronique, à côté de l'existence du dol général. En effet, la présence d'un dol spécial est inutile dans la plupart des cas, mais elle est nécessaire dans certains cas, particulièrement celui de l'administrateur de réseau[141]. En effet, les fonctions de ce dernier portent nécessairement atteinte au secret des correspondances. Étant donné que dans ce cas, le dol général ne soulève

---

[137] TGI. Paris, 2 nov. 2000, préc., note 126, p.191.
[138] Pau, 24 nov. 2005, LPA. 11 oct. 2006 n° 203, p. 16, note LASSERRE-CAPDEVILLE
[139] *Id.*
[140] Alain BLANCHOT et Isabelle POTTIER, « La violation des correspondances transmises par e-mail par une personne chargée d'une mission de service public », Gaz. Pal., 23 janv. 2001 n° 23, p. 18.
[141] V. PELTIER, préc., note 133, par.72.

pas de difficulté puisque l'administrateur réseau est conscient qu'il est en train de porter atteinte à un droit qu'il n'a pas, la seule justification possible pour qu'un administrateur réseau échappe à une responsabilité pénale est de démontrer l'absence d'un dol spécial, à savoir la mauvaise foi.

Ainsi, pour conclure ce chapitre concernant l'accès à un « système de traitement automatisé de données », on peut dire que le législateur français à travers l'article 323-1 al.1 du C.pén., souhaite sanctionner celui qui s'introduit ou se maintient, sans droit, dans tout ou une partie du « système » en ayant conscience de l'irrégularité de son acte. La même disposition peut être pertinente en cas d'atteinte aux communications dans la mesure où le « système de traitement automatisé de données » est défini d'une manière suffisamment large pour englober les réseaux informatiques et, par conséquent, les interceptions de communications informatiques effectuées lors de cet accès. Toutefois, par le biais de l'article 266-15 al. 2 du C.pén., le législateur assure une protection pénale aux correspondances privées réalisées par voie de télécommunications. Bien que le législateur canadien, par le biais de l'article 184(1) du C.cr., assure la même protection aux correspondances privées, il a de surcroît prévu une protection des communications informatiques au sein de l'article 342-1(1) du C.cr. relatif à l'utilisation non autorisée d'ordinateur. Justement, dans le chapitre qui suivra, on va traiter cette dernière infraction. À cet effet, on va pouvoir dégager, à la lumière de ce qu'on a étudié dans le chapitre 1, les ressemblances et les convergences entre les infractions prévues en droit pénal français et celles prévues en droit criminel canadien.

Chapitre 2 : L'utilisation non autorisée d'ordinateur en droit canadien

> « *Since computer time and services have economic value, it is logical that their misappropriation should be sanctioned as equally as are the misappropriation of other things of value of which a person can be de-prived.* »[142]

I) Introduction

En vertu de l'article 342-1 du C.cr., le législateur canadien réprime toute utilisation non autorisée d'ordinateur. Concrètement, il s'agit d'interdire toute obtention illicite de services d'ordinateur ainsi que toute interception des fonctions d'ordinateur, y compris les fonctions de communications.

On peut ainsi constater que l'infraction prévue par le législateur canadien au sein de l'article 342-1 du C.cr. est a priori plus large que celle prévue par le législateur français. En effet, en vertu de l'article 323-1 du C.pén., le législateur français réprime de façon expresse l'accès illicite à un « système de traitement automatisé de données ». Par ailleurs, les interceptions de communications informatiques ne peuvent être protégées que de manière indirecte par le biais de l'article 323-1 du C.pén. Cela est contraire à ce qu'a prévu le législateur canadien, qui réprime de façon expresse par le biais de l'article 342-1 du C.cr. aussi bien celui

[142] Donald. K. PIRAGOFF, « Computer Crimes and Other Crimes against Information Technology in Canada », (1993) 64 *International Review of Penal Law,* 20, 223, p. 227.

qui obtient de façon frauduleuse les services d'ordinateurs que celui qui intercepte les fonctions d'ordinateur, y compris les fonctions de communications.

Il faut rappeler à cet effet que jusqu'en 1985, il n'existait pas en droit criminel canadien de disposition qui sanctionne de façon expresse l'utilisation non autorisée d'un ordinateur. À cette époque, l'infraction de vol de service de télécommunication prévue par l'article 287(1) b) du C.cr.[143] semblait pouvoir s'appliquer en cas d'utilisation non autorisée d'un ordinateur. Toutefois, depuis 1980, la Cour suprême du Canada a écarté cette solution dans l'arrêt *R.* c. *McLaughlin*[144]. Par ailleurs, la décision de la Cour suprême du Canada dans cette affaire est, sans contredit, celle qui a poussé le législateur canadien à entreprendre une réforme législative en matière de crimes liés à l'informatique[145]. Il apparaît donc indispensable de faire un survol de cette affaire (A) avant de passer à la définition de l'objet de l'infraction relative à l'utilisation non autorisée d'ordinateur (B).

A) Analyse de l'affaire *R.* c. *McLaughlin*

En l'espèce, selon les faits, un étudiant a réussi à s'introduire dans le système informatique de l'Université de l'Alberta et a obtenu, sans autorisation, des programmes et des renseignements appartenant à d'autres personnes. Il fut accusé d'avoir commis un vol, conformément au sous-paragraphe 287(1) b) du C.cr. en vertu duquel « commet un vol quiconque, frauduleusement, malicieusement ou sans

---

[143] Aujourd'hui, c'est l'article 326(1) b) du C.cr.
[144] [1980] 2 R.C.S. 331.
[145] George S. TAKACH, *Computer Law*, 2e éd., Irwin Law, 2003, p. 238; Pierre ROBERT, « La criminalisation des abus informatiques en droit pénal canadien », dans Droit contemporain, *Rapports canadiens au Congrès international de droit comparé*, Montréal, Éditions Yvon Blais, 1990, p. 684; Anne-Marie BOISVERT, «Communicatique et responsabilité pénale : criminalité informatique et « vol » d'information », dans BEAUCHARD, Jean et al., *Le droit de la communicatique*, Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal, Thémis, 1990, p. 103; M. Stephen GEORGAS,« Bill C-18 and Computer Abuse», 5 Advocates' Soc. J. No. 2, p.14-19, en ligne : <http://www.lexisnexis.com>, (consulté le 08 juin 2011).

apparence de droit […] se sert d'installations ou obtient un service en matière de télécommunication ». Aux termes du paragraphe 287(2) du C.cr.[146], le terme « télécommunication » désigne « toute transmission, émission ou réception de signes, signaux, écrits, images, sons ou renseignements de toute nature, par radio, par un procédé visuel, électronique ou électromagnétique ».

La question en litige devant la Cour était de savoir si l'appropriation de programmes et de renseignements contenus dans un ordinateur implique l'utilisation d'une « installation de télécommunication ». En d'autres termes, il s'agit de déterminer si un ordinateur constitue une « installation de télécommunication » ?

En se fondant sur les composantes physiques d'un système informatique, à savoir l'unité centrale de traitement, la mémoire, les imprimantes et les terminaux, le juge du procès a déclaré que le système informatique constitue bien une « installation de télécommunication » et que, par conséquent, cela rendait les dispositions de l'article 287(1) b) du C.cr. applicables à l'accusé[147].

En appel, la Cour d'appel de l'Alberta a renversé à la majorité le jugement rendu en première instance [148]. S'appuyant sur la définition du terme « télécommunication » prévue par le législateur à l'article 287(2) du C.cr., le juge Morrow a déclaré qu'un ordinateur avec toutes ses composantes et ayant le calcul pour fonction principale ne peut constituer une installation de « télécommunication » au sens de l'article 287(1) b) du C.cr. [149]

---

[146] Aujourd'hui art. 326(2) du C.cr.
[147] *R.* v. *Christensen et al*. (1978), 26 *Ch. L.J.* 348, p. 350.
[148] *R.* v. *McLaughlin* (1979), 51 C.C.C. (2d) 243 (Alta. C.A).
[149] *Id.*, p. 249.

Ultérieurement, le pourvoi présenté par la Couronne devant la Cour suprême a été rejeté. La décision de la Cour d'appel de l'Alberta fut ainsi confirmée[150]. Sous la plume du juge en chef Laskin, la Cour suprême du Canada a précisé qu'un ordinateur n'est pas une « installation de télécommunication ». En effet, la Cour suprême du Canada a clairement établi la distinction entre un ordinateur et une « installation de communication » en s'appuyant sur la fonction que chaque installation peut exécuter. Au sens de la définition du terme « télécommunication » prévue à l'article 287(2) du C.cr., une « installation de télécommunication » a pour fonction la transmission et la réception de renseignements canalisés vers des destinataires extérieurs[151]. Par contre, l'ordinateur « sert plutôt à effectuer des calculs complexes, à traiter et à mettre en corrélation des renseignements et à les mettre en mémoire pour pouvoir les récupérer »[152]. Selon la Cour suprême du Canada, ce qui est en cause dans cette affaire est « une installation de traitement des données » :

> « C'est une installation de traitement de données qui est en cause ici plutôt qu'une installation de télécommunication, même si elle renferme de l'équipement électronique. Si l'on considère l'installation comme un tout (c'est-à-dire l'unité centrale de traitement et les terminaux), il n'y a eu aucune transmission ou réception à l'extérieur. Bien qu'il y ait eu transmission de renseignements d'une partie de l'installation à une autre, il n'y a pas eu de réception par d'autres installations ni émission à partir de l'installation en cause. »[153]

Il nous semble que par son interprétation stricte de la définition d' « installation de télécommunication », la Cour suprême du Canada a fermé la porte à l'utilisation de l'infraction de vol d'un service de télécommunication prévue à l'article 287(1) b) du C.cr. pour faire face à certains abus liés à l'informatique à

---

[150] *R.* c. *McLaughlin*, préc., note 144, p.331.
[151] *Id*., p. 336.
[152] *Id*.
[153] *Id*.

cette époque, notamment l'utilisation non autorisée d'ordinateur. Mais comme l'a justement précisé le juge Estey :

> « II ne fait aucun doute que si le législateur avait eu l'intention d'attacher des conséquences pénales à l'utilisation non autorisée d'un ordinateur, il l'aurait édicté dans un article du Code criminel ou dans une autre loi pénale où le terme, maintenant consacré dans notre langue, est employé. Le législateur ne s'attend pas à ce que la Cour déduise de mots généralement associés à l'industrie des communications qu'il a voulu attacher des conséquences pénales à l'utilisation non autorisée d'un ordinateur »[154].

Effectivement, peu de temps après l'affaire *McLaughlin*, le Parlement fédéral adoptait en 1985 une loi pour modifier le Code criminel[155]. L'article 342-1 fut ainsi ajouté au Code en vertu de l'article 46 de cette loi[156]. Désormais, commet une infraction d'utilisation non autorisée d'ordinateur :

> « Quiconque, frauduleusement et sans apparence de droit : a) directement ou indirectement, obtient des services d'un ordinateur, b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'ordinateur »[157].

Avant de passer à l'analyse des éléments constitutifs de l'infraction relative à l'utilisation non autorisée d'un ordinateur, il convient d'abord de définir la notion

---

[154] *Id*., p. 341-342.
[155] *Loi de 1985 modifiant le droit pénal*, préc., note 16.
[156] *Id*., art. 46, p. 272. En vertu de l'article 46 de cette loi, l'article 301.2 du C.cr. (aujourd'hui, c'est l'article 342.1) est inséré dans le Code criminel après l'article 301.1 du même code.
[157] Art. 342-1(1) a) et b) du C.cr.

d'ordinateur qui est au cœur de la réforme législative de 1985 en matière de crimes liés à l'informatique [158].

B) La définition de la notion d' «ordinateur »

Contrairement au législateur français, qui ne définit pas la notion de « système » au sein du Code pénal, le législateur canadien prévoit une définition de l' « ordinateur » au sein de l'article 342-1(2) du C.cr., qui se lit comme suit :

> « Un dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux : *a*) contiennent des programmes d'ordinateur ou d'autres données; *b*) conformément à des programmes d'ordinateur : (i) soit exécutent des fonctions logiques et de commande, (ii) soit peuvent exécuter toute autre fonction. »[159]

En vertu de cette définition, un ordinateur se compose donc d'un ou de plusieurs dispositifs. On peut noter essentiellement cinq éléments. Il y a d'abord le périphérique d'entrée, qui convertit les données conçues pour l'utilisateur en un code assimilable par la machine. Ensuite, vient l'unité centrale qui a pour rôle de contrôler et de coordonner les fonctions de l'ordinateur moyennant un programme appelé logiciel. Ce dernier est le cœur de la machine cybernétique. Son rôle est de régir le traitement des données. Puis, il y a les unités logiques, de mémoire et de contrôle qui permettent à l'ordinateur d'effectuer des calculs, de prendre des décisions et de mémoriser les données. Enfin, vient le périphérique de sortie qui

[158] *Loi de 1985 modifiant le droit pénal*, préc., note 16.
[159] Art. 342-1(2) du C.cr.

convertit les résultats conçus par l'ordinateur en un langage compréhensible pour l'utilisateur[160].

En se fondant sur la définition de l'ordinateur prévue dans l'article 342-1(2) du C.cr., on constate que pour constituer un ordinateur, la présence d'un ou de plusieurs éléments n'est pas suffisante. Il est nécessaire que l'un ou plusieurs de ces éléments exécutent une fonction. Par ailleurs, une « fonction » :

> « S'entend notamment des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé des données de même que des fonctions de communication ou de télécommunication de données à destination, à partir d'un ordinateur ou à l'intérieur de celui-ci. »[161]

L'emploi du terme *notamment* implique que cette liste n'est pas exhaustive. Le législateur ne donne que des exemples de fonctions qui, lorsqu'elles sont exécutées par un dispositif, permettent de qualifier ce dernier d'ordinateur. Il nous paraît donc que le législateur adopte une définition très large, trop même, de la notion d'ordinateur. En effet, avec le développement de la technologie, plusieurs objets qu'on utilise quotidiennement, telle une calculatrice de poche, sont capables d'exécuter les fonctions décrites dans l'article 342-1(2) du C.cr. Leur utilisation non autorisée peut ainsi rendre applicables les dispositions du Code criminel, notamment l'article 342-1(1)[162].

Contrairement au « système », défini par le Sénat et la jurisprudence en France comme étant un objet comportant certaines caractéristiques ou composantes

---

[160] Monique HÉBERT et Marilyn PILON, *Les délits informatiques*, Bibliothèque du parlement, service des recherches, 1991, p.4.
[161] Art. 342-1(2) du C.cr.
[162] D. K. PIRAGOFF, préc., note 142, p. 226; A.-M. BOISVERT, préc., note 145, p. 102.

physiques, on constate que l'ordinateur est défini par le législateur canadien par rapport aux fonctions qu'il peut exécuter[163].

II) Les éléments constitutifs de l'infraction d'utilisation non autorisée d'un ordinateur

À travers l'infraction d'utilisation non autorisée d'ordinateur, le législateur canadien entend réprimer l'accès non autorisé aux ordinateurs ainsi que l'interception de communications. Une interdiction quant à l'obtention frauduleuse des services d'ordinateur est alors prévue à l'alinéa 1 de l'article 342-1(1) du C.cr., alors que l'interception de toute fonction d'un ordinateur est prévue dans l'alinéa 2 de l'article 342-1(1) du C.cr. Pour cela, nous étudierons d'abord l'élément matériel de chaque infraction (l'*actus reus*) (A), pour ensuite essayer de définir l'élément moral, qui se révèle être le même pour les deux infractions (la *mens rea*) (B).

A) L'*actus reus*

Dans un premier temps, on va définir l'élément matériel de l'infraction d'obtention des services d'ordinateur (1), pour ensuite passer à l'examen de l'élément matériel de l'infraction d'interception des fonctions d'un ordinateur (2).

1) L'infraction d'obtention des services d'ordinateur

En vertu de l'article 342.1(1) a) du C.cr., le législateur entend réprimer quiconque qui obtient, directement ou indirectement, des services d'ordinateur. L'élément matériel de cette infraction comporte donc trois aspects : l'accusé doit obtenir, de façon directe ou indirecte, les services d'un ordinateur.

---

[163] A.-M. BOISVERT, préc., note 145, p. 102.

a) Obtenir

L'article 342-1(1) a) du C.cr. requiert que l'accusé doit obtenir les services d'un ordinateur. L'arrêt *R.* v. *Forsythe*[164] constitue l'une des quelques causes rapportées à ce jour au Canada relativement à une poursuite intentée sous l'alinéa 342-1(1) du C.cr. Dans cet arrêt, la Cour provinciale de l'Alberta a défini le terme « obtenir » de la façon suivante : « To obtain something is to gain or attain possession of it. It is an active verb as opposed to the passive action of only having or possessing. »[165] Il s'ensuit que pour obtenir quelque chose, une personne doit commettre des actes « actifs » dans le but de parvenir à la possession de cette chose. De plus, le fait de posséder quelque chose ne veut pas dire que nous l'avons « activement » obtenue. Par conséquent, le fait de trouver des fiches d'ordinateurs sur le bureau de l'accusé ne constitue pas, selon la Cour provinciale de l'Alberta, une preuve suffisante démontrant que l'accusé les a « activement » obtenues[166].

À travers l'article 342-1(1) a) du C.cr., l'objectif du législateur est donc de réprimer toute personne qui obtient « activement » les services d'un ordinateur, de façon frauduleuse bien évidemment.

b) Directement ou indirectement

Aux fins de l'article 342-1(1) a) du C.cr., l'obtention d'un service d'ordinateur doit être faite directement ou indirectement. Dans l'affaire *Forsythe*[167], des documents informatisés contenant des dossiers criminels qui appartenaient aux autorités policières d'Edmonton ont été trouvés sur le bureau de l'accusé. Ce dernier est poursuivi pour avoir obtenu, directement ou indirectement et de manière frauduleuse, les services d'ordinateur – violant ainsi l'article 342(1) a) du C.cr. La

[164] (1992), 137 A.R. 321(Alta. Prov. Ct.)
[165] *Id*., p. 322, par. 4.
[166] *Id.*, p. 322, par. 7.
[167] *R*. v. *Forsythe*, préc., note 164.

Cour provinciale de l'Alberta a acquitté l'accusé au motif que la preuve était insuffisante pour démontrer qu'il a agi de façon indirecte pour obtenir ces documents et ce, même s'il était au courant de la façon dont les fiches ont été obtenues et qu'il avait payé pour les obtenir[168].

Nous ne partageons pas la décision de la Cour qui reflète, selon nous, une lecture restreinte de l'article 342-1(1) a) du C.cr. En effet, lorsqu'on se réfère au dictionnaire, on voit que l'adverbe « indirectement » veut dire « d'une manière indirecte, détournée »[169]. Nous pensons que le sens commun de cet adverbe est assez large, comme l'a d'ailleurs soutenu la Couronne dans cette affaire[170], pour couvrir les agissements de l'accusé. Ce dernier a, d'une façon indirecte, détournée, obtenu les services d'ordinateur des autorités policières d'Edmonton et ce, notamment lorsqu'il a payé un ancien agent de police pour demander à un autre agent d'accéder au système et de faire sortir des documents.

Nous pensons enfin que l'interprétation restreinte de l'article 342-1(1) a) du C.cr. illustre la prudence avec laquelle les tribunaux appliquent les nouvelles dispositions relatives à la fraude informatique[171].

c) Un service d'ordinateur

Un service d'ordinateur « s'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données. »[172] La lecture de cette définition nous rappelle la définition d'une « fonction » d'ordinateur qu'on a vue ci-haut[173]. Il nous paraît ainsi que l'obtention frauduleuse prévue dans

---

[168] *Id*., p. 322, par. 8.
[169] Larousse.fr, en ligne <http://www.larousse.com> (consulté le 23 janvier 2011).
[170] *R*. v. *Forsythe*, préc., note 164, p. 322, par. 9.
[171] Robert W.K. DAVIS, Scott C. HUTCHISON, *Computer Crime in Canada*, Carswell, 1997, p. 166.
[172] Art. 342(2) du C.cr.
[173] Supra, p. 47.

l'article 342-1(1) a) du C.cr. vise les fonctions effectuées par un ordinateur, telles que les fonctions de mémorisation et de recouvrement ou de relevé des données, plutôt que les données qui y sont emmagasinées[174].

L'infraction d'obtention frauduleuse d'un service d'ordinateur peut ainsi s'appliquer dans la plupart des cas de « vol de service », comme c'est le cas de l'affaire *McLaughlin*[175]. Nous pensons à cet effet que l'accusé dans cette affaire aurait été condamné pour violation de l'article 342-1(1) a) du C.cr. si cet article avait été en place au moment des faits.

Il est à noter enfin que l'infraction prévue à l'article 342-1(1) a) du C.cr peut aussi être commise à la suite de l'interception d'une fonction d'un ordinateur[176]. Dans ce cas, il faut rester vigilant quant à la notion d'interception. En effet, ce n'est pas dans tous les cas qu'une interception entraîne l'obtention frauduleuse d'un service d'ordinateur[177].

2) L'infraction d'interception des fonctions d'un ordinateur

Le fait d'accéder à un ordinateur et d'intercepter ses communications constitue une atteinte à la protection des renseignements personnels, même si les données n'ont subi aucune atteinte. Cette conduite peut être assimilée à une interception de communication privée. En effet, le législateur canadien comme son homologue français interdit ce genre d'interception. L'article 184(1) du C.cr. dispose que : « Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication

---

[174] P. ROBERT, préc., note 145, p. 690 ; J. Fraser MANN, *Computer Technology and the Law in Canada,* Carswell, Toronto, 1987, p. 174 ; A.-M. BOISVERT, préc., note 145, p. 103.
[175] *R.* c. *McLaughlin,* préc., note 144.
[176] P. ROBERT, préc., note 145, p. 690.
[177] *Id.*

privée ». Cette disposition, comme on peut le remarquer, ne s'applique qu'en cas d'interception de communications privées, c'est-à-dire des communications qui s'établissent entre deux personnes. De la sorte, sont exclues du champ d'application de l'article 184(1) du C.cr. les communications informatiques, c'est-à-dire les communications entre deux systèmes informatiques appartenant à la même personne, entre deux ordinateurs plutôt qu'entre ordinateurs et les personnes qui les contrôlent, entre un système informatique et lui-même, ou enfin les communications entre un ordinateur et une personne[178].

Justement, c'est pour cette raison que le législateur canadien est intervenu en 1985 [179] pour protéger adéquatement les ordinateurs ainsi que leurs communications contre toutes les interceptions non autorisées. Il a ainsi adopté l'article 342-1(1) b) du C.cr. en vertu duquel il est interdit d'intercepter des communications informatiques. Notons qu'en droit pénal français, il n'existe pas de disposition similaire à l'article 342-1(1) du C.cr. pour protéger les communications informatiques. Ces dernières ne peuvent être protégées, sur le plan pénal, que de façon indirecte par le biais de l'infraction relative à l'accès frauduleux à un système de traitement automatisé de données, laquelle est prévue à l'article 323-1 du C.pén.

En effet, l'article 342-1(1) du C.cr. se lit comme suit : « Quiconque, frauduleusement et sans apparence de droit : b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur (…) ». À la lecture de cet article, il apparaît que l'infraction ne vise que les interceptions de communications effectuées au sein d'un réseau entre des systèmes informatiques[180]. Mais, eu égard aux définitions prévues par le législateur de l'interception, de la fonction et des dispositifs employés pour réaliser une telle interception au sein de l'article 342-1(2) du C.cr., cette disposition est en fait plus large qu'elle n'y paraît.

---

[178] G. S. TAKACH, préc., note 145, p. 239; D. K. PIRAGOFF, préc., note 142, p.218.
[179] *Loi de 1985 modifiant le droit pénal*, préc., note 16, art. 46.
[180] P. VERGUCHT, préc., note 34, par. 146.

En vertu de ces définitions, le comportement incriminé consiste en le fait d'écouter, d'enregistrer ou de prendre connaissance de la substance, de son sens ou de l'objet « des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé de données de même que des fonctions de communication ou de télécommunication de données à destination, à partir ou à l'intérieur d'un ordinateur ». L'interception doit être réalisée au moyen de tout dispositif ou appareil utilisé ou pouvant être utilisé pour « intercepter une fonction d'ordinateur, à l'exclusion d'un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale ».

L'article 342-1(1) b) du C.cr. s'applique donc en cas d'interception de communications à l'intérieur d'un ordinateur ou entre des ordinateurs, de même qu'en cas d'interception de communications destinées à un ordinateur ou encore envoyées à partir d'un ordinateur. Monsieur Sookman écrit :

> « Subsection (b) is intended to protect the privacy of a computer system from invasion by means of a device or apparatus that intercepts its functions. Because of the way in which the term "function" is defined, the subsection makes it an offence to intercept a communication or telecommunication to, from, or within a computer system. The use of an apparatus or device to capture data originating in or from a terminal connected directly to the computer system, or from a remote location, will be caught by the subsection. It will also be an offence fraudulently and without colour of right to monitor the internal operations of a computer system (i.e., the logic, control, and arithmetic functions). »[181]

L'article 342-1(1) b) du C.cr. peut aussi s'appliquer pour protéger indirectement l'acquisition non autorisée de données contenues dans un système

[181] Barry B. SOOKMAN, Sookman : Computer, Internet and electronic commerce Law, Carswell, Toronto, 1989, p. 7-21, 7-22.

informatique. En effet, en interdisant l'interception d'une fonction d'ordinateur, l'acquisition non autorisée des données contenues dans la fonction serait par conséquent interdite :

> « It is, of course, true that this new provision would prohibit indirectly the unauthorized acquisition of data from a computer system. If the interception of a function is prohibited, this will prohibit necessarily the unauthorized acquisition of the data that may be contained in that function. »[182]

Notons enfin que l'interception des communications informatiques peut être directe suite à un accès à un ordinateur par l'utilisation de l'un de ses terminaux, ou indirecte à travers l'utilisation de moyens d'écoute clandestine[183].

B) La *mens rea*

L'infraction d'obtention d'un service d'ordinateur et d'interception de fonction d'ordinateur exige la preuve que la personne a agi « frauduleusement » et « sans apparence de droit »[184]. Cela revient à démontrer, à cause de l'emploi du mot « frauduleusement », que l'accusé a eu un comportement malhonnête[185]. Dans *R.* c. *Zaltic*[186] et sous la plume du juge McLachlin, la Cour suprême du Canada a affirmé qu' « il n'est pas facile de définir avec précision la malhonnêteté. Elle implique cependant un dessein caché ayant pour effet de priver ou de risquer de priver d'autres personnes de ce qui leur appartient »[187]. La notion de malhonnêteté

---

[182] D. K. PIRAGOFF, préc., note 142, p. 220.
[183] *Id.,* p. 219.
[184] Art. 342-1(1) a) et b) du C.cr.
[185] P. ROBERT, préc., note 145, p. 690 ; A.-M. BOISVERT, préc., note 145, p. 104 ; R. W.K. DAVIS, S. C. HUTCHISON, préc., note 171, p. 163 ; D.K. PIRAGOFF, préc., note 142, p. 221; Vincent GAUTRAIS, « Code criminel et utilisation d'internet », par.4. En ligne :
< http : //www.gautrais.com/Code-criminel-et-utilisation-d> (consulté le 29 janvier 2011).
[186] [1993] 2 R.C.S. 29.
[187] *Id.*, p. 45.

sous-entend donc un facteur de turpitude morale qui donne au crime son caractère spécial distinct de toute autre conduite répréhensible mais non criminalisée[188].

En fait, dans le cadre de l'infraction d'obtention frauduleuse d'un service d'ordinateur dans l'affaire *R.* c. *Paré*[189], la Cour du Québec a relevé le comportement malhonnête de l'accusé qui a, de façon intentionnelle, obtenu un service d'ordinateur en sachant qu'il n'y avait pas droit. En l'espèce, la question en litige devant la Cour était de savoir si l'accusé a agi frauduleusement en obtenant sans apparence de droit les services d'ordinateur du Centre de Renseignements Policiers du Québec (C.R.P.Q.).

Selon le juge, l'accusé savait pertinemment qu'il n'avait pas le droit d'utiliser les services d'ordinateurs du C.R.P.Q. à des fins personnelles. Malgré cela, il s'est approprié des données qui y étaient contenues et les a détournées de l'usage auxquelles elles étaient destinées. Son comportement reflète « les éléments de la turpitude morale »[190], voire même « des éléments d'aveuglement volontaire et/ou d'insouciance »[191]. Selon le juge, l'accusé a eu « une intention frauduleuse de l'obtention des services d'ordinateur »[192]. L'accusé a été reconnu coupable d'avoir frauduleusement et sans apparence de droit, directement ou indirectement, obtenu des services d'ordinateur, violant ainsi l'article 342-1(1) a) du C.cr.[193]

Selon l'interprétation du tribunal, l'intention frauduleuse réside donc dans la connaissance de l'accusé du fait qu'il a obtenu des services d'ordinateurs alors qu'il n'avait pas l'autorisation requise pour le faire. Il en va de même en droit pénal français où l'adverbe « frauduleux », qui caractérise l'élément moral de l'infraction

---

[188] V. GAUTRAIS, préc., note 185.
[189] 1997 CarswellQue 651 (C.Q.) (WeC).
[190] *Id.*, par. 22.
[191] *Id*.
[192] *Id*.
[193] *Id*., par. 26.

d'accès et du maintien dans un « système »[194], suppose que l'auteur doit agir sans droit et avoir connaissance de l'irrégularité de son acte[195].

À l'exemple de l'infraction d'obtention frauduleuse d'un service d'ordinateur, l'interception doit être faite de façon frauduleuse. L'auteur de l'acte doit donc intercepter la communication en sachant qu'il n'avait pas le droit de le faire.

Il faut souligner, aussi, que bien que l'absence d'apparence de droit d'obtenir des services d'ordinateur ou d'interception de communications ne soit pas suffisante pour démontrer une intention frauduleuse[196], elle permet à l'accusé de se prévaloir d'un moyen de défense[197]. En effet, celui-ci peut invoquer sa croyance honnête, mais à tort, de penser avoir le droit d'obtenir des services d'ordinateur ou d'intercepter des communications. Selon la Cour d'appel de l'Ontario,

> « The term 'colour of right' generally, although not exclusively, refers to a situation where there is an assertion of proprietary or possessory right to the thing which is the subject matter of the alleged theft. One who is honestly asserting what he believes to be an honest claim cannot be said to act 'without colour of right' even though it may be unfounded in law or fact ... The term 'colour of right' is also used to denote an honest belief in a state of facts which, if it actually existed would in law justify or excuse the act done ... The term when used in the latter sense is merely a particular application of the doctrine of mistake of fact. »[198]

---

[194] Art. 323-1 du C.pén.
[195] Supra, p. 31.
[196] *R.* c. *Lecompte*, REJB 2004-657770 (C.Q.), par. 16.
[197] Sophie BOURQUE, « Les moyens de défense », dans Collection de droit 2009-10, École du Barreau du Québec, Vol. 12, *Droit pénal Infractions, moyens de défense et peine*, Cowansville, Éditions Yvon Blais, 2009, p. 181 à 214, p. 193.
[198] *R.* v. *DeMarco* (1973), 13 C.C.C. (2d) 369(Ont. C.A.), p. 373.

Notons qu'en droit français, l'accusé qui se croit autorisé à accéder par erreur à un « système » peut aussi être exonéré de sa responsabilité[199].

Enfin, comme en droit français, la mise en place d'un système de sécurité peut constituer un moyen de faire savoir à certaines personnes qu'elles n'ont pas le droit d'utiliser les services d'un ordinateur. La croyance honnête de penser avoir le droit d'obtenir des services d'ordinateur ou d'intercepter une communication peut ainsi facilement être affectée lorsqu'une personne pénètre dans un ordinateur protégé[200].

Ainsi pour conclure ce chapitre concernant l'utilisation non autorisée d'un ordinateur, on constate que le législateur canadien, par le biais l'article de l'article 342-1(1) (a) du C.cr., souhaite sanctionner l'introduction illicite dans un ordinateur. Afin de défier le caractère évolutif de la criminalité liée à l'informatique et d'empêcher à cet effet que cette disposition ne soit très vite dépassée, le législateur a octroyé aux expressions « ordinateur » et « service d'ordinateur » une définition large. Par conséquent, l'infraction 342-1(1) (a) du C.cr. ayant une portée très large, elle risque d'incriminer des comportements qui ne sont pas nécessairement criminels, mais qui peuvent être considérés comme tels du seul fait de la présence d'un élément lié à l'informatique. Toutefois, pour compenser cette méprise, le législateur exige la présence d'un état d'esprit caractérisé par la malhonnêteté, une notion qui reste très difficile à définir, notamment dans le cadre de crimes liés à l'informatique. Nous pensons à cet effet que le rôle des tribunaux sera crucial dans l'interprétation de la notion de malhonnêteté, laquelle notion devra selon nous s'interpréter de telle sorte que seuls les comportements criminels soient réprimés. Nous pensons aussi que le législateur peut intervenir et exclure du champ d'application de l'article 342-1(1) a) du C.cr. certains comportements pour éviter,

[199] Supra, p. 33.
[200] D. K. PIRAGOFF, préc., note 142, p. 221.

comme le fait remarquer un auteur[201], des résultats « absurdes » de l'adoption de telles définitions larges.

Pour compléter le cadre juridique lié à l'utilisation non autorisée d'ordinateurs, le législateur canadien a prévu un deuxième alinéa au sein de l'article 342-1(1), dans lequel il interdit les interceptions des fonctions d'ordinateur. À cause de la définition du terme « fonction », sont notamment visées par cette protection les communications informatiques. Désormais, commet une infraction au sens de l'article 342-1(1) b) celui qui intercepte une communication entre deux ordinateurs, une communication entre une personne et un ordinateur, ou enfin une communication à l'intérieur d'un système informatique.

À travers l'article 342-1(1) du C.cr., on constate que le législateur canadien offre un cadre juridique adéquat qui permet de protéger les ordinateurs, et leurs communications contre des actes malveillants.

[201] Chris WEBBER, « Recent Amendments to the Canadian Criminal Code Respecting Computer Abuses Offences », (1987) 3 *Santa Clara Computer & High Technology L.J.* 165, p. 171.

Conclusion de la partie 1

S'introduire simplement dans un système informatique ou s'introduire a fin de réaliser d'autres objectifs tels que l'interception des communications sont deux comportements réprimés aussi bien en droit pénal français qu'en doit criminel canadien. Toutefois, certaines différences demeurent.

En France, le législateur français vise à protéger un « système de traitement automatisé de données ». Cette dernière notion est définie de manière large de telle sorte qu'elle englobe le système informatique ainsi que les réseaux. Bien que l'infraction prévue au sein de l'article 323-1 du C.pén. soit pertinente pour sanctionner l'intrusion et/ou le maintien illicite dans le système informatique, on peut se fonder sur cet article pour sanctionner aussi l'interception de communications informatiques. Cela est d'autant plus pertinent que l'infraction prévue au sein de l'article 226-15 al.2 du C.pén. ne permet de sanctionner que l'interception des communications privées. Au Canada, l'infraction prévue à l'article 342-1(1) a) du C.cr. vise plutôt à protéger les fonctions de l'ordinateur. Désormais, toute personne qui s'introduit sans droit dans un ordinateur et utilise ses fonctions engage sa responsabilité pénale. Par contre, l'alinéa 342-1(1) b) du C.cr. est pertinent pour réprimer les interceptions de communications informatiques.

L'élément moral de l'infraction d'accès et/ou de maintien dans un « système » en droit pénal français réside dans le caractère « frauduleux » de l'accès et du maintien. Il semble que l'auteur doive agir sans droit et en ayant conscience de l'irrégularité de son acte. Le même état d'esprit est exigé par le législateur canadien pour constituer l'infraction relative à l'utilisation non autorisée d'un ordinateur.

La criminalisation de l'accès illicite aux systèmes informatiques a notamment pour avantage d'engager la responsabilité pénale de l'auteur de l'acte à un stade antérieur à celui d'induction de dommages. En effet, à la suite d'un accès, qu'il soit autorisé ou non, les systèmes informatiques peuvent subir des altérations réelles et très élevées qui affectent leur bon fonctionnement ou les données qu'ils peuvent contenir. C'est ce qui va faire l'objet de notre analyse dans une deuxième partie.

DEUXIÈME PARTIE : Les atteintes aux systèmes et aux données informatiques

Les infrastructures de l'information sont la cible de plusieurs formes d'atteintes. Dans notre étude, on s'intéresse particulièrement à celles qui sont dirigées vers le système informatique dans le but d'altérer son fonctionnement et/ou les données qu'il contient.

Une distinction doit par ailleurs être faite entre les atteintes aux données et celles au fonctionnement d'un système. Plusieurs raisons sont en cause.

1. Tout d'abord, il est toujours considéré que les atteintes au fonctionnement des systèmes informatiques sont plus graves que les atteintes vis-à-vis des données[202].
2. Ensuite, il est possible de porter atteinte au fonctionnement d'un système sans nuire aux données qui s'y trouvent. La situation inverse est aussi valable.

Pour lutter contre ces attaques, des incriminations ont été prévues en droit pénal français et en droit criminel canadien. Bien que leurs objectifs s'avèrent les mêmes, ces deux pays, qui ont une approche juridique différente, ont choisi de faire face à ces attaques chacun à sa manière.

En France, le législateur a adopté deux infractions distinctes pour incriminer les atteintes au fonctionnement d'un système informatique d'une part, et aux données qui s'y trouvent d'autre part (Chapitre I). Au Canada, le législateur a, quant à lui, préféré regrouper les deux atteintes au sein d'une seule infraction, soit l'infraction de méfaits (Chapitre II).

---

[202] P. VERGUCHT, préc., note 34, par. 173.

Chapitre I: Adoption d'infractions distinctes en droit français

En France, le législateur a prévu l'atteinte au fonctionnement d'un « système » à l'article 323-2 du C.pén., alors que l'atteinte aux données, elle, est prévue à l'article 323-3 du même code. Pour soutenir la distinction faite par le législateur, nous allons analyser les deux infractions indépendamment l'une de l'autre.

I) Les atteintes à un système informatique et à son fonctionnement

L'article 323-2 du C.pén. se lit comme suit : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » L'infraction prévue dans cet article suppose donc que le « système » est entravé ou faussé, deux comportements qui caractérisent l'élément matériel de cette infraction et qui vont faire l'objet de notre analyse dans une première partie (A), pour ensuite tenter de relever l'élément moral (B).

A) L'élément matériel

L'analyse de l'élément matériel de l'infraction d'atteinte au fonctionnement d'un système nécessite que l'on essaye de cerner le sens des actions punissables, soit « l'entrave » et l'action de « fausser ».

1) « Entraver »

Le législateur ne définissant pas « l'entrave », on se tournera alors vers le sens commun pour considérer qu'il s'agit d'un « empêchement, [d']un frein, [d']une gêne, [d']un obstacle »[203]. Le délit d'entrave peut alors être constitué à partir d'un empêchement, d'une gêne ou d'un obstacle au fonctionnement d'un « système ». La Cour d'appel de Paris a qualifié d'entrave tout acte perpétré qui crée une perturbation dans la performance du « système » et qui entraîne un ralentissement des serveurs :

> « (…) commettent le délit d'entrave au fonctionnement d'un système de traitement automatisé de données, réprimé par l'article 323-2 du Code pénal, les prévenus qui ont procédé à l'envoi automatique [dans une messagerie accessible par le 3615] de messages et ont utilisé des programmes stimulant la connexion de multiples Minitels aux autres serveurs concernés qui ont eu des effets perturbateurs sur les performances des systèmes de traitement automatisé de données visés par ces manœuvres et ont entraîné un ralentissement de la capacité des serveurs. »[204]

Est aussi jugée constitutive d'entrave au fonctionnement d'un « système » l'utilisation d'un logiciel qui permet l'envoi d'un très grand nombre de messages (23 millions en 3 jours) en vue de saturer un serveur de messagerie[205]. Il en va de même pour l'envoi massif de courriels, qualifié de « mail bombing », en vue de saturer des boites électroniques[206].

---

[203] Dictionnaire *Le Petit Robert*, Paris, 2006.
[204] Paris, 5 avril 1994, préc., note 52, p. 13; D. 1994, Flash, n°18.
[205] Aix-en-Provence, 22 sept. 2004 : Juris-Data n° 258368, en ligne : <http://www.lexisnexis.com>,(consulté le 20 mars 2011).
[206] TGI Le Mans, 7 nov. 2003, Gaz. Pal. 20 juil. 2004, n°202, p. 44, note Barbry.

Les attaques de type déni de service – destinées à altérer le fonctionnement d'un site par une saturation de requêtes – sont aussi qualifiées d'entrave au fonctionnement d'un « système »[207].

Est également qualifiée d'entrave l'introduction d'un programme malicieux qui va paralyser le fonctionnement d'un « système »[208]. En ce sens, la Cour d'appel de Paris a jugé que :

> « La personne qui a mis au point un système dit de sécurité… qui n'avait d'autre finalité que de paralyser à échéance régulière le fonctionnement du réseau informatique de la société, et ce aux fins de s'assurer le paiement de ses factures de maintenance aux échéances convenues… qu'une telle manipulation clandestine du système informatique dont il s'agit caractérise l'intention délibérée de celui-ci, en l'occurrence, en introduisant au complet insu de l'utilisateur un verrouillage différé de données de la société par l'introduction d'une bombe logique temporisée ayant pour effet de bloquer l'exploitation du système informatique de ladite entreprise. »[209]

En somme, tous les actes qui vont saturer, paralyser ou ralentir le fonctionnement d'un système, peu importe les moyens utilisés, constitueront une entrave au fonctionnement d'un système au sens de l'article 323-2 du C.pén.

Par ailleurs, le champ de l'infraction prévue dans l'article 323-3 du C.pén. peut s'étendre au-delà des atteintes qui vont saturer, paralyser ou ralentir le système, pour contenir toute conduite ayant pour effet d'entraver le fonctionnement d'un système. En effet, la Cour d'appel de Paris a rendu un arrêt important le 5

---

[207] TGI Paris, 19 mai 2006, Gaz. Pal. 18 janv. 2007, n°18, p.35, note Forgeron et Fiévée.
[208] Alain HOLLANDE et Xavier LINANT DE BELLEFONDS, *Pratique du droit de l'informatique et de l'Internet : logiciels, systèmes, Internet*, 6e éd., Delmas, 2008, par. 1410, p. 353.
[209] Paris, 15 mars 1994, Expertises 1994, n°178, p.441.

octobre 1994[210]. Après avoir relevé que le directeur technique qui a bloqué le système informatique de l'entreprise en ne communiquant pas aux utilisateurs les clefs d'accès nécessaires a commis une infraction d'entrave au fonctionnement d'un « système », la Cour a précisé que le prévenu ne s'était pas contenté d'une simple abstention mais qu'il avait modifié le programme des clefs d'accès.

Il apparaît clairement que la Cour a hésité à admettre qu'une entrave au fonctionnement d'un système peut résulter d'une simple abstention tel le fait de ne pas communiquer les clefs d'accès. En effet, lors des travaux préparatoires à la loi du 5 janvier 1988, il a été dit que l'entrave suppose une action positive et qu'il ne saurait y avoir d'entrave par abstention[211]. Alors que cette thèse a été relevée par certains auteurs qui considèrent qu'entraver le fonctionnement d'un « système », c'est l'empêcher de fonctionner par une action positive[212], d'autres, en revanche, ont une opinion contraire, à laquelle on souscrit. Selon cette doctrine, tous les comportements qui ont pour objectif d'empêcher le fonctionnement normal d'un système constituent une entrave à ce dernier. Selon l'auteur :

> « Le terme « entraver » couvre tous les comportements qui, quelle qu'en soit la forme, ont pour résultat d'empêcher l'aboutissement du traitement : l'entrave pourrait donc être réalisée non seulement par la destruction ou la dégradation du système, mais aussi par le blocage de l'accès au système (notamment par occupation des locaux du service informatique d'une entreprise). »[213]

Il ne peut être aussi qualifié d'entrave au sens de l'article 323-2 du C.pén. la cessation de travail suite à une grève des personnels informaticiens, ce qui a eu pour effet d'entraîner une entrave au fonctionnement d'un système[214]. En revanche, le

---

[210] Paris, 5 oct. 1994, JCP E. 1995.I, étude n°461, n°21, p. 207 obs. Vivant et Le Stanc.
[211] J.O. déb.,Ass. Nat., 16 juin 1987, p.2388.
[212] R. Gassin, préc., note 38, par. 159
[213] H. CROZE, préc., note 69, par. 22.
[214] M. VIVANT *et al*.,, préc., note 87, par. 3261, p. 1910.

fait d'empêcher un non-gréviste ou l'employeur de faire fonctionner le « système » pourrait être qualifié d'entrave. Il en va de même pour les actes de sabotage ayant lieu en période de grève et atteignant les systèmes informatiques[215].

L'entrave ne peut pas non plus être constituée dans le cas d'un prestataire de services informatiques qui a refusé de continuer d'assurer ses prestations à la suite d'un litige qui l'opposait à son client ou dans le cas d'une rupture de contrat entraînant une perturbation dans le fonctionnement du système informatique[216]. Dans ce cas, la perturbation apportée au « système » « a une origine qui n'a aucun caractère délictueux, et ne saurait donc être sanctionnée comme telle »[217].

Avec l'article 323-2 du C.pén., le législateur français n'incrimine pas seulement l'entrave au fonctionnement d'un « système », mais également l'action de « fausser » le fonctionnement d'un « système ».

2) L'action de « fausser »

Le législateur ne définit pas l'action de « fausser ». Selon le *Petit Robert*, le verbe « fausser » signifie exercer une pression excessive sur un objet, ce qui va l'altérer, le changer, le dénaturer ou le rendre inutilisable[218]. On peut ainsi considérer que le fonctionnement d'un système est faussé dès lors qu'on exerce sur lui une action qui, sans nécessairement empêcher son fonctionnement, le change, le dénature, voire le rend presque inutilisable[219]. La Cour d'appel de Nîmes a rappelé qu'il y a altération du système au sens de l'article 323-2 du C.pén. dès lors que le système « produit un résultat différent de ce qu'il aurait dû être »[220]. Par conséquent,

---

[215] P. VERGUCHT, préc., note 34, par.183.
[216] A. HOLLANDE, X.-L. DE BELLEFONDS, préc., note 208, par. 1410, p. 353.
[217] Rapport ANDRÉ,, préc., note 17, n° 1087, p. 7.
[218] Dictionnaire *Le Petit Robert*, Paris, 2006.
[219] J-P BUFFELAN, préc., note 107, n° 103.
[220] Nîmes, 24 sept. 1998, LPA. 15 août 2001 n° 162, p. 4, note Mas-Bellissent et al.

a faussé le système[221] l'employé qui a changé les paramètres d'un radiotéléphone afin que soient transmises de fausses informations de façon à empêcher le déclenchement de la procédure de sécurité de même et pouvoir ainsi utiliser les lignes téléphoniques de son employeur.

Notons que les techniques employées pour fausser le fonctionnement d'un système sont diverses même si, lors des travaux préparatoires de la loi de 1988[222], monsieur André, le rapporteur à l'Assemblée nationale, a précisé que l'action de fausser visait particulièrement l'altération des ordinateurs par les « bombes logiques »[223]. En effet, on considère que l'action de « fausser » est plus large et englobe l'altération des ordinateurs par l'insertion de programmes malicieux[224]. Ces derniers peuvent causer la modification des programmes ainsi que le ralentissement ou la perturbation du fonctionnement du système. Ils peuvent aussi entraîner la destruction même de l'ordinateur. En plus des « bombes logiques », on note à titre d'exemple, les « chevaux de Troie », les« virus » et les « vers », etc.

En informatique, on appelle « bombes logiques », les programmes introduits dans l'ordinateur dans le but d'altérer le fonctionnement d'un ordinateur en introduisant des instructions qui peuvent être activées à distance. Ce type de virus est généralement employé par les compagnies de logiciels pour assurer le paiement de leurs services et produits.

Les « virus » sont des programmes d'ordinateur conçus pour se propager à d'autres ordinateurs. Ils peuvent perturber gravement le fonctionnement d'un ordinateur : destruction ou modification des fichiers ou effacement du disque dur, ce qui entraîne la perte des données. Les virus se propagent sous la forme de fichiers joints à des messages électroniques. Pour illustrer la gravité des effets des

---

[221] Paris, 18 nov. 1992, JCP E, 1994, I, étude n°359, par. 15, p. 252, obs. Vivant et Le Stanc.
[222] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.
[223] Rapport ANDRÉ, préc., note 17, n° 744, p.15.
[224] J. DEVÈZE, préc., note 87, par.59.

« virus » sur les systèmes informatiques et les réseaux, on peut citer celui nommé « I Love You », qui a provoqué en 2000 une crise mondiale sur les réseaux informatiques. Ayant les caractéristiques d'un « cheval de Troie » et d'un « virus », il se servait de la messagerie électronique Outlook pour se propager. Tentés par un message d'amour, les internautes se sont vus piégés par un virus à très haute propagation. En effet, une fois que l'internaute ouvrait le message, un cheval de Troie contenu dans ledit message effaçait les données de l'ordinateur et lisait les mots de passe avant de les envoyer à une adresse déterminée à l'avance.

D'ailleurs, un « cheval de Troie » est un programme caché à l'intérieur d'un autre programme. Une fois activé, il peut prendre des informations concernant un individu accessibles à des tiers. Il peut aussi empêcher le bon fonctionnement d'un programme.

D'autres formes de programme malicieux peuvent être rencontrées comme les « vers » qui sont des programmes conçus spécialement pour se propager à travers les réseaux. Ils sont employés pour neutraliser ou ralentir le fonctionnement des ordinateurs. Le ver libéré par Robert Tappan Morris Jr., le 2 novembre 1988, figure parmi les programmes d'ordinateur les plus destructifs. En vue de tester la vulnérabilité des ordinateurs vis-à-vis des programmes malicieux, cet étudiant a libéré un ver d'ordinateur à travers le réseau Internet. Il a ainsi causé des dommages substantiels à un très grand nombre d'ordinateurs, y compris à ceux du gouvernement et des universités aux états unis. En agissant de la sorte Morris a commis une infraction prévue dans la sous –section 1030(a) (5) (A) (i) du CFAA aux états unis[225], en vertu de laquelle il est interdit à toute personne de causer la transmission d'un programme causant des dommages a un ordinateur protégé[226].

[225] *Computer Fraud and Abuse Act*, 18 U.S.C. §1030 (a) (5) (A) (i)
[226] *U.S.* v. *Morris*, 928 F. 2d 504 (2d Cir.), cert. Denied, 502 U.S. 817 (1991)

Enfin, de l'analyse des actions susceptibles de fausser le fonctionnement d'un « système », il nous apparaît que celles-ci ressemblent beaucoup aux actions pouvant entraver le fonctionnement d'un système. Par ailleurs, « s'il est possible, en théorie, de distinguer l'action de fausser de celle d'entraver, la différence tend à s'estomper, dans certains cas du moins, à l'application »[227]. Par contre, ce qui est sûr, c'est que pour engager la responsabilité pénale de l'auteur de ces actes, il faut établir son intention délibérée de commettre un acte prohibé.

B) L'élément moral

En vertu de l'ancien article 462-3 du C.pén., l'élément moral de l'infraction supposait qu'on démontre que celui qui a entravé ou faussé le fonctionnement d'un « système » a agi « intentionnellement et au mépris des droits d'autrui ». Cette dernière expression a disparu avec le nouveau Code pénal dans son article 323-2[228]. Par ailleurs, on doit se référer aux règles de droit commun, précisément à l'article 121-3 al. 1 du C.pén., qui dispose qu'« il n'y a point de crime ou de délit sans intention de le commettre », et considérer de la sorte que le délit de l'article 323-2 du C.pén. suppose une intention[229]. Concrètement, l'auteur de l'acte doit agir en ayant conscience des conséquences de ses actes[230]. Ainsi, le prévenu qui est accusé d'avoir volontairement introduit un virus dans un logiciel d'un client, entraînant par là même l'altération de l'ensemble de son système informatique, doit être relaxé si la preuve qu'il connaissait l'existence de ce virus au moment de la duplication[231] n'est pas faite.

---

[227] R. GASSIN, préc., note 38, par.168, p.36.
[228] *Code pénal français,*, préc., note 36.
[229] M. VIVANT *et al*., préc., note 87, par. 3261, p. 1910.
[230] J. DEVÈZE, préc., note 87, par. 60.
[231] Crim, 12 déc. 1996, *Bullt. Crim*., 1996, n° 465, p. 1353.

En fait, le caractère intentionnel de l'entrave ou de l'action de fausser va souvent être relevé des faits et des circonstances de leurs commissions[232]. Justement, la Cour d'appel de Paris a jugé que la preuve du caractère intentionnel d'agissements délictueux ayant pour objet de ralentir la capacité des serveurs découle « des circonstances – éminemment volontaires – de leur commission. »[233]

Ainsi, les agissements du prévenu qui avait introduit une bombe logique dans le « système », ayant pour effet de paralyser celui-ci régulièrement dans le but de garantir le paiement de redevances de maintenances, démontrent bien son intention délibérée d'entraver le système[234]. De même, le professionnel en informatique qui a pénétré dans un système et envoyé une grande quantité de courriers électroniques et de gros fichiers à son ex-employeur pour saturer sa bande passante savait que cette pratique allait saturer le « système », et donc causer un préjudice « évidemment recherché »[235].

Notons enfin que par un jugement rendu le 20 janvier 2011, le Tribunal de grande instance de Bordeaux a relaxé du délit d'entrave au fonctionnement d'un système automatisé de données l'auteur présumé d'une attaque en déni de services contre le site d'une entreprise. Le tribunal a estimé que les faits ne relèvent pas de l'intention de nuire du prévenu[236].

II) Les atteintes aux données

L'article 323-3 du C.pén. français incrimine « le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de

---

[232] M. VIVANT *et al*., préc., note 87, par. 3261, p. 1910.
[233] Paris, 5 avril 1994, préc., note 52, p. 13.
[234] Paris, 14 mars1994, JCP E 1995, etude n° 461, n° 21, p. 207.
[235] TGI Lyon, 20 fév. 2001, Gaz. Pal. 2001, p.1686, somm.3351, note Blanchot.
[236] TGI Bordeaux, 06 janv. 2011, legalis.net, 28 mars 2011, en ligne :
<http://legalis.net/spip.php?page=jurisprudence-decision&id_article=3134>
(Site consulté le 28 mars 2011.)

supprimer ou de modifier frauduleusement les données qu'il contient ». Il convient d'abord de constater que pour l'application de cet article, le législateur exige expressément que les actions réprimées portent sur des données contenues dans le système[237]. Par conséquent, une action sur des données sorties d'un système, par exemple la manipulation de données contenues dans une disquette, ne rend pas l'article 323-3 du C.pén. applicable[238]. En revanche, la loi s'applique lorsque les données sont réintroduites dans le système[239].

La constitution de l'infraction prévue dans l'article 323-3 du C.pén. suppose la réunion d'un élément matériel (A) et d'un autre, moral (B).

A) L'élément matériel

L'article 323-3 du C.pén. définit trois façons de commettre une atteinte à l'égard des données, à savoir l'introduction, la modification et la suppression de données.

1) L'introduction de données

Introduire des données, « c'est incorporer des caractères magnétiques nouveaux dans un support existant, soit vierge, soit contenant déjà d'autres caractères magnétiques… C'est une des opérations élémentaires du traitement de l'information »[240]. À la suite de cette définition, il convient de se demander si l'objet de l'introduction est la donnée ou s'il peut aussi inclure un programme. La Cour d'appel de Paris a jugé que les prévenus qui ont distribué une disquette

---

[237] François CHAMOUX, «La loi sur la fraude informatique : de nouvelles incriminations», J.C.P. 1988. I, étude n° 3321, par.10 ; R. GASSIN, préc., note 38, par. 187; J. DEVÈZE, préc., note 87, par.64.
[238] J. DEVÈZE, préc., note 87, par.64.
[239] *Id.*
[240] J.-P. BUFFELAN, préc., note 107, n° 103.

infectée par un virus doivent être relaxés, au bénéfice du doute, du chef du délit prévu à l'article 323-3 du C.pén.[241] Le Tribunal correctionnel de Limoges a condamné pour introduction de données dans un système une personne qui avait inséré un cheval de Troie dans un système au lieu d'un autre programme chargé de gérer les entrées[242]. Ainsi, il semble que l'insertion d'un programme puisse rendre l'article 323-3 du C.pén. applicable. Par ailleurs, un constat important doit être fait. Admettons que l'on interprète la donnée d'une façon stricte et que l'on considère qu'il n'y a pas introduction de données lorsqu'il y a eu insertion d'un programme malicieux dans un système. En pratique, cette interprétation ne va pas empêcher l'application de l'article 323-3 du C.pén. dans la mesure où l'insertion d'un programme malicieux va modifier, sinon supprimer, des données contenues dans le système[243].

Notons enfin que l'introduction des données peut entrainer l'entrave d'un système informatique ou une partie de celui-ci en cas d'introduction d'un cheval de trois par exemple[244].

2) La suppression de données

Supprimer des données, c'est « retrancher des caractères enregistrés sur un support magnétique par effacement de ceux-ci, ou [effectuer] un écrasement par surimpression de nouveaux caractères sur les anciens, ou encore par transfert et stockage des caractères à supprimer dans une zone réservée de mémoire »[245]. Supprimer des données constitue donc une atteinte à leur intégrité physique, par exemple par un « effacement » ou un « écrasement »[246]. La Cour d'appel de Paris, a condamné pour la suppression ou modification frauduleuses de données dans un

[241] Paris, 15 mars 1995, JCP E 1995, étude n° 596, p. 184.
[242] Trib. corr. Limoges, 14 mars 1994, Expertises. 1994, p. 238, obs. Teboul.
[243] J. DEVÈZE, préc., note 87, par.64.
[244] P. VERGUCHT, préc., note 34, par. 179.
[245] J.-P. BUFFELAN, préc., note 107, n° 103.
[246] J. DEVÈZE, préc., note 87,par. 69.

système, les prévenus qui se sont introduits frauduleusement sur un site internet officiel et ont remplacé un texte qui y figurait par un autre dans le but de tourner en dérision le rôle d'un organisme gouvernemental[247].

En revanche, la simple copie des données si l'on n'a rien ajouté, ni modifié, ni supprimé ne constitue pas une atteinte au sens de l'article 323-3 du C.pén.[248]

Notons enfin, que la suppression des données est une opération secondaire parce qu'elle suppose l'existence préalable d'une opération d'introduction des données[249].

3) La modification de données

La modification de données « est un changement apporté à l'état des données existantes sans en modifier la nature magnétique »[250]. En effet, et à titre d'exemple, il a été à bon droit déclarée coupable de modification frauduleuse de données dans un « système » la prévenue, employée en qualité d'agent administratif dans une inspection académique, qui a majoré les notes de 17 candidats par le biais d'un logiciel de gestion des examens et ce, afin que ces derniers obtiennent leur diplôme[251]. Dans une autre affaire, un associé a procédé à une modification, dans le système de gestion informatique de la société, de la cotation des actes médicaux qu'il réalisait afin de masquer le fait qu'il percevait des honoraires supérieurs à ceux qui étaient enregistrés. Il a été reconnu coupable de modification frauduleuse de

---

[247] Paris, 28 janv. 2010: Juris-Data n°001050, en ligne : <http://www.lexisnexis.com>, (consulté le 01 juin 2011).
[248] J. DEVÈZE, préc., note 87, par. 69.
[249] J.-P. BUFFELAN, préc., note 107, n° 103.
[250] R. GASSIN, préc., note 38, par.184, p.39.
[251] Paris, 18 nov. 2010 : Juris-data n°024404, en ligne : <http://www.lexisnexis.com>,(consulté le 20 mars 2011).

données dans un système informatique, infraction prévue à l'article 323-3 du C.pén[252].

Une séparation radicale entre la modification, l'introduction et la suppression de données est très difficile[253]. En effet, pour modifier quelque chose, il faut effectuer soit des ajouts, soit des suppressions, soit des déplacements[254]. Quoi qu'il en soit, il faut que ces actions soient commises « frauduleusement » sur les données pour que l'article 323-3 du C.pén. puisse s'appliquer.

B) L'élément moral

Pour l'application de l'article 323-3 du C.pén., l'introduction, la suppression ou la modification de données doivent être commises « frauduleusement »[255]. Le délit d'atteinte aux données suppose donc un dol général. Concrètement, l'auteur de l'acte doit agir en ayant conscience qu'il n'avait pas le droit d'introduire de nouvelles données ni de supprimer ou de modifier les données contenues dans le « système »[256]. Ainsi, selon la Cour d'appel de Paris, il ne peut être reproché à un prévenu une action frauduleuse sans qu'il soit démontré l'existence de méthodes de travail ou de règles de sécurité que celui-ci aurait violées en connaissance de cause, et qui préexistaient au comportement incriminé[257]. Les prévenus qui ne savaient pas que la disquette de démonstration qu'ils ont distribuée était infectée par un virus doivent, selon la Cour d'appel de Paris, être relaxés[258]. En effet, afin d'établir l'élément moral de l'infraction prévue à l'article 323-3 du C.pén., il faut démontrer que l'auteur de l'acte a agi en sachant que l'introduction,

---

[252] Aix-en-Provence, 22 fév. 2011, Juris-data n°012158, en ligne : <http://www.lexisnexis.com>, (consulté le 20 mai 2011).
[253] Guillaume CHAMPY, *La fraude informatique*, t. 2, PU d'Aix-en-Provence, 1992, p. 553.
[254] *Id.*
[255] Art 323-3 du C.pén.
[256] J. DEVÈZE, préc., note 87, par. 72.
[257] Paris, 19 mai 1999, Gaz. Pal.18 avril 2000 n° 109, p. 51 note Tessalonikos.
[258] Paris, 15 mars 1995, préc., note 241, étude n° . 596, p. 184.

la suppression ou la modification n'étaient pas autorisées, et qu'en agissant de la sorte, il était en train de violer un interdit[259].

Par ailleurs, pour établir l'élément moral de l'infraction prévue à l'article 323-3 du C.pén., il n'est pas nécessaire de démontrer une intention de nuire. La Cour de cassation dans un arrêt rendu le 8 décembre 1999 a clairement précisé que :

> « Le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal, sans qu'il ne soit nécessaire que ces modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système, ni que leur auteur soit animé de la volonté de nuire. »[260]

Selon la Cour de cassation, l'élément moral du délit d'atteinte aux données réside dans la volonté de l'auteur de l'acte de violer un interdit. En l'espèce, un salarié a introduit une écriture dans un système comptable automatisé en sachant pertinemment que cette écriture constituait une donnée dont la suppression et la modification étaient prohibées par les règles et les principes comptables[261].

Enfin, il revient toujours aux juges de fond d'établir la preuve de l'intention frauduleuse de l'auteur de l'acte prohibé et ce, en s'appuyant sur les faits.

Pour conclure ce chapitre relatif aux atteintes au fonctionnement d'un système et aux données informatiques en droit français, on note qu'à travers l'article 323-2 du C.pén., le législateur apporte une protection efficace au « système » en incriminant celui qui entrave ou fausse son fonctionnement. Cette protection est complétée par l'article 323-3 du C.pén. qui, pour sa part, incrimine les

---

[259] J. DEVÈZE, préc., note 87, par. 73.
[260] Crim, 8 déc. 1999, *Bull. Crim*. 1999, n° 296, p. 917.
[261] *Id.*

altérations frauduleuses des données que contient le système, notamment par l'introduction de nouvelles données et la suppression ou modification des données existantes.

Toutefois, il nous apparaît que les deux infractions ont des objectifs relativement proches, entraînant par là même un risque d'incohérence. En effet, à la lumière de la jurisprudence citée, on a pu constater que ce sont principalement les atteintes perpétrées par l'utilisation de programmes malicieux, notamment les « bombes logiques », les « virus », les « chevaux de Troie », qui sont réprimées par les articles 323-2 et 323-3 du C.pén. Par conséquent, un seul acte peut répondre à la fois à l'infraction d'atteinte au fonctionnement d'un « système » et à l'infraction d'atteinte aux données. Par exemple, l'introduction d'un virus dans un système informatique peut :1) entraîner un ralentissement dans le système –délit réprimé par l'article 323-2 du C.pén. ; 2) modifier ou détruire des données – délit réprimé par l'article 323-2 du C.pén.

Cela dit, il ne faut pas non plus oublier que l'infraction d'atteinte au fonctionnement d'un « système » peut être perpétrée sans porter atteinte aux données. Il vaut mieux donc avoir une vision simple et considérer que les deux infractions sont bien complémentaires.

Contrairement au législateur français qui a prévu deux infractions distinctes pour incriminer les atteintes au fonctionnement d'un système informatique et celles aux données contenues dans ledit système, le législateur canadien, lui, a préféré adopter une seule infraction dite « synthétique »[262] pour incriminer en même temps les atteintes aux données et celles aux ordinateurs. On parle de l'infraction de « méfaits », qui va faire l'objet de notre analyse dans le chapitre qui va suivre.

[262] P. VERGUCHT, préc., note 34, par.173.

Chapitre 2 : Adoption d'une infraction « synthétique » en droit canadien : les méfaits

I) Introduction

En droit criminel canadien, il n'existe pas de disposition expresse pour réprimer les atteintes au fonctionnement d'un ordinateur et ce, à la différence du droit pénal français qui réprime de façon expresse, au sein de l'article 323-2 du C.pén., les actes commis dans le but d'entraver ou de fausser le fonctionnement d'un « système »[263].

En revanche, une protection appropriée à l'ordinateur et à son fonctionnement peut être assurée par le biais de l'infraction de méfait prévue à l'article 430(1) du C.cr.[264] Cet article se lit comme suit :

> « Commet un méfait quiconque volontairement, selon le cas : *a*) détruit ou détériore un bien; *b*) rend un bien dangereux, inutile, inopérant ou inefficace; *c*) empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime d'un bien; *d*) empêche, interrompt ou gêne une personne dans l'emploi, la jouissance ou l'exploitation légitime d'un bien. »[265]

À la lecture de cet article, on constate que le législateur réprime plusieurs comportements qui portent atteinte à un bien. L'article 428 du C.cr. définit un « bien » comme « un bien corporel immeuble ou meuble »[266]. En se basant sur cette définition, on peut donc admettre que l'ordinateur, étant un bien meuble, peut rentrer dans le champ d'application de l'article 430(1) du C.cr. et bénéficier de la

[263] Supra, p. 62.
[264] P. ROBERT, préc., note 145, p. 691.
[265] Art 430(1) du C.cr.
[266] *Code criminel*, préc., note 37, art. 428.

sorte de la protection du législateur. Ainsi, l'article 430(1) du C.cr. peut servir de fondement juridique pour sanctionner des comportements portant atteinte aux ordinateurs et à leur fonctionnement.

Il est à noter aussi que, bien avant l'entrée en vigueur de la loi de 1985 modifiant le Code criminel[267], l'infraction de méfait a aussi servi de fondement juridique pour réprimer les atteintes aux données informatiques et ce, d'une façon indirecte. Dans l'affaire *R.* v. *Turner*[268], l'accusé a manipulé un programme afin d'empêcher une compagnie américaine d'accéder à ses données stockées sur une bande d'ordinateur. L'individu en question est accusé d'avoir commis une infraction de méfait prévue au sous-paragraphe 387(1) (d) du C.cr[269] Pour sa défense, l'accusé s'est bien évidemment appuyé sur la définition d'un « bien » prévue, à cette époque, dans le cadre de l'article 385 du C.cr.[270] Il a ainsi allégué que l'article 387(1) du C.cr. ne prohibe pas les atteintes aux données stockées sur une bande d'ordinateur tant que l'ordinateur et la bande n'ont pas été endommagés. La Cour suprême de l'Ontario a rejeté cet argument, qui représente selon elle une interprétation stricte de la loi. Elle a conclu que suite aux agissements de l'accusé, la compagnie américaine ne peut plus utiliser les bandes qui sont nécessaires à l'accomplissement de son travail. La Cour a ajouté que l'infraction prévue au sous-paragraphe 387(1) d) du C.cr. ne s'applique pas lorsqu'il y a atteinte physique à un bien mais qu'elle s'applique bien lorsqu'on a gêné une personne dans la jouissance de son bien :

> « I propose to give the words of ss. 385 and 387(1) their ordinary meaning. It was on the evidence, impossible for the American companies to process their work or to use their tapes. The retrieval was interfered with. With s. 387(1) d), the physical alteration of the property is not the gist of the offence. The interference with enjoyment of

[267] *Loi de 1985 modifiant le droit pénal*, préc., note 16.
[268] (1984), 13 C.C.C. (3d) 430(Ont. H.Ct.).
[269] Aujourd'hui, c'est l'article 430(1)d) du C.cr.
[270] Aujourd'hui, c'est l'article 428 du C.cr.

> the property is the gist of the offence. I am giving the words in s. 387(1) their clear and unambiguous meaning. »[271]

On remarque ainsi que le droit criminel canadien traditionnel pouvait apporter une protection indirecte aux données informatiques par le biais de l'infraction générale de méfait, notamment lorsque les données sont fixées sur un support informatique, ou encore lorsque l'ordinateur lui-même a été l'objet d'un méfait, en conséquence duquel il est possible de perdre les données qui s'y trouvaient. Malgré cela, et vu l'importance de telles données au sein de l'entreprise, et surtout l'ampleur des atteintes aux données informatiques et de leurs répercussions sur les entreprises, il était indispensable pour le législateur à cet époque d'intervenir et de mettre en place un cadre juridique adéquat par le biais d'une infraction spécifique afin de protéger les données informatiques. En 1985, le paragraphe (1.1) fut ajouté à l'article 430 du C.cr.[272] Il se lit comme suit :

> « Commet un méfait quiconque volontairement, selon le cas : *a*) détruit ou modifie des données; *b*) dépouille des données de leur sens, les rend inutiles ou inopérantes; *c*) empêche, interrompt ou gêne l'emploi légitime des données; *d*) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit. »[273]

Aujourd'hui, par le biais de l'article 430 aux paragraphes (1) et (1.1) du C.cr., la protection du législateur canadien s'est étendue pour contenir les systèmes informatiques ainsi que les données. Par ailleurs, les paragraphes (1) et (1.1) de l'article 430 du C.cr. doivent se lire conjointement avec le paragraphe (5.1), qui incrimine toute personne qui a volontairement commis un acte ou qui a omis d'accomplir un acte alors qu'elle avait le devoir de le faire alors que, à la suite de

---

[271] *R.* v. *Turner*, préc., note 268, p. 434.
[272] *Loi de 1985 modifiant le droit pénal*, préc., note 16, art. 58.
[273] Art 430(1.1) du C.cr.

cet acte ou de cette omission d'agir, il y a eu méfait à l'égard de biens ou de données[274].

D'ores et déjà, on peut constater que le législateur canadien présente une particularité par rapport au législateur français en ce que ce dernier, à travers les articles 323-2 et 323-3 du C.pén. relatifs réciproquement au délit d'atteinte au fonctionnement d'un « système » et aux données, ne réprime que des comportements positifs tels que le fait d'entraver ou de fausser le fonctionnement d'un « système », ou encore le fait d'introduire, de supprimer ou de modifier des données. De son côté, à travers l'article 430 du C.cr., le législateur canadien semble vouloir élargir son champ de répression pour couvrir non seulement des comportements positifs – tel le fait de détruire un bien ou des données, ou de rendre ces biens ou ces données inopérants et inutiles – mais aussi des comportements négatifs[275]. En effet, en droit criminel canadien, lorsqu'une personne omet d'agir alors qu'elle avait le devoir de le faire en vertu de la loi et de la *Common Law*, elle commet une infraction d'omission[276]. Par conséquent, dans le cas d'une telle omission et si, à la suite de cette inaction, un méfait a été causé à un bien ou à des données selon les paragraphes 430 (1) et (1.1) du C.cr., cette personne est coupable d'un méfait à l'égard de biens ou de données tel que défini au sous-paragraphe 430 (5.1) du C.cr.[277]

II) Les éléments constitutifs de l'infraction de méfait

L'auteur de l'acte est condamné pour une infraction de méfait à l'égard de biens ou de données en vertu de l'article 430 du C.cr. si l'élément matériel (*actus reus*) et l'élément moral (*mens rea*) de l'infraction sont réunis. Dans l'analyse qui

[274] Art 430(5.1) du C.cr.
[275] Rachel GRONDIN, *Les infractions contre la personne et contre les biens,* 6e éd., Wilson & Lafleur, 2007, par. 161, p.178.
[276] Hugues PARENT, *Traité de droit criminel. La culpabilité (*actus reus *et* mens rea*)*, t. 2, 2e éd., Éditions Thémis, 2005, par. 38, p. 24.
[277] *R.* c. *D. (s.)* (2002), 164 C.C.C. (3d) 1 (Nfld. C.A.), par. 49.

va suivre, on va définir l'élément matériel de chaque infraction (A), pour ensuite essayer de définir l'élément moral qui se révèle le même pour les deux infractions (B).

A) L'*actus reus*

Dans un premier temps, on va définir l'élément matériel de l'infraction de méfait a l'égard d'un bien (1), pour ensuite passer à l'examen de l'élément matériel de l'infraction de méfait à l'égard des données (2).

1) Le méfait à l'égard d'un bien

L'article 430 (1) du C.cr. vise quatre façons de commettre un méfait à l'égard d'un bien.

a) La destruction ou la détérioration d'un bien

Le méfait est caractérisé au sous-paragraphe 430 (1) a) du C.cr. par « *le fait de détruire ou de détériorer un bien* »[278].

Le législateur canadien ne définit pas les verbes « *détruire* » et « *détériorer* ». En effet, le verbe « *détruire* » ne cause pas de problème d'interprétation : le méfait est commis dans ce cas lorsqu'un bien est physiquement brisé[279]. En matière informatique, on rencontre généralement cette situation lorsque

[278] Art 430(1)a) du C.cr.
[279] R. GRONDIN, préc., note 275, par. 158, pp. 176-177.

des documents imprimés, des bandes et des disquettes d'ordinateur ont été détruites, ou simplement lorsque l'ordinateur lui-même a été détruit[280].

Le problème réside plutôt au sens qu'il faut accorder au verbe « *détériorer »* pour qu'il y ait méfait. Lorsqu'on se réfère au dictionnaire, le verbe « *détériorer »* signifie « mettre quelque chose en mauvais état, le rendre inutilisable »[281]. On peut donc considérer qu'il y a méfait lorsque le bien, sans qu'il ne soit détruit, est devenu en mauvais état et inutilisable. Dans ce cas, le bien ne peut plus remplir ses fonctions comme il le faisait normalement avant d'avoir subi le dommage. Dans *Quickfall* c. *La Reine*, la question du litige résidait dans le sens qu'il faut accorder au mot « *détériorer »* utilisé à l'article 430(1)a)[282]. La Cour d'appel du Québec a jugé que :

> « Le verbe « détériorer » signifie que, du moins temporairement, l'usage ou la valeur du bien est diminué (« impaired »), que le bien a été mis en mauvais état ou gâté : en ce sens, et avec respect pour l'opinion contraire, je ne crois pas que « le moindre dommage » suffit pour constituer un méfait. »[283]

On constate ainsi que le méfait n'est pas caractérisé par des actes qui, tout en ne dépassant pas la limite de la tolérance, ne sont susceptibles de causer que des dommages très minimes à un bien. Par ailleurs, il faut que le dommage atteigne un certain « degré » pour constituer un méfait au sens du Code criminel[284]. Dans *R.* c. *Kealey*[285], la Cour d'appel du Québec a suivi la décision de la Cour dans *Quickfall* et a jugé qu'il n'y a pas eu méfait au sens de l'article 430 (1) a) du C.cr. en l'absence d'un abus réel et de dommages considérables à un bien public :

---

[280] V. GAUTRAIS, préc., note 185; D. K. PIRAGOFF, préc., note 142, p. 213.
[281] Larousse.fr, en ligne <http://www.larousse.com> (consulté le 23 novembre 2010).
[282] [1993] R.J.Q. 468 (C.A. Qué.)
[283] *Id.,* p. 471.
[284] *Id.*
[285] 1996 CarswellQue 313(WeC).

> « Given the evident political purpose of the stickers in this case, the absence of any real abuse or damage to public property, and the relatively insignificant clean-up costs, the principle set out in the *Quickfall* case should be applied here.
> In coming to this Conclusion, we do not wish to suggest that all postering, in any circumstances, however abusive or damaging to public property, will be protected and can never constitute mischief. There may well be cases where the affixing of posters will be abusive and involve serious damage to public property or serious danger to public safety. But none of such abusive or extreme circumstances were present in this case. »[286]

On constate ainsi que le méfait à l'égard d'un ordinateur, au sens de l'article 430 (1) a) du C.cr., est constitué dès lors qu'une personne commet des actes qui sont susceptibles de le détériorer. Concrètement, il s'agit de mettre l'ordinateur en mauvais état et donc de l'empêcher de remplir ses fonctions comme il le faisait normalement avant d'avoir subi le dommage. On remarque que ces actes ressemblent beaucoup à ceux qui ont pour objectif de fausser le fonctionnement d'un « système » en droit pénal français – lesquels sont prohibés en vertu de l'article 323-2 du C.pén.

Alors qu'au sous-paragraphe 430 (1) a) du C.cr., le méfait est caractérisé par le fait de *détruire* ou de *détériorer*, le sous-paragraphe 430 (1) b) du C.cr. parle d'un méfait qui rend un bien « inefficace, inutile ou inopérant », décrivant ainsi une détérioration plus marquée qu'au sous-paragraphe 430 (1) a) du C.cr.[287] Ces actes font l'objet de notre analyse dans ce qui suit.

---

[286] *Id*., par. 14-15.
[287] *Quickfall* c. *La Reine*, préc., note 282, p. 471.

b) Rendre un bien dangereux, inutile, inopérant ou inefficace

Le sous-paragraphe 430 (1) b) du C.cr. vise les cas où le bien, sans qu'il ne soit détruit, est devenu dangereux, inutile, inopérant ou inefficace. En droit français, c'est l'équivalent de l'action de « *fausser* »[288], qui a été définie comme étant « l'action exercée sur le système informatique qui, sans empêcher son fonctionnement, le change, le dénature, voire le rend presque inutilisable ». Bien qu'il y ait une différence dans la terminologie, le législateur canadien et son homologue français entendent réprimer les mêmes comportements. Il s'agit en faite de réprimer les actes qui ont pour objectif de perturber, de ralentir et de paralyser le fonctionnement d'un système informatique. Ces actes sont divers, mais il s'agit notamment de l'introduction de programmes malicieux. On note par exemple l'insertion d'un cheval de Troie, de bombes logiques, de virus informatiques ou aussi de vers.

Les sous-paragraphes 430 (1) c) et d) du C.cr. vont être traités ensemble dans ce qui suit.

c) L'empêchement, l'interruption ou la gêne dans l'emploi, la jouissance ou l'exploitation légitime d'un bien

Les sous-paragraphes 430 (1) c) et d) du C.cr. s'appliquent lorsqu'il y a eu empêchement ou gêne dans l'emploi, la jouissance ou l'exploitation légitime d'un ordinateur. Le verbe « empêcher » signifie « faire obstacle », le verbe « interrompre » signifie « rompre la continuité de » et, enfin, le terme « gêner » veut dire « interposer »[289]. En droit français, le législateur a plutôt employé le mot « *entraver* », au sein de l'article 323-2 du C.pén. pour réprimer les atteintes au

---

[288] Supra, p.66.
[289] *R.* c. *Hnatiuk*, [2000] A.J. No. 545 (Alta. Q.B.), en ligne sur <www.lexisnexis.com>, par. 46 (consulté le 01 juin 2011.)

fonctionnement d'un « système », défini ci-haut comme étant « un empêchement, une gêne, un obstacle au fonctionnement d'un système »[290]. On dénote ainsi une grande ressemblance au niveau des comportements incriminés en droit pénal français et en droit criminel canadien.

En pratique, l'infraction de méfait à l'égard d'un bien a été retenue dans le cas d'une étudiante qui a participé à une barricade organisée par plusieurs étudiants dans le but d'empêcher l'accès au centre d'informatique de l'université. Notons que cela est contraire au sous-paragraphe 372(1)c) du C.cr.[291] À cause de ses actes, les étudiants, le personnel et les chercheurs de ladite université ne pouvaient plus utiliser les ordinateurs du centre et leurs travaux se sont trouvés interrompus pendant plusieurs jours[292]. De même, en 1985, un fonctionnaire a été condamné sous 37 chefs d'accusation de méfaits concernant un bien et ce, pour avoir perturbé et arrêté, de façon continue et répétée le système informatique gouvernemental sur lequel il travaillait. L'interruption du système informatique a causé des dommages élevés à cent trente-huit mille dollars (138 000$) ainsi que l'arrêt de travail du personnel de cent cinquante (150) points d'émission des chèques au Québec, entraînant par là même des retards dans l'émission de ces derniers[293].

En ce qui a trait au mot « *jouissance* », un débat a eu lieu sur le sens qu'il faut lui donner. Doit-on interpréter le mot « *jouissance* » d'un point de vue objectif et limiter ainsi le sens de ce mot au seul droit de posséder un bien? Ou doit-on l'interpréter d'un point de vue subjectif en lui donnant un sens plus large qui inclut l'action de tirer d'un bien qu'une personne détient légalement les satisfactions que ce bien est en mesure de procurer?

---

[290] Supra, p. 63.
[291] Aujourd'hui, c'est l'art. 430(1)c) du C.cr.
[292] *Re A.C.S.* (1969), 7 C.R.N.S. 42 (C.S. Que.), p.42.
[293] *R.* c. *Lachance*, 1985 CarswellQue 126 (C.S.P.) (WeC)

Dans *R.* c. *Drapeau*, le juge Fish a interprété d'une façon objective le mot « *jouissance* » :

> « I do not believe that « enjoyment » in section 430(1) d refers to a purely subjective state, such as the nature or intensity of the pleasure derived from a property by its owner, possessor or occupant. Nor I believe that a person, who diminishes that pleasure, even knowingly, is liable for that reason alone to conviction for criminal mischief.
> To conclude otherwise, in my respectful view, is to make of crime in relation to property an offence against feelings and tastes. »[294]

Contrairement au juge Fish, le juge Chamberland, dissident, a interprété d'un point de vue subjectif le mot « *jouissance* » :

> « Si le parlement avait voulu que le mot « jouissance » signifie « possession », il aurait utilisé le mot « possession ». L'article 430(1)d) est rédigé de manière à viser le bien dans son aspect dynamique (l'emploi, la jouissance ou l'exploitation d'un bien) plutôt que dans son aspect statique (la propriété, le louage ou la possession). L'utilisation du mot « jouissance » s'inscrit tout à fait dans cette logique.
> À mon avis, le mot « jouissance » a ici un sens plus englobant que le seul fait d'être titulaire d'un droit à la possession du bien; il inclut l'action de tirer d'un bien qu'une personne détient légalement les satisfactions que ce bien est en mesure de procurer. »[295]

[294] *R.* c. *Drapeau*, [1995] R.J.Q. 320 (C.A. Qué), p. 325.
[295] *Id.,* p. 328-329.

Il est à noter que plusieurs décisions qui ont suivi l'affaire *Drapeau* ont adopté l'opinion du juge Chamberland et ont interprété le mot « *jouissance* » d'un point de vue subjectif[296].

L'infraction de méfait prévue au sous-paragraphe 430(1)d) du C.cr. est retenue dans l'affaire *Turner* où la Cour supérieure de l'Ontario a jugé que l'accusé a gêné la compagnie, pour laquelle il travaille, dans la jouissance de son bien[297] et ce, lorsqu'il a manipulé un programme pour empêcher celle-ci d'accéder à la bande d'ordinateur.

En revanche, la personne qui a cessé de travailler – et a donc interrompu le fonctionnement d'un système – suite à un désaccord avec son employeur sur une question quelconque touchant son emploi ne commet pas un méfait[298]. De ce fait, on constate qu'en droit criminel canadien, comme en droit pénal français d'ailleurs, la cessation de travail ne constitue pas une atteinte au fonctionnement d'un système informatique.

2) Le méfait à l'égard des données

Au sens du sous-paragraphe 430(1.1) du C.cr., quatre comportements peuvent constituer une infraction à l'égard des données. Mais avant de passer à l'analyse de ces comportements, rappelons tout d'abord la définition du terme « données » prévue par le législateur canadien au sein de l'article 342.1(2) du C.cr. Une « donnée » est définie comme étant « la représentation d'information ou de concept qui est préparée ou l'a été de façon à pouvoir être utilisée dans un ordinateur »[299]. L'infraction de méfait s'applique essentiellement en cas d'atteinte

---

[296] *R.* c. *Maddeaux* (1997), 6 C.R. (5th) 176(Ont. C.A.), par. 11-12, p. 181; *R.* c. *Nicol* (2002), 170 C.C.C. (3d) 59(Man.CA.), par.5, p. 61.
[297] *R* v.*Turner*, préc., note 268, p. 434.
[298] Art 430 (6) a) du C.cr.
[299] Art 342.1(2) du C.cr.

aux données contenues dans un ordinateur. Toutefois, en raison de l'expression « à pouvoir être utilisée dans un ordinateur » employée dans la définition du terme « donnée », cette infraction conserve toute sa pertinence lorsque les données ne se trouvent pas dans l'ordinateur[300]. L'infraction de méfait peut alors s'appliquer lorsque les données sont en cours de transmission ou lorsqu'elles sont inscrites sur un dispositif mobile non relié à l'ordinateur :

> « It is also important to note that data does not have to be within a computer at the time of its destruction, alteration or interference. Computer data may be attacked in the course of telecommunication or by placing a strong magnet, for example, in close proximity to a tape or disk, thereby erasing or rearranging the electromagnetic representations recorded therein. In Canada, the use of the phrase « in a form suitable for use in computer system » in the definition of « data », as opposed to « in a computer system », includes within the scope of protection not only data in transmission but data in a computer media which may not, at the relevant time, be in direct association with the computer system. With the refinement of optical readers and audio input and output, this definition could in future include program source code or other data in hard copy form, such as writings on paper, and oral speech. »[301]

À cet égard, il faut rappeler qu'à la différence du législateur canadien, le législateur français prévoit de façon expresse au sein même de l'article 323-3 du Code pénal français, relatif aux atteintes aux données, que ce dernier ne s'applique que lorsqu'il y a eu atteinte aux données se trouvant dans un « système ». Peut-on conclure ainsi que le droit criminel canadien offre une protection plus large aux données que celle prévue en droit pénal français ? A priori, il nous semble que la réponse à cette question est oui. Cela est certainement dû au caractère évolutif du crime informatique. En adoptant une infraction large, le législateur n'est pas obligé d'intervenir à chaque fois qu'un changement est opéré dans la technologie.

---

[300] D.K. PIRAGOFF, préc., note 142, p. 216.
[301] *Id.*

Toutefois, il faut être prudent et attendre de voir comment les tribunaux, au Canada, vont interpréter et appliquer le paragraphe 430(1.1) du C.cr., et ce, d'autant plus que jusqu'à aujourd'hui, en 2011, la jurisprudence relative à l'application du paragraphe 430(1.1) du C.cr. est quasi absente.

L'article 430(1.1) du C.cr. définit quatre façons de commettre un méfait à l'égard des données. Il est à noter que la jurisprudence relative à l'application du paragraphe 430(1.1) du C.cr. est quasi absente. Pour les fins de notre analyse, on va se référer au besoin à la jurisprudence américaine, qui est très abondante en matière de crimes contre les ordinateurs[302].

a) La destruction ou la modification de données

Dans le sous-paragraphe 430(1.1) a) du C.cr., le législateur canadien incrimine le fait de « *détruire* » des données. A titre d'exemple, Dans *R.* v. *Downs*[303], le défendeur a supprimé des données qui se trouvaient dans l'ordinateur de son ex-employeur. Selon la Cour provinciale de la Saskatchewan, la destruction des données par le défendeur caractérise une infraction de méfait prévue au paragraphe 430(5) du C.cr.[304] Selon cette décision, tout effacement ou toute suppression de données constituent une destruction de données. On constate ainsi que, tout comme son homologue français, le législateur canadien considère que la suppression des données informatiques constitue une atteinte à celles-ci.

Les techniques utilisées pour détruire les données sont diverses. S'inspirant de la jurisprudence américaine en matière de crimes contre les ordinateurs, on constate que la destruction de données peut avoir lieu suite à l'insertion d'un

[302] On a jugé intéressant de faire référence à la jurisprudence américaine étant donné que la jurisprudence canadienne en matière d'atteinte aux données est quasi absente.
[303] [1996] S.J. NO 703 (Sask. Prov. Ct.), en ligne : <www.lexisnexis.com>, (consulté le 01 juin 2011)
[304] *Id*., par. 8.

programme malicieux ou d'un microcode dans un ordinateur[305]. Il faut préciser à cet effet que dans plusieurs États américains, les lois relatives aux crimes reliés aux ordinateurs confèrent une grande importance au droit de maintenir l'intégrité des données qui se trouvent dans un système informatique. On peut citer à titre d'exemple le Code pénal de l'État de New York qui incrimine, comme l'article 430(1.1) a) du C.cr, le fait de détruire ou d'altérer intentionnellement les données informatiques au sein de sa section 156-25(4)[306]. En pratique, la Cour civile de l'État de New York a condamné un consultant en informatique pour avoir détruit des données qui se trouvaient dans le système informatique d'une firme d'avocats lorsqu'il a installé une bombe logique dans ledit système[307].

Le sous-paragraphe 430(1.1) a) du C.cr. incrimine le fait de détruire des données, mais aussi le fait de les modifier. Le verbe « modifier » n'est toutefois pas défini. Par ailleurs, dans la version anglaise, le législateur canadien emploie au sous-paragraphe 430(1.1) a) du C.cr. le mot « alter ». Dans l'affaire *People* v. *Versaggi*[308]*,* la Cour d'appel de l'État de New York définit ainsi ce terme :

> « As commonly understood, « alter » means to change or modify. When something is altered it is made « different in some particular characteristic * * * without changing [it] into something else » (Webster's Third New International Dictionary 63 [Unabridged]). For an alteration to occur, the identity of the thing need not be destroyed, nor need an entirely new thing be substituted. It is sufficient if some of the « elements or ingredients or

[305] *Burleson* v. *State*, 802 S.W. 2d 429 (Tex. App.—Fort Worth 1991); *State* v. *Corcoran,* 186 Wis.2d 616(Wis. Ct. App. 1994).
[306] NY. PEN. LAW §156-25(4). En ligne : <http://ypdcrime.com/penal.law/article156.htm#156.25>, (consulté le 30 mai 2011). Cette disposition se lit comme suit: "A person is guilty of computer tampering in the third degree when he commits the crime of computer tampering in the fourth degree and : 4)he intentionally alters in any manner or destroys computer data or a computer program so as to cause damages in an aggregate amount exceeding one thousand dollars."
[307] *Werner, Zaroff, Slotnick, Stern & Askenazy* v. *Lewis*, 588 N.Y.S. 2d 960 (N.Y. Civ. Ct. 1992)
[308] 608 N.Y.S. 2d 155 (NY. Ct. App. 1994)

> details » are changed (Black's Law Dictionary 103 [4th ed]). »[309]

S'inspirant de cette jurisprudence, on peut admettre qu'il y a altération de données lorsque, sans qu'elles ne soient détruites, on a apporté un changement ou une modification à leur état initial.

Justement, dans *R.* c. *Dessureault*[310], la Cour du Québec a condamné l'accusée pour avoir commis l'infraction de méfait à l'égard de données. Selon les faits, il a modifié des données d'ordinateur, qui servent à émettre des chèques d'aide sociale, pour pouvoir transférer des fonds publics dans un compte fictif et en bénéficier avec conjoint. Ils ont retiré un total d'un peu plus de 22 000,00 $.

À cet effet, notons que le législateur français, comme son homologue canadien, incrimine les actes qui ont pour but la modification de données[311]. Cette dernière expression est aussi définie comme étant « un changement apporté à l'état des données existantes sans en modifier la nature magnétique »[312].

b) Dépouiller les données de leur sens, les rendre inutiles ou inopérantes

Le fait de dépouiller les données de leur sens, de les rendre inutiles ou inopérantes constitue aussi un méfait à l'égard de données. Notons à cet effet, que l'atteinte aux données ici peut consister en une modification de celle-ci[313]. En effet,

---

[309] *Id*., p. 159, par. 2.
[310] 1990 WL 1053246 (C.Q.)(WeC)
[311] Art. 323-3 du C.pén.
[312] Supra, p.73.
[313] P. VERGUCHT, préc., note 34, par. 175.

pour dépouiller les données de leurs sens, pour les rendre inutilisables voire inopérantes, il faut nécessairement les changer[314].

c) L'empêchement, l'interruption ou la gêne dans l'emploi légitime des données ou le refus de fournir l'accès à des données à une personne qui y a droit

Les sous-paragraphes 430(1.1)c) et d) du C.cr. prévoient que les actes ayant pour but d'intervenir dans l'emploi légitime de données ou de refuser l'accès à des données à une personne qui y a droit constituent un méfait à l'égard de données. L'affaire *Turner*[315] illustre bien cette situation. Rappelons que dans cette affaire, le défendeur a manipulé un programme d'ordinateur afin d'empêcher une compagnie américaine d'accéder à ses données stockées sur une bande d'ordinateur. Cet individu est accusé d'avoir commis une infraction de méfait prévue au sous-paragraphe 430(1) (d) du C. cr. L'infraction de méfait a aussi été retenue dans le cas d'attaques informatiques faites contre le serveur d'une compagnie, lesquelles ont causé une congestion du service internet durant plusieurs jours. Par conséquent, ce service a été soit carrément interrompu ou dispensé de façon intermittente, Cela a généré des coûts importants pour les propriétaires du serveur s'élevant à 100 000,00 $ ainsi que la perte de nombreux clients, dont l'un apportait des revenus annuels de 20 000,00$[316].

On constate ainsi que le fait de détruire des données, de les modifier, de les dépouiller de leur sens, de les rendre inutiles ou inopérantes, d'empêcher, gêner ou interrompre leur emploi ou refuser de fournir l'accès à des données à une personne qui y a droit constitue un méfait à l'égard des données.

---

[314] *Id.*
[315] *R.* v. *Turner*, préc., note 268.
[316] *R.* c. *Paiement*, [2003] J.Q. NO 4605 (C.Q.)

Par ailleurs, une question très importante s'est posée devant la Cour supérieure de l'Ontario dans *R.* v. *Alexandre*[317]. Il s'agissait de savoir si le champ de l'infraction de méfait telle que décrite par le législateur au paragraphe 430(1.1) du C.cr., pouvait s'étendre au delà des atteintes prévues expressément, au vol de données.

En l'espèce, la prévenue a accédé de façon frauduleuse et sans aucun droit à l'ordinateur de la Banque Royale en Ontario pour voler des données confidentielles. Elle fut accusée d'avoir commis l'infraction prévue à l'article 342.1(1)c) du C.cr., qui interdit à quiconque, frauduleusement et sans apparence de droit, d'utiliser directement ou indirectement un ordinateur dans l'intention de commettre l'infraction de méfait.

Selon la Cour supérieure de justice de l'Ontario, lorsque le Parlement a énuméré les différentes façons de commettre un méfait à l'égard de données, il n'avait pas l'intention d'inclure le vol de données dans le sous-paragraphe 430(1.1) du C.cr. Toutefois, cela n'exclut pas le fait que le vol de données peut entraîner un méfait à l'égard de données tel que décrit à l'article 430(1.1) du C.cr. :

> « the application of the maxim expressio unius, exclusivio alterius to s. 430 (1.1) does suggest that Parliament, in enumerating various ways in which mischief to data can be committed, did not mean to include the stealing of data as a form of mischief to data. On the other hand, this is a highly technical area and it seems at least possible that if data, or some part thereof, was « stolen », this same act could possibly alter the data [s. 430(1.1) (a)]; render it meaningless, useless or ineffective [s. 430(1.1) (b)]; or obstruct, interrupt or interfere with its lawful use [s. 430(1.1) (c) and (d)]. Therefore, it would be unwise to

[317] 2006 CarswellOnt 4765(S.C.J.) (WeC)

> attempt to resolve this issue without the assistance of expert evidence with respect to computer data. »[318]

Avec raison, la Cour a répondu à cette question avec prudence. Personnellement, je partage l'avis de la Cour. En effet, si le législateur avait voulu considérer le vol de données comme un acte constituant de l'infraction de méfait à l'égard de données, il l'aurait expressément prévu dans l'article 430(1.1) du C.cr.

Pour qu'un individu soit reconnu coupable d'une infraction de méfait à l'égard de biens ou de données, le législateur exige en plus d'un acte matériel une intention criminelle lors de la perpétration des actes interdits (la *mens rea*).

B) La *mens rea*

Le législateur prévoit à l'article 430 du C.cr. que l'acte prohibé doit être accompli « volontairement ». Cet adverbe est expressément défini au sein de l'article 429(1) du C.cr. Selon cette disposition :

> « Quiconque cause la production d'un événement en accomplissant un acte, ou en omettant d'accomplir un acte qu'il est tenu d'accomplir, sachant que cet acte ou cette omission causera probablement la production de l'événement et sans se soucier que l'événement se produise ou non, est, pour l'application de la présente partie, réputé avoir causé volontairement la production de l'événement. »[319]

D'après l'article 429(1) du C.cr, l'adverbe « volontairement » exige que l'auteur de l'acte prohibé ait connaissance que son acte ou son omission d'agir va certainement causer un résultat interdit. De ce fait, il a agi intentionnellement ou par

---

[318] *Id.,* par. 61.
[319] Art. 429(1) du C.cr.

insouciance quant à la production du résultat interdit[320]. L'insouciance a été définie par la Cour suprême du Canada dans *Sansregret* c. *La Reine*[321], sous la plume du juge McIntyre :

> « Conformément aux principes bien établis en matière de détermination de la responsabilité criminelle, l'insouciance doit comporter un élément subjectif pour entrer dans la composition de la *mens rea* criminelle. Cet élément se trouve dans l'attitude de celui qui, conscient que sa conduite risque d'engendrer le résultat prohibé par le droit criminel, persiste néanmoins malgré ce risque. En d'autres termes, il s'agit de la conduite de celui qui voit le risque et prend une chance. »[322]

Une personne commet donc un méfait « volontairement » lorsqu'il a été prouvé qu'elle avait une intention de détruire les biens ou les données ou si elle a tout de même persisté sans se soucier des conséquences de l'acte posé alors qu'elle était consciente que son acte ou son omission d'agir risque d'engendrer un résultat prohibé par la loi. L'infraction de méfait exige donc une intention générale[323]. Dans *R.* c. *Worrell*, le juge de la Cour municipale de Montréal a statué que « l'infraction prévue à l'article 430 du Code criminel en est une d'intention générale. Il suffit que la poursuite démontre que l'accusé savait ou aurait dû raisonnablement savoir ou prévoir la conséquence naturelle de ses actes. »[324] Ainsi, l'infraction de méfait n'exige-t-elle pas une preuve d'intention spécifique, comme l'a d'ailleurs rappelé la Cour d'appel du Québec dans *R.* c. *Guillemette* :

> « On pourrait dire que le méfait exige une intention spécifique en ce sens que la poursuite doit prouver la volonté de l'inculpé de détruire ou de détériorer un bien (art. 387 C. cr.). Cependant, la seule connaissance du prévenu que l'acte qu'il pose, causera probablement la

[320] H. PARENT, préc., note 276, p. 184; R. GRONDIN, préc., note 275, par. 163, p. 180.
[321] [1985] 1 R.C.S. 570.
[322] *Id*., p. 582.
[323] H. PARENT, préc., note 276, p. 184; R. GRONDIN, préc., note 275, par. 163, p. 180.
[324] [1993] R.J.Q. 295, 304, en ligne sur <www.lexisnexis.com>, par. 76, (consulté le 01 juin 2011.)

> destruction ou la détérioration d'un bien et son insouciance quant à ce résultat suffisent pour que l'acte soit considéré comme volontaire (art. 386 C. cr.).
> Il s'agit dès lors moins qu'une intention spécifique puisque la seule connaissance des conséquences de l'acte et l'insouciance du résultat suppléent à la volonté spécifique de commettre la destruction.»[325]

Il apparaît ainsi que le législateur canadien, tout comme son homologue français, n'exige pas d'intention spécifique pour caractériser l'élément moral du délit d'atteinte au fonctionnement d'un « système » ou aux données[326]. Dans ce cas, une intention générale de commettre un acte interdit par la loi est suffisante.

Notons enfin que, même si sa *mens rea* de l'infraction de méfait est prouvée, un accusé peut être disculpé s'il fournit une justification ou une excuse légale à son comportement ou encore s'il a agi avec apparence de droit. Le paragraphe 429(2) du C.cr. prévoit : « Nul ne peut être déclaré coupable d'une infraction visée aux articles 430 à 446 s'il prouve qu'il a agi avec une justification ou une excuse légale et avec apparence de droit »[327]. Doit-on alors comprendre que pour être disculpé d'une infraction de méfait, l'accusé doit, en sus de fournir une justification ou une excuse légale, prouver qu'il a agi avec apparence de droit ? Selon la Cour d'appel de l'Ontario, la réponse est non :

> « We are all of the view that the word 'and' which precedes the words 'with colour of right' in s. 386(2) should be read as 'or'. Manifestly, it would not be sensible to require the accused to prove not only that he acted with legal justification or excuse, but also with color of right. If the accused acted with legal justification or excuse he is not criminally liable and that is the end of

[325] [1981] J.Q. no 132 (C.A. Qué.), en ligne sur <www.lexisnexis.com>, par. 11-12, (consulté le 01 juin 2011). Voir dans le même sens *R.* c. *Toma* (2000), 147 C.C.C. (3d) 252(B-C. C.A.), p. par. 15-16-17, p. 257-258. (Selon la Cour d'appel de la Colombie Britannique, « L'emploi du mot "volontairement" à l'article 430 du *Code criminel* ne signifie pas que le ministère public doit prouver une « intention malicieuse ».)
[326] Supra, p. 66et 71.
[327] Art. 429(2) du C.cr.

> the matter and there is no need to resort to colour of right. We think that 'colour of right' in this context means an honest belief in a state of facts which, if it existed, would be a legal justification or excuse: see *R.* v. *Johnson* (1904), 7 O.L.R. 525. » [328]

Suivant cette interprétation, l'accusé n'est donc pas obligé, lorsqu'il a une justification ou une excuse légale, de démontrer en plus une apparence de droit. À cet effet, une « apparence de droit » comprendrait toute situation dans laquelle une personne croit honnêtement, mais à tort, qu'elle a le droit de poser l'acte qu'on lui a reproché. Citons par exemple la destruction ou la modification de données. Cela permet à l'accusé de « soulever une erreur provenant de l'ignorance de la loi ou de la mauvaise interprétation d'un texte de loi »[329].

Pour conclure ce chapitre relatif aux atteintes au fonctionnement d'un ordinateur et aux données en droit canadien, on constate que le droit criminel canadien s'est adapté à la nouvelle technologie de l'information. Il a su apporter une réponse adéquate quant aux atteintes relatives aux ordinateurs par le biais de l'infraction générale de méfait. Par l'insertion du paragraphe (1.1) à l'article 430 du C.cr., le droit criminel canadien offre a priori aussi aux données informatiques une protection satisfaisante. En effet, une évaluation effective de cette infraction ne peut avoir lieu tant que les tribunaux ne l'ont pas analysée à la lumière de cas réels. Or, comme on l'a déjà mentionné ci-haut, la jurisprudence relative à cette infraction est quasi absente[330].

---

[328] *R.* v. *Creaghan*, (1982) 1C.C.C. (3d) 449(Ont. C.A.), p. 453*;* l'interprétation donnée par la Cour d'appel au mot « et » employé dans le paragraphe 429(2) du C.cr. fut adoptée dans plusieurs affaires ultérieures : *Steward* c. *Canada (Ministère de l'Emploi et de l'Immigration)*, [1988] 3 C.F. 487, p.492; *R.* c. *Ospina*, [1990] J.Q. nº 1936, no 8(C.S.)(QL/LN); *R.* v. *Corroll*, (2007) 296 Sask. R. 303(Prov. Ct.), par. 9, p. 304.
[329] R. GRONDIN, préc., note 275, par. 165, p. 182.
[330] Supra, p.86.

Conclusion de la partie II

L'étude des atteintes aux systèmes informatiques et aux données nous a permis de voir comment deux pays de conceptions juridiques différentes ont fait face à la criminalité liée à l'informatique. On a pu constater dans cette partie que, même si chaque pays a choisi sa manière de résoudre le problème, leurs objectifs se sont finalement révélés être les mêmes.

Alors que le législateur français a choisi de traiter l'atteinte aux systèmes informatiques et celle aux données indépendamment l'une de l'autre, le législateur canadien a préféré regrouper les deux infractions au sein d'une seule infraction. L'étude de ces infractions nous a montré que ce sont presque les mêmes comportements qui sont réprimés. Toutefois, certaines différences demeurent.

D'abord, concernant les comportements incriminés, le législateur canadien a prévu dans le paragraphe 430(5.1) du C.cr. que toute omission d'agir entraînant une atteinte à un bien ou à des données est aussi réprimée. À la différence du législateur canadien, le législateur français, eu égard aux paragraphes 323-2 et 323-3 du C.pén., n'entend réprimer que les actes positifs. Cela rend l'infraction en droit criminel canadien plus large que celle prévue par le droit pénal français.

En suite, l'autre spécificité que l'on peut mentionner est celle qui se rapporte à l'infraction d'atteinte aux données. Alors que le législateur français ne protège que les données qui se trouvent dans un « système », le législateur canadien entend élargir sa protection pour couvrir les données contenues dans un ordinateur, mais aussi celles qui sont en cours de transmission ou qui sont inscrites sur un dispositif mobile non relié à l'ordinateur.

CONCLUSION GÉNÉRALE

En traitant certaines infractions qui portent atteinte à la sécurité et à l'intégrité du système informatique dans l'entreprise à la lumière du droit pénal français et du droit criminel canadien, on a pu constater que les deux pays disposent d'un cadre juridique adéquat pour lutter contre ces infractions, mais également que les conceptions de tradition civiliste et de *Common Law* ne présentent plus de grandes différences.

Lors de ce travail, on a vu que le législateur français et son homologue canadien ont renforcé leurs cadres juridiques respectifs afin de lutter contre certains crimes liés à l'émergence des technologies de l'information et de la communication et ce, non seulement dans notre vie quotidienne mais surtout dans celle des entreprises. De la sorte, le législateur français a adopté la loi « Godfrain » en 1988[331], en vertu de laquelle il a ajouté certaines dispositions au Code pénal qui traitent des atteintes au « système de traitement automatisé des données ». Bien avant cela, en 1985, le législateur canadien a adopté la même démarche et a modifié le Code criminel en y ajoutant des dispositions qui visent à protéger l'ordinateur et les données informatiques. Par ailleurs, on a pu constater que malgré certaines différences, ces dispositions tendent à réprimer deux comportements essentiels : l'accès illicite au système informatique (incluant les réseaux) et les atteintes que ce dernier ainsi que les données peuvent subir suite à cela.

Dans un premier temps, notre étude a porté sur l'infraction d'accès illicite aux systèmes et aux données informatiques. On a pu constater que l'infraction prévue au sein de l'article 323-1 du C.pen. se présente en droit pénal français sous une double forme : l'accès a « système de traitement automatisé de données » et le maintien dans celui-ci. Bien que la notion« système de traitement automatisé de

[331] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, préc., note 17.

données » soit définie de manière suffisamment large pour englober les réseaux informatiques et, par conséquent, les interceptions de communications effectuées grâce à cet accès, on a relevé que le législateur a préféré traiter l'interception des communications, au niveau du Code pénal, dans la partie relative à l'atteinte au secret des correspondances. Notons à cet effet que seules les communications privées bénéficient de cette protection pénale. Par conséquent, les communications informatiques ne peuvent être protégées que de manière indirecte à travers l'infraction d'accès prévue à l'article 323-1 du C.pén.

A la différence du législateur français, le législateur canadien a adopté une démarche différente : à travers l'infraction d'utilisation non autorisée prévue dans l'article 342-1(1) du C.cr. il réprime dans le premier alinéa celui qui obtient un service d'ordinateur. Du fait de la définition de « service d'ordinateur », cette infraction vise à protéger les fonctions effectuées par l'ordinateur. Dans le deuxième alinéa, le législateur interdit les interceptions des fonctions d'ordinateur. Sont notamment visées par cette protection les communications informatiques, en l'occurrence les communications entre deux ordinateurs, celles entre une personne et un ordinateur ou, enfin, celles à l'intérieur d'un système informatique.

On a pu constater dans la première partie que le législateur français comme son homologue canadien souhaitent sanctionner tous les cas dans lesquels une personne se sera introduite dans un système informatique, avec la conscience du caractère irrégulier de son acte.

Dans un second temps, notre étude a porté sur les atteintes que le système et les données informatiques peuvent subir. En effet, à la suite d'un accès à un système informatique, qu'il soit licite ou illicite, des dommages au fonctionnement d'un système et/ou aux données informatiques peuvent être provoqués.

On a pu constater que le législateur français a adopté deux infractions distinctes pour réprimer d'un côté les atteintes au fonctionnement d'un « système », et de l'autre côté, celles aux données. Par contre, à travers l'infraction de méfait, le législateur canadien sanctionne aussi bien les atteintes à l'ordinateur que celles relatives aux données. Malgré cette différence dans la manière de procéder, on a pu constater qu'il existe beaucoup de ressemblances entre les infractions françaises et canadiennes, même si certaines spécificités demeurent.

En fait, l'étude de ces infractions nous a montré que ce sont presque les mêmes comportements qui sont réprimés par les deux législateurs. Concernant les atteintes au système informatique, c'est le fait d'empêcher, d'entraver, de perturber, de ralentir et de paralyser le fonctionnement ou l'utilisation d'un système informatique, voire même le fait de produire un fonctionnement erroné ou de fausser celui-ci – notamment par l'introduction de programmes malicieux–, qui est visé par les infractions française et canadienne. Pour ce qui est des atteintes aux données, ce sont les actes qui ont pour objet de modifier, de détruire ou de supprimer les données qui sont aussi visées. À ce stade, on a aussi pu constater qu'à la différence du législateur canadien, le législateur français prévoit de façon expresse, au sein même de l'article 323-3 du C.pén. relatif aux atteintes aux données, que ce dernier ne s'applique que lorsqu'il y a eu atteinte aux données se trouvant dans un « système ». Cela est contraire à ce qu'a fait le législateur canadien qui entend élargir sa protection pour couvrir les données contenues dans un ordinateur, mais aussi celles qui sont en cours de transmission ou qui sont inscrites sur un dispositif mobile non relié à l'ordinateur. Enfin, on a pu également remarquer que l'infraction de méfait prévue en droit criminel canadien est plus large que les infractions relatives à l'atteinte au fonctionnement d'un « système » et aux données prévues en droit pénal français. En effet, à côté des actes positifs expressément décrits et réprimés au sein de l'article 430 (1) et (1.1) du C.cr., le législateur canadien a aussi prévu dans le paragraphe 430(5.1) du C.cr. que toute omission d'agir entraînant une atteinte à un bien ou à des données est aussi

réprimée. Cela est contraire à ce qu'a fait le législateur français qui, eu égard aux paragraphes 323-2 et 323-3 du C.pén., n'entend réprimer que les actes positifs.

Il nous semble finalement que les cadres juridiques mis en place par les législateurs français et canadien sont en mesure d'apporter des réponses satisfaisantes pour lutter contre certains crimes liés à l'informatique, notamment ceux relatifs à l'accès non autorisé aux systèmes informatiques, aux interceptions de communications, de même que les atteintes au fonctionnement du système informatique et aux données. Par ailleurs, il est important de ne pas négliger le fait que les crimes liés à l'informatique ont un caractère évolutif. C'est pour cela qu'ils vont toujours avoir de l'avance par rapport au droit. Pour cette raison, nous pensons qu'il serait nécessaire pour chaque pays de réviser de façon constante sa législation afin de l'adapter aux nouvelles formes d'atteintes.

LES TABLES BIBLIOGRAPHIQUES

TABLE DE LA LÉGISLATION

Canada

Code criminel, L.R.C. (1985), c. C-46, mod. par L.R.C. (1985), c.2 (1er supp.), en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-46/derniere/lrc-1985-c-c-46.html>, (consulté le 03 mai 2011)

Loi de 1985 modifiant le droit pénal, S.C. 1985, C-18, c. 19, art. 46 et art. 58
Loi sur la preuve au Canada, L.R., 1985, ch. C-5, en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-5/derniere/lrc-1985-c-c-5.html>, (consulté le 08 juin 2011)

Loi sur le droit d'auteur, LRC 1985, c C-42, en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-c-42/derniere/lrc-1985-c-c-42.html>, (consulté le 08 juin 2011)

Loi sur l'entraide juridique en matière criminelle, L.R. 1985, ch.30(4e Suppl), en ligne : <http://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-30-4e-suppl/derniere/lrc-1985-c-30-4e-suppl.html>, (consulté le 08 juin 2011)

Loi de 1996 visant à améliorer la législation pénale, L.C. 1997, ch. 18, art. 19.

États-Unis

Texte fédéral

Computer Fraud and Abuse Act, 18 U.S.C. §1030 (a) (5) (A) (i)

Texte étatique

NY. PEN. LAW §156-25(4). En ligne : <http://ypdcrime.com/penal.law/article156.htm#156.25>

France

Textes législatifs

Code de procédure pénale, en ligne :
<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&dateTexte=20091003>, art. 100 et suiv.

Code des postes et des communications électroniques, En ligne:
<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987&dateTexte=20080505> (consulte le 04 mai 2011), art. L-32.

Code pénal français, 108e édition, Paris, Dalloz, 2011, en ligne :
<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110503>, (consulté le 03 mai 2011)

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 7 janv. 1978, p.227, en ligne :
<http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19780107&numTexte=&pageDebut=00227&pageFin= >, (consulté le 08 juin 2011)

Loi n° 85-660, du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle, J.O. 04 juil. 1985*,* en ligne :
<http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000693451>, (consulté le 08 juin 2011)

Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique, J.O. 6 janv. 1988, p.231. En ligne :
<http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19880106&numTexte=&pageDebut=00231&pageFin=>, (consulté le 12 mars 2011)

Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, J.O. n°66 du 19 mars 2003, en ligne :
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199>, (consulté le 08 juin 2011)

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O. n°143 du 22 Juin 2004, en ligne :
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=>, (consulté le 08 juin 2011)

Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, J.O. 10 juil. 2004, en ligne :
<http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399>, (consulté le 08 juin 2011)

Loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (J.O. 20 mai 2005)

Arrêtés, Rapports et autres textes

Arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique, J.O. 17 jan. 1982, p. 624, liste 1, p. 625. En ligne : <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19820117&numTexte=&pageDebut=50624&pageFin= >, (consulté le 12 mars 2011).

Circ. 17 janvier 1988 prise en application de la loi no 86-1067 du 30 septembre 1986, J.O. du 09 mars 1988.

Rapport ANDRÉ, Doc. AN, 1986-1987, n° 1087

Rapport ANDRÉ, Doc. AN, 1986-1987, 2e session ordinaire, n° 744

Rapport J. THYRAUD, Doc. Sénat, 1987-1988, 1re session, n° 3

Europe

La *Convention sur la cybercriminalité*, 23.XI.2001, Budapest, S.T.E n°185, en ligne : <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm>, (consulté le 11juin 2011).

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, art 2)c), en ligne : < http://www.conventions.coe.int/Treaty/FR/Treaties/Html/108.htm>, (consulté le 03 mars 2011.)

Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995, art 2)b), J.O. n° L 281 du 23.11.1995, p. 31–50, en ligne : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:NOT>, (consulte le 15 mai 2011)

TABLE DES JUGEMENTS

Jurisprudence canadienne

R. c. *Paiement*, [2003] J.Q. NO 4605 (C.Q.)

R. c. *Paré*, 1997 CarswellQue 651 (C.Q.) (WeC)

R. c. *Kealey,* [1996] 38 M.P.L.R. (2e éd.) 196 (C.A. Qué.)

R. c. *Toma* (2000), 147 C.C.C. (3d) 252(B-C. C.A.)

R. v. *Turner*, (1984), 13 C.C.C. (3d) 430(Ont. H.Ct.).

Re A.C.S. (1969), 7 C.R.N.S. 42 (C.S. Qué.)

R. c. *Worrell,* [1993] R.J.Q. 295, 304

R. c. *Zaltic*, [1993] 2 R.C.S. 29

Steward c. *Canada (Ministère de l'Emploi et de l'Immigration)*, [1988] 3 C.F. 487

Sansregret c. *La Reine,* [1985] 1 R.C.S. 570.

Jurisprudence américaine

Burleson v. *State*, 802 S.W. 2d 429 (Tex. App.—Fort Worth 1991)

People v. *Versaggi,* 608 N.Y.S. 2d 155(NY. Ct. App. 1994)

State v. *Corcoran,* 186 Wis.2d 616(Wis. Ct. App. 1994)

U.S. v. *Morris*, 928 F. 2d 504 (2d Cir.), cert. Denied, 502 U.S. 817 (1991)

Werner, Zaroff, Slotnick, Stern & Askenazy v. *Lewis,* 588 N.Y.S. 2d 960(N.Y.Civ. Ct. 1992)

Jurisprudence française

Douai, 7 oct. 1992, Gaz. Pal. 1993, p. 236, note Latry-Bonnart.

Paris, 18 nov. 1992, JCP E, 1994, I, étude n° 359, par. 15, p. 252, obs. Vivant et Le Stanc.

Trib. Corr. Limoges, 14 mars 1994, Expertises. 1994, p.238, obs. Teboul.

Crim. 5 janv. 1994, JCP E. 1994.I, étude n° 359, p. 252, par. 16, note Vivant et le Stanc.

Paris, 15 mars 1994, Expertises. 1994, n°178, p.441.

Paris, 15 mars 1995, JCP E 1995, étude n° 596, p. 184.

Paris, 5 avril 1994 : Juris-Data n° 021093, en ligne : <http://www.lexisnexis.com>, (consulté le 11 mai 2011)

Paris, 5 oct. 1994, JCP E 1995.I, étude n° 461, par. 21, obs. Vivant et Le Stanc.

Paris, 14 mars1994, JCP E 1995, étude n° 461, par. 21, p. 207.

Trib. corr. Limoges, 14 mars 1994, Expertises. 1994, p. 238, obs. Teboul.

Trib. corr. Brest, 14 mars 1995, LPA. 28 juin1995, n°77, p. 4, note Choisy.

Rouen, 17 mars 2005 : Juris-Data n°291578, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011)

TGI Paris, 26 juin 1995, LPA. Mars 1996, n°27, p.4, note Alvarez .

Rennes, 6 févr. 1996 : Juris-Data n°042141, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011)

Crim, 12 déc. 1996, *Bullt. Crim*., 1996, n° 465, p. 1353.

Nîmes, 24 sept. 1998, LPA. 15 août 2001, n° 162, p. 4, note Mas-Bellissent et al.

Crim., 10 déc. 1998, N° de pourvoi : 97-85867, en ligne: http://www.lexinter.net/JPTXT2/intrusion_dans_un_systeme_automatise_de_traitement.htm (Site consulté le 11 mars 2011.)

Toulouse, 21 janv. 1999 : Juris-Data n° 040054, en ligne : <http://www.lexisnexis.com>,(consulté le 8 mars 2011)\

Crim.14 avr. 1999, JCP G 1999, II, étude n° 10312.

Paris, 19 mai 1999, Gaz. Pal.18 avril 2000 n° 109, p. 51 note Tessalonikos.

Crim, 8 déc. 1999, *Bull. Crim*. 1999, n° 296, p. 917.

Paris, 15 décembre 1999 : Juris-Data n°106710 en ligne :

<http://www.lexisnexis.com>,(consulté le 8 mars 2011.)
TGI Paris, 25 fév. 2000, D. 2000, n° 18, p. 220, note Delpech.

Grenoble, 4 mai 2000 : Juris-Data n°122622, en ligne :
<http://www.lexisnexis.com>,(consulté le 8 mars 2011), p.3.

TGI Paris, 2 nov. 2000, Expertises. 2001, p.91, note X. Furst.

TGI Lyon, 20 fév. 2001, Gaz. Pal. 2001, p.1686, somm.3351, note Blanchot.

Paris, 15 mai 2001 : Juris-Data n°148055, en ligne :
<http://www.lexisnexis.com>,(consulté le 8 mars 2011)

Paris, 30 octobre 2002, Expertises 2003, n° 266, p. 36.

TGI Le Mans, 7 nov. 2003, Gaz. Pal. 20 juil. 2004, n°202, p. 44, note Barbry.

Aix-en-Provence, 22 sept. 2004 : Juris-Data n° 258368, en ligne :
<http://www.lexisnexis.com>,(consulté le 20 mars 2011)

TGI, Vannes, 13 juillet 2005 : Juris-Data n° 294765, en ligne :
<http://www.lexisnexis.com>,(consulté le 8 mars 2011)

Pau, 24 nov. 2005, LPA. 11 oct. 2006 n° 203, p. 16, note LASSERRE-CAPDEVILLE.

TGI Paris, 19 mai 2006, Gaz. Pal. 18 janv. 2007, n°18, p.35, note Forgeron et Fiévée.

Crim. 3 oct. 2007, *Bull.crim*., n° 236, p. 995.

TGI Quimper, 17 juill. 2008, en ligne :
< http://www.legalis.net/jurisprudence-decision.php3?id_article=2387> (consulté le 30 août 2009)

Paris, 13 oct. 2010 : Juris-Data n°021727, en ligne :
<http://www.lexisnexis.com>,(consulté le 8 mars 2011)

Paris, 18 nov. 2010 : Juris-data n°024404, en ligne :
<http://www.lexisnexis.com>,(consulté le 20 mars 2011)

Paris, 28 janv. 2010: Juris-Data n°001050, en ligne : <http://www.lexisnexis.com>, (consulté le 01 juin 2011).

Aix-en-Provence, 22 fév. 2011, Juris-data n°012158, en ligne :
<http://www.lexisnexis.com>, (consulté le 20 mai 2011).

TGI Bordeaux, 06 janv. 2011, legalis.net, 28 mars 2011, en ligne : <http://legalis.net/spip.php?page=jurisprudence-decision&id_article=3134> (Site consulté le 28 mars 2011.)

BIBLIOGRAPHIE

Monographie et ouvrages collectifs

CASILE, J.F., *Le code pénal à l'épreuve de la délinquance informatique*, PU D'AIX-Marseille, 2002

CATALA, P., *Le droit à l'épreuve du numérique – Jus ex machina*, PUF, 1998, p. 9.

CHAMPY, G., *La fraude informatique*, t.1, PU D'Aix-en-Provence, 1992, p.124

CORNU, G. (dir.), *Vocabulaire juridique*, Association Henry Capitant, PUF

CHAMPY, G., *la fraude informatique*, t. 2, PU D'Aix-en-Provence, 1992, p. 553

DAVIS, R.W.K. et S.C. HUTCHISON, *Computer Crime in Canada*, Carswell, 1997, p. 161

EL CHAER, N., *La criminalité informatique devant la justice pénale*, Beyrouth, Liban, Éditions Sader, 2004

FILIOL, É et RICHARD, P., *Cyber criminalité : enquête sur les mafias qui envahissent le web*, DUNOD, 2006, p. 187.

GRONDIN, R., *Les infractions contre la personne et contre les biens,* 6e éd., Wilson & Lafleur, 2007, par. 161, p.178

HOLLANDE, A. et X. L. DE BELLEFONDS, *Pratique du droit de l'informatique et de l'Internet : logiciels, systèmes, Internet*, 6e éd., Delmas, 2008, p. 353

LEMMENS, J.F., *Les PME et la sécurité : « vers une approche intégrale ? »*, Best Of Publishing – IDG Belgium, 2007.

MANN, J. F., *Computer Technology and the Law in Canada*, Carswell, Toronto, 1987, p.156

MARTIN, D., *La criminalité informatique*, Puf, 1997, p.23.

PARENT, H., *Traité de droit criminel. La culpabilité (*actus reus *et* mens rea*)*, t. 2, 2e éd., Éditions Thémis, 2005, par. 38, p. 24.

SCOTT, A. H., *Computer and Intellectual Property Crime: Federal and state Law*, 639-1300 (2001)

SOOKMAN, B.B., *Sookman computer, Internet, and electronic commerce law,* Toronto: Carswell, 1989

TAKACH, G. S., *Computer Law*, 2 éd., Irwin Law, 2003, p. 238

VIVANT, M., et ali., *Droit de l'informatique et des réseaux*, Lamy, 2007

Articles de revues et études d'ouvrages collectifs

ADAMS, J.A.-M., «Controlling cyberspace: Applying the computer fraud and abuse act to the internet», 12 *SANTA CLARA COMPUTER & HIGH TECH. L.J.* 403 (1996)

BELLOIR, P., « L'application des règles de procédure pénale aux infractions commises sur le réseau internet », Legalis.net. 2002. II, p.21.

BLANCHOT, A et POTTIER, I., « La violation des correspondances transmises par e-mail par une personne chargée d'une mission de service public », Gaz. Pal., 23 janv. 2001 n° 23, p. 18.

BOISVERT, A- M., «Communicatique et responsabilité pénale : criminalité informatique et «vol» d'information», dans BEAUCHARD, Jean et al., *Le droit de la communicatique*, Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal, Thémis, 1990, p. 93

BOURQUE, S., « Les moyens de défense », dans Collection de droit 2009-10, École du Barreau du Québec, Vol. 12, *Droit pénal Infractions, moyens de défense et peine*, Cowansville, Éditions Yvon Blais, 2009, p. 181 à 214

BUFFELAN, J.P., «La répression de la fraude informatique », Expertises. 1989, n° 103.

CHAMOUX, F., «La loi sur la fraude informatique : de nouvelles incriminations», J.C.P. 1988.I, étude n° 3321, par.10.

CROZE, H., «L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi no 88-19 du 5 janvier 1988 relative à la fraude informatique) », J.C.P. 1988.I, étude n°3333, par.7.

DELPECH, X., « Fraude à la carte bancaire : aspects juridiques », D. 2000, p.222

DEVÈZE, J., «Commentaire de la proposition de loi relative à la fraude informatique présentée par M. J. Godfrain le 5 août 1986 », D.I. 1987

«Chronique Droit pénal des affaires », JCP E. 1988.II, étude n°15122, p.125

FALVEY, J.J. et MCCALLEN, A.M., « General Legal Issues », 2 *INTER. L. and PRAC.* § 26:9(2009) (WeC) (Site consulté le 08 janvier 2010)

GASSIN, R., «La protection pénale d'une nouvelle «universalité de fait » en droit français : les systèmes de traitement automatisé de données», (Commentaire de la loi n 88-19 du 5 janvier 1988 relative à la fraude informatique), A.L.D. 1989

«Au sujet du délit d'atteinte volontaire aux données contenues dans un système de traitement automatisé de données (commentaire d'un arrêt de la chambre criminelle du 5 janvier 1994) », Lamy D.I.1996

GAUTRAIS, V., «Code criminel et utilisation d'internet », en ligne : < http : //www.gautrais.com/Code-criminel-et-utilisation-d> (consulté le 29 janvier 2011)

GEORGAS, M.S.,« Bill C-18 and Computer Abuse», 5 Advocates' Soc. J. No. 2, p.14-19, en ligne : <http://www.lexisnexis.com>, (consulté le 08 juin 2011)

GRIFFITH, D.S., «The Computer Fraud and Abuse Act of 1986: A Measured Respond to a Growing Problem», 43 *VAND. L. REV*. 456 (1990)

HÉBERT M. et PILON M., *Les délits informatiques*, Bibliothèque du parlement, service des recherches, 1991, p.4.

LE STANC C. et TRÉFIGNY P., « Droit du numérique », D. 19 juil. 2007, n° 28, p. 1998.

MARLOT-DEHAN, C., « Les évolutions du secret de la correspondance », R.D.P. 2005. II, p. 369.

PIRAGOFF, D.K., «Computer Crimes and Other Crimes against Information Technology in Canada», (1993) 64 *International Review of Penal Law* 20, 223

PRADEL, J., « La lecture d'un «Tatoo» n'est pas une écoute téléphonique», D.1999, p. 324

PRAT, V. et BRÉBAN Y., «Note sous Cour d'appel de Paris, douzième Chambre, section A, Ministère public, Société Tati », Gaz. Pal. 2003, no 205, p.23.

ROBERT, P., «La criminalisation des abus informatiques en droit pénal Canadien», dans Droit Contemporain, *rapports canadiens au Congrès international de droit comparé*, Montréal, Éditions Yvon Blais, 1990, p. 680

TOWER, J.A., «Hacking Vermont's Computer Crimes Statute », 25 *VT. L. REV.* 945 (2001)

WEBBER, C., « Recent Amendments to the Canadian Criminal Code Respecting Computer Abuses Offences », (1987) 3 Santa Clara Computer & High Technology L.J. 165, p. 171.

Études comprises dans les encyclopédies juridiques

BITAN, F., « Courrier électronique», *J.-Cl. Comm*., fasc. 4740, par. 62, en ligne : <http://www.lexisnexis.com>, (consulté le 08 mars 2011)

DEVÈZE, J., «Atteintes aux systèmes de traitement automatisé de données», *J.-Cl. Pén.*, fasc. unique n° 1et suiv. en ligne : <http://www.lexisnexis.com>, (consulté le 08 mars 2011)

PELTIER, V., «Atteintes au secret des correspondances commises par des particuliers», 2008, *J.-Cl. Pén.*, art. 226-15, par. 51. en ligne : <http://www.lexisnexis.com>, (consulté le 08 mars 2011)

Thèses et mémoires

VERGUCHT, P., *La répression des délits informatiques dans une perspective internationale*, thèse en droit, Université de Montpellier, 1996

Documents internationaux

Une nouvelle économie? Transformation du rôle de l'innovation et des technologies de l'information dans la croissance, OCDE, éd.2000, p.53

Perspectives des technologies de l'information de l'OCDE, éd. 2008

« La diffusion des TIC dans les entreprises : examens collectifs par pays », OCDE, en ligne :
<http://www.oecd.org/document/35/0,3343,fr_2649_33757_35223715_1_1_1_1,00.html> (consulté le 26 Novembre 2009)

«Perspectives des technologies de l'information de l'OCDE 2010, principales conclusions», OCDE, en ligne :
<http://www.oecd.org/dataoecd/4/9/46478073.pdf>, (consulté le 08 juin 2011), p. 7.

« Menaces informatiques et pratiques de sécurité en France », CLUSIF – 2010, en ligne : <https://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf>, (consulté le 11 juin 2011), p.16.

Bulletins, journaux et magasines

« Deux mois ferme pour la stagiaire chinoise de Valeo », TF1 NEWS, 18 décembre 2007, en ligne,
<http://lci.tf1.fr/france/justice/2007-12/deux-mois-ferme-pour-stagiaire-chinoise-valeo-4866420.html>, (consult**é** le 08 juin 2011)

« Des espions chinois dans les ordinateurs des géants du pétrole », La Tribune .fr, 28 janvier 2011, en ligne :
<http://www.latribune.fr/entreprises-finance/industrie/energie environnement/20110210trib000600289/des-espions-chinois-dans-les-ordinateurs-des-geants-du-petrole-.html>, (consulté le 08 juin 2011)

« Les réseaux informatiques d'Ottawa attaqués», en ligne :
<http://www.radio-canada.ca/nouvelles/National/2011/02/16/002-cyber-attaque-informatique-federal.shtml>, (consulté le 4 mars 2011)

« Comment Google a été attaqué depuis la Chine », Le Figaro. Fr, 24 février 2010, en ligne :
< http://www.lefigaro.fr/web/2010/01/13/01022-20100113ARTFIG00819-comment-google-a-ete-attaque-depuis-la-chine-.php>, (consulté le 08 juin 2011)

« Sony victime d'une nouvelle intrusion informatique », Le Monde.fr, 06, juin 2011, en ligne :<http://www.lemonde.fr/technologies/article/2011/06/06/sony-victime-d-une-nouvelle-intrusion-informatique_1532338_651865.html >, (consulté le 08 juin 2011)

Les dictionnaires

Larousse.fr, en ligne <http://www.larousse.com> (consulté le 2 mars 2011.)

Larousse.fr, Encyclopédie et dictionnaires Larousse, en ligne : <http://www.larousse.fr> (consulté le 30 août 2009)

Dictionnaire Le Petit Robert, Paris, 2006