Vol, fraude et autres infractions semblables et Internet

Sevgi Kelci

Lex Electronica, vol.12 n°1 (Printemps / Spring 2007)

http://www.lex-electronica.org/articles/v12-1/kelci.htm
http://www.lex-electronica.org/articles/v12-1/kelci.pdf

Introduction

L'explosion de l'utilisation des technologies de l'information et du commerce électronique a engendré une croissance significative des transactions en ligne[1]. La révolution technologique a également entraîné l'apparition de la cybercriminalité, plus spécifiquement d'infractions économiques telles que la fraude, le vol et l'escroquerie, dont l'ampleur est difficilement déterminable et quantifiable à cause de la difficulté d'obtenir des données empiriques démontrant la gravité du problème[2]. D'autant plus que les caractéristiques du cyberespace et l'Architecture du réseau ont favorisé la commission de ces infractions et empêché la détection des crimes.

---

1 La valeur des ventes en ligne au Canada était de 28.3M$ en 2004 alors qu'elle était de 5.7 M$ en 2000, ce qui constitue une croissance de 400% par rapport à l'an 2000 : Travaux publics et Services gouvernementaux Canada, « Commerce électronique, instaurer la confiance », novembre 2005, http://www.tpsgc.gc.ca/recgen/colloquium2005/presentations/group-1-peter-ferguson-f.html.

2 R. Grant HAMMOND, « Quantum Physics, Econometrics Models and Property Rights to Information », (1981), 27 *R.D. Mcgill* 47, 47-50.

La fraude[3], le vol et l'escroquerie seront étudiés en regard du droit pénal canadien. Nous n'aborderons pas les problèmes de juridiction pouvant apparaître dans le contexte de fraudes transfrontalières commises par exemple, par l'utilisation de cartes de crédit. Il est à noter que le simple lien de rattachement au Canada serait suffisant pour que le Canada ait juridiction en la matière[4]. Notre objectif consiste à faire reconnaître la difficulté réelle de sanctionner efficacement la fraude informatique. Nous supposons que la difficulté découle en premier lieu de la portée générale des infractions et en deuxième lieu de l'efficacité des procédés techniques d'escroqueries. Le libellé des infractions est trop large et non adapté à l'environnement en réseau et le *Code criminel* ne prévoit pas d'infraction spécifique sur l'usurpation d'identité. Dans cette perspective, nous sommes d'avis qu'il est urgent que le législateur se penche sur la problématique et qu'il établisse un cadre juridique pour la répréhension de l'usurpation d'identité.

En premier lieu, le présent article vise l'étude du cadre juridique de la fraude, du vol et de l'escroquerie. En deuxième lieu, les procédés techniques permettant de commettre l'escroquerie informatique, plus précisément l'usurpation d'identité, comme crime connexe à la fraude informatique, comme l'usurpation d'adresse IP, le hameçonnage, le pourriel et le programme malveillant seront ensuite examinés.

I. Cadre juridique de la fraude, du vol et de l'escroquerie, comme crime connexe à la fraude informatique, en droit pénal canadien

Les infractions de la fraude, du vol et de l'escroquerie seront respectivement examinées dans la présente section.

1. Le cas de la fraude

La fraude est spécifiquement incriminée à l'article 8 de la *Convention sur la cybercriminalité*. La définition traditionnelle de la fraude était le fait d'influer l'état d'esprit d'un individu de façon à l'amener à se départir d'un bien moyennant supercherie ou mensonge alors que celle du vol comportait un élément physique, soit le fait de subtiliser le bien d'un individu à son insu[5]. On faisait ainsi une distinction entre la fraude et le vol. Or, avec le développement des technologies de l'information et la sophistication des moyens de commission de crimes, ces définitions ont progressivement évolué avec le temps pour être délaissées entre les mains des juges qui n'ont pas hésité à procéder à l'activisme judiciaire.

À première vue, la définition de la fraude nous paraît simple mais elle est « non seulement mal circonscrite, mais elle offre aussi aux tribunaux la possibilité d'élargir le champ de la répression en créant de nouvelles infractions »[6]. Le *Code criminel* par le biais de son article 380 n'offre pas de réelle définition de la fraude. La disposition ne fait qu'énumérer les diverses modalités du

---

3 La fraude informatique est explicitement sanctionnée dans la *Convention sur la cybercriminalité* par le biais de son article 8.

4 R c *Libman*, [1985] 2 RCS 178.

5 *Re London & Globe Finance Co*., [1903] 1 Ch. 728, p. 732-733.

6 Anne-Marie BOISVERT, « La fraude criminelle : Sommes-nous allés trop loin? », (1995) 40 *Mcgill R.D.* 415, p. 485.

comportement frauduleux dont le mensonge, la supercherie ou autre moyen dolosif[7], par lesquels l'individu « frustre » la victime de quelque bien, service ou valeur. Ladite disposition ne comporte pas d'expressions précises permettant de définir la *mens rea* de l'infraction. L'arrêt *Théroux*[8] vient apporter quelques précisions sur cet élément de l'infraction dont nous aborderons un peu plus loin.

L'évolution jurisprudentielle de la définition de fraude est manifeste dans l'arrêt *Olan*[9]. Bien que le juge Dickson dans cette affaire reconnaisse la difficulté de circonscrire précisément le mot « frauder », il affirme que les deux éléments essentiels du crime qui devront être prouvés par le ministère public sont la « malhonnêteté » et la « privation ». Se contentant de définir la fraude comme une privation malhonnête, il ne fournit pas de paramètres fixes permettant d'identifier ce que signifie une privation malhonnête. Il n'a traité que des éléments matériels de l'infraction, soient la « privation malhonnête », il ne s'est véritablement pas penché sur la question de la « mens rea » de la fraude[10]. Comment faire pour délimiter la notion de malhonnêteté ? Le caractère à la fois subjectif et objectif de l'acte malhonnête n'a pas permis d'arrêter le débat sur un point précis. Est-ce seulement un acte qui est moralement répréhensible qui est sanctionné par ladite disposition ou bien celui qui « risque » de l'être, comme il ressort de l'arrêt *Olan*? Comment différencier le *mens rea* de la malhonnêteté ? Toutes ces questions ont semé de la confusion dans la définition de l'infraction de fraude.

L'auteur du crime peut recourir à divers moyens dolosifs pour causer une privation à la victime, notamment des « mensonges », « supercheries » ou « autres moyens dolosifs ». Lorsque l'inculpation est fondée sur un « autre moyen dolosif », il n'est pas nécessaire de faire un lien entre l'auteur de la fraude et la victime alors que si le moyen frauduleux provient d'une « supercherie » ou d'un « mensonge », un tel lien doit être fait. Dans l'arrêt *Olan*[11], le juge qualifie de « autres moyens dolosifs » les crimes qui ne sont ni des mensonges ni des supercheries mais qui englobent tous les autres moyens pouvant être qualifiés de malhonnêtes.

Les faits sont particulièrement complexes, il convient de les résumer[12]. Dans cette affaire, les accusés qui veulent faire l'acquisition de la compagnie cible, Langley, ont sollicité l'actionnaire majoritaire de cette compagnie pour négocier l'achat de toutes ses actions au coût de 1,025M$. Pour financer cette somme, ils ont eu recours aux services d'une banque. Bien que celle-ci accepta d'émettre un chèque tiré sur une compagnie de transit possédée par les accusés, Beauport Holdings, elle refusa de se départir du chèque puisque la valeur des actifs de Beauport Holdings était inférieure à 1,025M$. Sachant que la banque ne s'était pas départie du chèque, les accusés offrirent tout de même ce chèque certifié en paiement lors de l'achat de la compagnie cible.

Les accusés deviendront ensuite les actionnaires majoritaires de la compagnie cible et procédèrent à la liquidation de ses meilleurs actifs, notamment en lui faisant faire l'acquisition

---

7 L'interprétation donnée à l'expression « autre moyen dolosif » peut autant englober passiveté, réticence ou inaction. Le fait de taire que les obligations d'épargne étaient volées constitue un geste malhonnête. Donc, le silence peut également constituer un autre moyen dolosif : *Vézina* c. *La Reine*, [1986] 1 R.C.S. 2.

8 *R.* c. *Théroux*, [1993] 2 R.C.S. 5.

9 *R.* c. *Olan*, [1978] 2 R.C.S. 1175.

10 David H. DOHERTY, "The Mens Rea of Fraud", 25 Cr. *Law Q.* 348.

11 *R.* c. *Olan*, *supra* note 9.

12 Anne-Marie BOISVERT, *supra* note 6 à la page 421.

des actions d'une compagnie d'investissement qu'ils détiennent le contrôle, Beauport Financial. Étant donné que cette compagnie de finance disposait d'actifs suffisants, elle a pu consentir un prêt à la compagnie de transit qui, détenant également suffisamment de liquidités, la banque accepta de se départir du chèque certifié et le remit au vendeur de la compagnie cible, qui était anciennement l'actionnaire majoritaire de la compagnie cible. Ainsi, les accusés avaient mis sur pied ce stratagème pour financer la prise de contrôle de la compagnie cible à l'aide de ses propres actifs.

Les accusés ont affirmé qu'en aucun moment ils ont usé de supercherie ou de mensonge pour faire les transactions envers la compagnie cible et qu'aucun préjudice n'avait été causé à cette compagnie puisque les transactions n'avaient pas comme objectif de nuire à la santé financière de la compagnie cible[13]. Et ils ont indiqué que rien ne prouvait qu'ils n'avaient pas l'intention de rembourser les prêts consentis par la compagnie de finance à la compagnie de transit[14].

Le juge Sopinka est d'avis que, malgré des apparences de légitimité, ces opérations constituent un trompe-l'œil[15]. Le juge Dickson, en s'appuyant sur l'arrêt R. c. *Allsop*[16], a affirmé que la mise en péril des intérêts économiques de la victime était un élément suffisant pour établir l'élément de privation[17]. La compagnie cible, Langley, qui détenait initialement un portefeuille de valeurs sûres avait mis en péril ses propres biens en consentant un prêt à la compagnie de transit, Beauport Holdings, puisque cette dernière n'aurait pas pu effectuer l'emprunt si la compagnie cible n'avait pas risqué de détenir à la fin de la transaction des valeurs hautement spéculatives[18].

La Cour a considéré que les agissements des dirigeants de la compagnie de transit étaient des actes malhonnêtes. Ainsi, le juge Dickson s'appuie sur un arrêt anglais, *R.* c. *Sinclair*[19], pour conclure que le fait pour les administrateurs d'utiliser les biens d'une compagnie à des fins personnelles plutôt que dans l'intérêt de celle-ci peut constituer un acte malhonnête qui est visé par l'expression « autres moyens dolosifs »[20].

L'emprunt au droit anglais du concept de malhonnêteté serait erroné selon Mme Boisvert puisque des controverses existent toujours en Angleterre au sujet de la *mens rea* d'infractions de common law distinctes du crime de fraude en droit canadien et que cette référence ne permet pas définir l'actus reus de la fraude[21]. Selon elle, il faut éviter de recourir aux précédents anglais pour circonscrire les éléments matériels de la fraude lorsqu'elle est commise par « autre moyen dolosif », en faisant référence à l'état d'esprit de l'accusé à l'égard des conséquences de sa conduite[22]. Selon Mme Boisvert qui cite l'arrêt *Sinclair*, seuls les actes posés sans droit, en

---

13 Anne-Marie BOISVERT, *supra* note 6 à la page 422.

14 *ibid*.

15 *ibid*. à la page 459.

16 *R.* c. *Allsop* (1976) 64 Cr. App. R. 29 (C.A. Ang.).

17 Anne-Marie BOISVERT, *supra* note 6 à la page 423.

18 *ibid*.

19 (1968), 52 Crim. App. R. 618, [1968] 3 All. E.R. 241 (C.A.).

20 Anne-Marie BOISVERT, *supra* note 6 à la page 430.

21 *ibid*. En Angleterre, le concept de malhonnêteté s'applique à la mens rea de la fraude.

22 *ibid*.

violation avec un devoir ou sans autorisation lorsque requise peuvent constituer des moyens dolosifs[23].

La Cour s'est contenté de qualifier les agissements des dirigeants, n'a pas vraiment donné de précision sur les paramètres à utiliser sur la détermination d'actes malhonnêtes[24]. Il s'en est suivi l'élargissement de l'infraction de fraude. Or, comme il est indiqué dans l'arrêt *Bernard*, « il n'appartient pas aux tribunaux de créer de nouvelles infractions ni de donner plus d'extension à la responsabilité »[25]. Et la tâche de délimiter les contours est délaissée entre les mains des tribunaux canadiens.

Devant la confusion qui règne autour de cette notion, deux décisions, soient *Zlatic*[26] et *Théroux*[27], ont apporté quelques précisions sur les éléments matériels et la *mens rea* de l'infraction. Dans l'affaire *Zlatic*, l'accusé a acheté pour environ 375 000$ de marchandise auprès de trois fournisseurs qui ont livré ladite marchandise à ce dernier sans qu'il ne puisse les payer en raison de la perte au jeu de tout l'actif comprenant le produit de la vente des marchandises[28]. Il aurait ensuite fait faillite.

Le juge McLachlin fait référence au critère de la personne raisonnable pour déterminer si le moyen utilisé par l'accusé viserait cet autre moyen dolosif. Le fait d'accepter la livraison des marchandises sans pouvoir les payer pour ensuite spéculer au jeu la valeur qu'elles représentent, sachant qu'il s'agit d'une dépense « risquée » pouvant entraîner une privation à la victime et sa propre insolvabilité, serait hautement réprimé par une personne honnête ordinaire[29].

La majorité est d'avis que l'agissement de l'accusé constituerait cet « autre moyen dolosif » selon le critère de personne raisonnable. Ainsi, l'élément de privation de la fraude est évalué en termes de risques pris illégitimement avec le patrimoine d'autrui. La perception de l'accusé à l'égard du risque encouru ne peut à elle seule conduire à la fraude criminelle, en l'absence de moyens malhonnêtes causant une privation à la victime[30]. La même analogie s'applique aux procédés déloyaux lorsqu'une personne profite d'« une occasion d'affaires au détriment d'une personne moins astucieuse »[31]. En l'espèce, l'accusé est coupable de fraude en raison de son insouciance

---

23 *ibid*. à la page 459.

24 Anne-Marie BOISVERT, *supra* note 6 à la page 418.

25 *R*. c. *Bernard*, [1988] 2 R.C.S. 833 à la page 861

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

27 *R*. c. *Théroux*, *supra* note 8

28 Anne-Marie BOISVERT, *supra* note 6 à la page 425.

29 Comme le fait remarquer le juge McLachlin dans *Zlatic* : « À mon avis, la façon la plus raisonnable de percevoir les motifs du juge du procès consiste à conclure que, pour celui-ci, le fait d'accepter les marchandises sans se soucier de les payer, conjugué à la perte au jeu de la valeur qu'elles représentaient, constituait une conduite malhonnête [...]. La question est donc de savoir si la méthode exposée constitue un « autre moyen dolosif » au sens du troisième volet de l'infraction énoncée au par. 380(1) du *Code criminel*. À mon avis, c'est le cas » (Zlatic, ibid. aux pp. 43, 44).

30 Anne-Marie BOISVERT, *supra* note 6 à la page 425.

31 *R*. c. *Théroux*, *supra* note 8 ; Rachel GRONDIN, « Les infractions contre la personne et contre les biens », 5e éd., Montréal, Wilson & Lafleur ltée, 2003, p. 152

qui est appréciée ici avec un critère objectif[32]. Or, dans notre droit canadien, l'insouciance s'apprécie avec un critère subjectif, comme il est indiqué dans l'arrêt *Sansregret*[33].

De plus, selon ce raisonnement, l'individu qui est propriétaire de son argent, n'avait pas le droit de le dépenser comme il l'entend. Il en ressort la criminalisation de la façon de dépenser son argent et non la criminalisation de la fraude, comme l'indique le juge Sopinka dissident[34]. Qu'en serait-il si l'accusé avait dépensé cet argent dans une société à but non lucratif dont la mission est de venir en aide aux personnes handicapées ou aux enfants malades ? Selon le juge Sopinka, le fait de miner délibérément sa capacité de payer serait un acte malhonnête[35]. Cependant, le fait que les créanciers aient un « intérêt » à être payés ne leur confère aucun droit dans la « chose » de l'accusé qu'il a perdue au jeu[36]. Le seul droit qu'ils peuvent réclamer est la créance qu'ils détenaient à l'égard de l'accusé[37].

Bien que le critère de personne raisonnable nous permette de juger de l'honnêteté de la conduite de l'individu, elle n'est pas très précise, pouvant conduire à de l'arbitraire[38]. La définition de « conduite malhonnête » qui est donnée par Ewart –et repris par le juge McLachlin- et connue comme étant « ce qu'une personne honnête ordinaire jugerait indigne parce qu'elle est nettement incompatible avec les activités honnêtes ou honorables » ne permet pas de connaître à l'avance les conduites incriminées[39].

Selon Mme Boisvert cette norme communautaire n'étant pas suffisamment précise pour formuler une norme intelligible permettant aux simples citoyens de concevoir les conséquences de leur conduite enfreindrait les principes de justice fondamentale[40].

La fraude est un crime d'intention spécifique[41]. Chaque élément matériel de l'infraction doit se rattacher à chaque élément de l'infraction. Le ministère public doit ainsi prouver que l'accusé

---

32 Anne-Marie BOISVERT, *supra* note 6 à la page 477.

33 *ibid*. ; *Sansregret* c. *R*., [1985] 1 R.C.S. 570, à la page 582 : « 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. C'est dans ce sens qu'on emploie le terme « insouciance » en droit criminel et il est nettement distinct du concept de négligence en matière civile ».

34 *R*. c. *Zlatic*, note 26 à la page 34 : « Bien que nous ne soyons pas appelés à renverser une décision particulière, je crains qu'en l'espèce nous criminalisions le défaut de payer des dettes parce que nous désapprouvons la façon dont le débiteur a dépensé son argent ».

35 *ibid*. à la page 36.

36 Anne-Marie BOISVERT, *supra* note 6 à la page 452.

37 *ibid*.

38 *ibid*. à la page 428.

39 *R*. c. *Zlatic*, note 26 à la page 45 ; J.D. EWART, « Criminal Fraud », Toronto, Carswell, 1986 à la page 99.

40 Anne-Marie BOISVERT, *supra* note 6 à la page 442.

41 Rachel GRONDIN, *supra* note 31 aux pp. 147 à 152 ; Jacques GAGNÉ et Pierre RAINVILLE, « Les infractions contre la propriété : le vol, la fraude et certains crimes connexes », Cowansville, Éditions Yvon Blais inc, 1996, à la page 278 ; Anne-Marie BOISVERT, *supra* note 6 à la page 433.

avait subjectivement l'intention d'agir malhonnêtement pour que sa culpabilité soit établie[42]. Il s'agit de savoir si l'accusé était subjectivement conscient des conséquences de l'acte prohibé ou si il était insouciant quant aux conséquences possibles, et non s'il croyait que ses actes ou leurs conséquences étaient morales.

L'arrêt *Théroux* vient résumer les éléments constitutifs de l'infraction : 1) actus reus : a) acte prohibé, qu'il s'agisse de mensonge, supercherie ou autre moyen dolosif ; b) privation causée par cet acte prohibé, qui peut consister en une perte véritable ou dans le fait de mettre en péril les intérêts pécuniaires de la victime ; 2) mens rea : a) connaissance subjective de l'acte prohibé ; b) connaissance subjective que l'acte prohibé pourrait causer une privation à autrui[43]. La croyance de l'accusé que ses actes ou conséquences étaient moraux n'est pas prise en compte. Il n'est pas nécessaire de savoir si l'accusé saisit la malhonnêteté de ses actes, il suffit qu'il comprenne subjectivement que cette conduite peut entraîner une privation[44].

Le juge McLachlin a raison de mettre de côté l'évaluation personnelle que fait l'accusé de l'honnêteté de sa conduite puisque il s'en suivrait l'élargissement des moyens de défense qu'il pourrait invoquer[45]. Dans la mesure où la norme d'honnêteté devrait être uniforme, laisser l'accusé le loisir d'établir sa propre échelle de valeurs reviendrait à faire du *Code criminel* un régime auquel il est loisible de choisir d'adhérer ou non, selon l'auteur Rainville[46].

Après la confusion régnant dans l'arrêt *Olan* à l'égard de la définition de la fraude, les affaires *Zlatic* et *Théroux* viennent apporter des éclaircissements sur la *mens rea* de l'infraction[47]. Le débat est clôt à savoir si la fraude est un crime d'intention spécifique ou générale et l'évaluation personnelle de l'accusé sur l'honnêteté de sa conduite n'est plus pertinente[48]. Toutefois, la Cour suprême n'a pas fournit de paramètres précis sur la détermination des éléments matériels de l'infraction et le test objectif proposé par l'arrêt *Zlatic* est ambigu[49].

2. Le cas du vol

Le vol n'est pas directement visé par la *Convention sur la cybercriminalité*. Traditionnellement, l'existence ou non de consentement était le critère distinctif entre le vol et la fraude selon le document de travail de la Commission de réforme du Canada[50]. L'arrêt *Milne*[51] a démontré que

---

42 Il s'agit d'un test à la fois subjectif et objectif : subjectif en ce sens que l'accusé doit être subjectivement conscient que l'acte malhonnête peut causer une privation à la victime et objectif dans la mesure où l'évaluation personnelle de l'accusé sur la qualification de l'acte malhonnête n'est pas pris en compte. Anne-Marie BOISVERT, *supra* note 6 à la page 467.

43 *R.* c. *Théroux*, *supra* note 8 à la page 20.

44 Anne-Marie BOISVERT, *supra* note 6 à la page 469.

45 *ibid*. à la page 468.

46 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 211.

47 Anne-Marie BOISVERT, *supra* note 6 à la page 484.

48 *ibid*.

49 *ibid*. à la page 485.

50 Dans le cas du vol, l'individu s'approprie du bien sans le consentement de la victime alors que dans le cas de la fraude, l'individu amène la victime à consentir en recourant à la ruse pour pratiquer l'appropriation : COMMISSION DE RÉFORME DU DROIT DU CANADA, « Le vol et la fraude », *Document de travail 19*, Ottawa, Ministre des Approvisionnements et Services Canada, 1977 à la page 58.

51 *R.* c. *Milne*, [1992] 1 R.C.S. 697.

ce critère ne permettait pas de distinguer le vol de la fraude. Ainsi, celui qui s'approprie d'un bien remis par erreur peut se rendre coupable de vol même si la victime lui a remis le bien puisqu' aucun droit n'a été transféré au sens du droit criminel.

Le vol consiste en un détournement, à son propre usage ou à l'usage de quelqu'un d'autre, de biens animés ou inanimés de façon temporaire ou permanente. Le vol n'est consommé que lorsque la chose volée est déplacée ou devient amovible. L'infraction est définie à l'article 322 du C.cr. Le terme « détourne » renvoie au fait de s'emparer de l'objet avec l'intention de le détourner[52]. Ainsi, l'on peut se demander si l'acte du détournement se limite à un acte positif ou si il peut aussi englober une simple omission.

Dans l'affaire *Coté* c. *La Reine*[53], la Cour d'appel est d'avis que l'acte de détournement peut être réalisé autant par une omission que par un acte positif. L'appelant avait séjourné en Ontario en omettant de payer toutes les mensualités au concessionnaire après avoir loué une voiture auprès du créancier. La Cour a conclu que l'accusé avait l'intention de détourner la voiture et d'en priver son propriétaire[54].

Alors que dans l'arrêt *DeMarco*[55], la Cour écarte l'idée que l'accusé avait omis de rapporter le véhicule loué. L'accusé avait présenté une défense d'apparence de droit selon laquelle il croyait que le locateur ne s'objecterait pas à ce qu'elle conserve la voiture au-delà du temps alloué et qu'il avait l'intention de rembourser le créancier[56]. Il est évident que le départ temporaire de l'appelant ne peut constituer à lui seul un détournement d'une chose, sans aucune preuve démontrant l'intention de détourner l'objet, comme l'indique l'auteur Rainville[57]. Ou le fait de conserver un livre emprunté à la bibliothèque au-delà du temps alloué pour le prêt ne peut à lui seul référer au détournement d'une chose, mais il en serait différemment si l'emprunteur décidait de le passer à un tiers sans son autorisation.

L'individu qui obtient un transfert de propriété consenti par le cédant à la suite d'un oubli ou d'une erreur de sa part peut être reconnu coupable de vol si il connaissait l'erreur faite par le cédant et ce dernier jouira ainsi d'un droit de recouvrement, comme il est indiqué dans R. c. Milne[58]. Ainsi, si le caissier d'une banque remet erronément à un client un chèque d'un montant de 60$ au lieu de lui rendre 30$, ce dernier peut être condamné de vol si il était au courant de l'erreur commise par le caissier. Ainsi, en droit criminel canadien, c'est l'intention du receveur qui détermine l'existence ou non du vol[59].

L'objet du vol est défini de façon très large par la loi. L'expression « une chose quelconque animée ou inanimée » englobe tous les biens meubles ou immeubles amovibles, peu importe si la

---

52 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 22.

53 [1991] R.L. 110.

54 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 24.

55 (1974) 13 C.C.C. (2d) 369.

56 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 22.

57 R. c. *Ouellette*, [1998] A.Q. n° 1230 (C.A.) : le défaut par l'accusé de rapporter un véhicule loué dans le délai prévu dans le contrat de location ne constitue pas un vol en l'absence de l'élément de malhonnêteté.

58 *supra* note 51; Rachel GRONDIN, *supra* note 31 à la page 126.

59 *ibid*.

possession du bien est illégale[60]. Elle vise notamment un arbre déraciné, des animaux en captivité, un billet d'avion et une maison mobile[61]. La personne faisant l'objet du vol doit avoir « un droit de propriété spécial ou un intérêt spécial » dans la chose volée. La Commission de réforme du droit du Canada interprète cette expression conformément à la jurisprudence[62] de façon à inclure « quelque chose de moins que la propriété ou la possession, par exemple les privilèges, la garde ou mêmes les droits en équité »[63]. Par exemple, l'acheteur d'un bien en vertu du contrat de vente[64] ou le garagiste qui a un droit de rétention pour garantir le paiement des réparations possède un droit de propriété spéciale dans ce bien.

Le libellé de la disposition vise surtout les choses tangibles susceptibles d'être l'objet du vol. Or, dans l'arrêt *Scallen*[65], la Cour a conclu que l'expression « une chose quelconque » pouvait également être un crédit bancaire. Ainsi, les choses intangibles ne sont pas complètement exclues.

Qu'en est-il de l'information? L'information étant une chose intangible peut-elle faire l'objet d'un vol au sens de la disposition?

Dans l'affaire *Stewart*[66], il était question de savoir si les renseignements confidentiels pouvaient faire l'objet d'un vol au sens de ladite disposition? Dans cette affaire, M. Stewart avait offert de l'argent à un agent de sécurité à l'hôtel pour qu'il lui procure une liste des noms et adresses des employés de cet hôtel. Ce dernier n'était pas autorisé à consulter ces dossiers et il savait que ces renseignements étaient considérés comme confidentiels par la direction de l'hôtel. M. Stewart aurait conseillé à l'agent de sécurité de copier à la main l'information sans déplacer les dossiers. Ainsi, aucun objet tangible n'aurait été pris si le plan avait été exécuté.

Le juge Lamer a indiqué que « c'est en fonction du droit criminel que doit être tranchée la question de savoir si les renseignements confidentiels sont des biens aux fins du *Code criminel* »[67]. Selon lui, les renseignements confidentiels n'étant pas des biens en vertu du droit criminel, il n'y a pas eu de vol d'information. Il ressort de l'article 322 C.cr. que la « chose volée » doit être de nature à faire l'objet d'un droit de propriété « et elle doit être susceptible d'être prise ou détournée d'une manière qui occasionne une privation à la victime »[68]. Toujours selon le juge Lamer, pour viser l'expression « une chose quelconque », un bien doit pouvoir être pris ou détourné d'une manière qui entraîne une privation pour la victime. Or, les choses intangibles, comme elles n'ont d'existence matérielle que lorsqu'elles font corps avec un objet

---

60 R. c. *Grasser*, (1981) 64 C.C.C. (2d) 520 (C.S. N.-É., Div. App.).

61 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 25.

62 R. v. *Harry Smith* (1963) 1 C.C.C. 68 (C.A. Ont.) et R. v. *Hagen* (1969) 68 W.W.R. 348.

63 COMMISSION DE RÉFORME DU DROIT DU CANADA, « Le vol et la fraude », *Rapport n°12*, Ottawa, Ministre des Approvisionnements et Services Canada, 1979, à la page 74.

64 R. c. *Maroney*, [1975] 2 R.C.S. 306.

65 R. c. *Scallen*, (1974) 15 C.C.C. (2d) 441 (C.A.C.-B.).

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

67 R. c. *Stewart*, *supra* à la page 976.

68 *ibid*. à la page 974.

tangible, par exemple un document contenant des renseignements personnels ou une liste de clients[69], elles ne peuvent être prises.

Quant au détournement, les renseignements confidentiels ne sont pas susceptibles d'être détournés puisque n'entraînent pas de privation à la victime, comme l'indique le juge Lamer : « si l'on s'approprie des renseignements confidentiels sans s'emparer d'un objet matériel, par exemple en mémorisant ou en copiant les renseignements, le propriétaire ne se voit limité ni de l'usage ni de la propriété de ces renseignements, [il ne serait limité que du caractère confidentiel de ces renseignements] »[70].

Le même argument s'applique pour le chef d'incitation à la fraude. Par conséquent, les renseignements confidentiels n'étant susceptibles d'être pris ou détournés, l'information ne pouvait faire l'objet d'un vol au sens de l'article 322 C.cr[71]. Ainsi, le vol des idées ou de l'information n'est pas une infraction prévue au *Code criminel*.

En résumé, la mémorisation d'un document contenant des renseignements personnels ne serait pas incriminée mais la subtilisation du document le serait. Il est vrai qu'il y a absence de privation dans le premier cas pour la victime qui ne se voit privée que de la confidentialité des renseignements[72].

Qu'arriverait-il si le détenteur de cette information se souviendrait du contenu des documents après la disparition du document subtilisé? Si le critère utilisé est le préjudice causé à la victime, peut-on parler d'un réel préjudice si ce dernier se souvient de la teneur des informations? Ainsi quelle serait la différence entre la subtilisation d'un document ou sa reproduction ou sa mémorisation sur le plan de préjudice que ressent la victime?

Il est vrai que la condamnation de Desroches était évidente, cependant, selon les critères retenus par les affaires *Stewart* et *Desroches*, celui qui ne fait que mémoriser le contenu du document resterait impuni alors que sa conduite est aussi répréhensible que celui qui subtilise le document. L'auteur Rainville[73] suggère de privilégier une inculpation de fraude avec l'ajout de l'article 342.1 C.cr. contre l'appropriation illicite de renseignements personnels dans le contexte de données informatiques[74].

L'analyse jurisprudentielle de l'actus reus de l'infraction de vol nous porte à conclure que des problèmes y logent[75]. L'interprétation de la *mens rea* de l'infraction nous mène à des difficultés semblables.

---

69 Par exemple, dans l'affaire R. c. *Desroches*, (1992) 16 C.R. (4th) 182 (C.A. Qué), l'accusé a été reconnu coupable de vol de document de son employeur. Il avait subtilisé la liste de clients et de documents décrivant des procédés techniques de très grande valeur. Il s'agit du vol d'objets tangibles, visé par l'article 322 C.cr.

70 R. c. *Stewart*, *supra* à la page 964.

71 *ibid*. à la page 979.

72 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 52.

73 *ibid*. à la page 53.

74 Dans cette perspective, l'infraction relative à l'accès illégal de la *Convention sur la cybercriminalité* peut recevoir application.

75 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 54.

L'élément mental du crime se rapporte à l'intention spécifique de priver de façon permanente ou temporaire la victime du bien. La disposition indique que la chose doit être prise ou détournée « frauduleusement » et « sans apparence de droit » pour constituer une infraction de vol. Ainsi, la personne doit avoir pris ou détourné la chose « sans apparence de droit » et avec une intention malhonnête, c'est-à-dire avec un état d'esprit qui dépasse la simple connaissance.

Les tribunaux ont eu beaucoup de difficulté à définir l'expression « frauduleusement » comme un élément distinct de la notion « d'apparence de droit »[76]. Selon l'auteur Rainville, l'interprétation restrictive de cette notion a amené une confusion entre ces deux notions alors qu'une interprétation libérale de cet élément mental y a substitué la notion de « malhonnêteté », en introduisant la notion de « turpitude morale » sans la définir[77]. L'auteur propose de définir le mot « frauduleusement » tout en lui donnant une connotation de turpitude morale. Ainsi, cet élément mental exigerait la conscience par l'accusé de risquer de nuire aux intérêts patrimoniaux de la victime[78]. Celui qui prend délibérément un bien appartenant à autrui, sachant qu'il n'a aucun droit sur ce bien et sachant qu'il risque de porter atteinte aux intérêts patrimoniaux de la victime dénote une turpitude morale. Le seul fait de s'emparer du bien sans le consentement de la victime et sans apparence de droit ne peut se rapporter à l'infraction de vol, sans un état d'esprit blâmable, comme l'indique la Commission de réforme du droit du Canada[79]. Cette définition de turpitude morale éviterait alors l'évaluation personnelle de la malhonnêteté par les jurys et servirait d'ailleurs de fondement à la défense de plaisanterie[80].

L'analyse de la notion « d'apparence de droit » représente un défi analogue à celui existant pour le mot « frauduleusement »[81]. L'erreur de droit peut-elle donner une ouverture à un moyen de défense ? Il existe deux tendances jurisprudentielles en la matière : l'école restrictive[82] qui y répond par la négative et l'école libérale[83] qui interprète ces mots de façon à inclure autant une erreur de droit qu'une erreur de fait.

L'auteur Rainville est d'avis qu'une défense fondée sur une erreur de droit peut être accueillie, à la condition de remplir les critères s'y rattachant[84] : en premier lieu, l'accusé doit entretenir une croyance erronée de droit ou de fait, laquelle doit être sincère et de bonne foi[85] ; en deuxième

---

76 *ibid*. à la page 62.

77 *ibid*. à la page 62. Le vrai danger n'est pas d'introduire la notion de turpitude morale mais de s'abstenir de définition cette notion ambiguë : *R.* c. *Théroux*, *supra* note 8 aux pp. 22-23.

78 *ibid*. à la page 62.

79 COMMISSION DE RÉFORME DU DROIT DU CANADA, « Pour une nouvelle codification du droit pénal », *Rapport n°31*, Ottawa, Ministre des Approvisionnements et Services Canada, 1987 à la page 89.

80 R. c. *Smith*, (1989) 231 A.P.R. 280.

81 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 91.

82 R. c. *Shymkowich*, [1954] R.C.S. 606: La croyance que, par la loi générale du pays, l'accusé peut s'emparer des billots de bois, constitue une erreur de droit qui ne peut être accueillie.

83 R. c. *Howson*, [1966] 3 C.C.C. 348, 47 C.R. 322 (C.A. Ont.) aussi *R*. v. *Hemmerly* (1977) 30 C.C.C. (2e) 141 (C.A. Ont.).

84 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 78. D'ailleurs, la Commission de réforme du droit du Canada est du même avis : « l'expression s'interprète « tantôt de manière à inclure l'erreur de fait commise de bonne foi ou l'erreur de droit commise de bonne foi, tantôt comme étant restreinte à l'erreur de bonne foi portant sur une question de droit privé » : COMMISSION DE RÉFORME DU DROIT DU CANADA, supra note 69 à la page 28.

85 *R*. c. *Shymkowich*, *supra* note 82.

lieu, cette croyance doit justifier que l'accusé détient un droit légal, par opposition à un droit moral, à s'emparer d'une chose ou à la détourner et enfin, l'erreur de l'accusé doit être une de droit privé. Bien que cette proposition semble intéressante, la jurisprudence ne semble pas s'enligner sur une même voie.

En somme, l'analyse de l'actus reus et de la mens rea des infractions de fraude et du vol conduit à de l'imprécision qui persiste dans le cas de l'escroquerie.

3. Le cas de l'escroquerie (une infraction plus tatillonne)

Le présent travail examinera l'escroquerie comme crime connexe au vol et à la fraude commis sur Internet. La présente section analysera l'escroquerie en faisant des liens avec le vol et la fraude, étant donné le caractère économique de ces trois crimes. L'infraction plus générale de la fraude informatique se présentant dans la *Convention sur la cybercriminalité* couvre l'escroquerie qui est incriminée à l'article 362(1) du C.cr. Bien qu'elle comporte des ressemblances frappantes avec la fraude, elle a ses caractéristiques propres[86]. La portée de cette infraction est beaucoup plus restreinte que celle de la fraude[87]. Chaque alinéa de l'infraction d'escroquerie comporte une infraction distincte et autonome[88] alors que l'infraction de fraude réprime l'ensemble des moyens dolosifs.

Les alinéas a) et b) couvrent deux infractions de faux-semblant : 1) l'obtention d'une chose par faux semblant et 2) l'obtention de crédit par faux-semblant[89]. Et les derniers alinéas se rapportent à l'obtention effective ou souhaitée d'un avantage au moyen de faux-semblant, de fausse déclaration écrite ou par un chèque sans provision[90]. L'infraction vise à faire réprimer la malhonnêteté pouvant s'inscrire entre les rapports humains. L'accomplissement d'une escroquerie présuppose l'existence d'un leurre alors que l'infraction de fraude qui pénalise l'ensemble de moyens dolosifs ne l'exige pas[91]. Ainsi, la chose ou les services doivent être obtenus à la suite d'une duperie alors que dans le cas de la fraude, il n'est pas nécessaire que l'accusé ait dupé un tiers, il suffit qu'il ait délibérément commis un acte malhonnête pouvant entraîner un préjudice patrimonial à la victime[92]. Les alinéas a) et b) prévoient que l'escroquerie doit porter sur une chose susceptible d'être volée. Ainsi, les renseignements confidentiels, les immeubles et l'obtention d'un délai de paiement ne font pas partie des choses pouvant faire l'objet de vol[93]. De plus, la victime doit avoir obtenu la chose au moyen de faux semblant. Suffit-il qu'elle ait acquis la possession du bien ou doit-elle avoir un droit réel ou un droit de propriété sur la chose ? La simple lecture de l'alinéa b) nous indique que le terme « obtient » ne signifie pas nécessairement le transfert d'un droit réel ou voire d'un droit de propriété puisque celui qui

---

86 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 394.

87 Pierre RAINVILLE, *supra* note 41 à la page 397.

88 *Abbas* c. *La Reine*, [1984] 2 R.C.S. 526, 534.

89 Rachel GRONDIN, *supra* note 31 à la page 154.

90 *ibid*. La présomption d'intention frauduleuse ressortant de la présentation d'un chèque sans provision a été déclarée inconstitutionnelle, l'article 362(2) C.cr. étant contraire à l'article 11d) de la Charte canadienne. Ainsi, la personne qui remet un chèque sans provision sera acquittée si elle croyait approvisionner le compte en temps utile, même en l'absence de motifs raisonnables.

91 Pierre RAINVILLE, *supra* note 41 à la page 397.

92 *ibid*. Par exemple, l'individu qui reproduit des cassettes videos et les écoule sur le commerce commet une fraude.

93 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 402.

acquiert un bien par crédit n'est pas le propriétaire du crédit et ne détient pas plus de droit réel sur ce crédit[94].

Par conséquent, celui qui obtient la possession à la suite d'une supercherie peut être condamnée soit pour fraude, soit pour vol ou soit pour escroquerie[95]. Même si ces trois infractions peuvent s'appliquer à cette situation, il faut faire ressortir les subtilités s'y rattachant : les alinéas a), c) et d) de l'article 362 du C.cr. visent uniquement les cas de supercherie alors que le vol et la fraude peuvent être commis en l'absence de toute supercherie[96]. Il est possible que la fraude et le vol soient perpétrés en l'absence et à l'insu de la victime tandis que l'escroquerie nécessite l'existence de liens avec la victime[97].

Il y a controverse à savoir si la création d'un risque de préjudice dans le patrimoine de la victime est nécessaire relativement à l'infraction de l'escroquerie[98]. Même si l'alinéa c)[99] tranche la question en affirmant par la négative, il en est tout autrement pour les alinéas a) et b) de la disposition. La simple lecture de ces alinéas ne semble pas exiger un quelconque préjudice patrimonial, se contentant d'indiquer l'obtention par l'accusé d'un avantage escompté. Celui qui se procure de la drogue à la pharmacie en empruntant l'identité d'un tiers serait condamné sous l'article 321(1)a)C.cr., même si le pharmacien n'a subit aucun préjudice. Le débat n'étant pas clos, il y a l'autre thèse voulant que l'existence d'un préjudice pécuniaire soit préférable[100]. Ainsi, dans l'affaire *MacDonald*, étant donné que la valeur des cigarettes demandée par l'inculpé était moindre que le prix offert sur le marché, l'accusé a été acquitté, même si il a menti à la victime sur la marque de cigarette, considérant l'inexistence de risque de préjudice pécuniaire[101].

Le même débat s'enclenche relativement à la *mens rea* de l'infraction. L'accusé doit avoir connaissance des éléments matériels énoncés aux alinéas de la disposition. L'incertitude entourant l'élément matériel relativement au risque de préjudice pécuniaire se transpose dans la *mens rea* de l'infraction : l'accusé doit-il avoir l'intention de causer un risque de préjudice dans le patrimoine de la victime ?

En conclusion, l'analyse des éléments matériels des infractions de fraude, du vol et de l'escroquerie soulève des difficultés de circonscrire clairement les contours de l'actus reus de ces infractions.

---

94 Rachel GRONDIN, *supra* note 31 à la page 154.

95 Elles ne sont pas interchangeables à cause du principe de l'interdiction de condamnations multiples : *Kineapple* c. *R.*, [1975] 1 R.C.S. 729.

96 Jacques GAGNÉ et Pierre RAINVILLE, *supra* note 41 à la page 397.

97 *ibid*.

98 *ibid*. à la page 409. Dans le cas de la fraude, le comportement malhonnête doit nécessairement créer un risque de préjudice sur le patrimoine de la victime alors que dans le cas de l'escroquerie, il suffit que l'accusé ait obtenu l'avantage souhaité, le risque de préjudice n'étant pas nécessaire. Ainsi, l'arrêt *Olan* serait inapplicable en l'espèce.

99 *ibid*. L'alinéa c) incrimine la tentative d'escroquerie.

100 *R.* c. *MacDonald*, (1946) 3 C.R. 259 (C. sup. N.-É.).

101 *ibid*.

II. Escroquerie informatique, crime connexe à la fraude informatique

Comme mentionné plus haut, le crime de l'escroquerie comporte des liens de parenté manifestes avec le vol et la fraude. Ces trois infractions visent l'utilisation de moyens frauduleux en vue de soutirer un avantage économique à la victime. L'escroquerie s'applique aux cas de supercherie tandis que la fraude couvre l'ensemble de moyens dolosifs. L'infraction de vol nécessite l'existence d'une chose susceptible d'être volée, tout comme l'escroquerie.

L'escroquerie peut également être commis sur le réseau Internet[102] aux moyens de procédés techniques servant à tromper la victime afin de lui soutirer un quelconque intérêt pécuniaire. L'escroquerie informatique se rapporte à l'idée d'une certaine sollicitation auprès de celle-ci dont le consentement lui sera arraché alors que dans le cas de la fraude informatique, les manipulations illicites à l'égard du système informatique aux moyens de dispositifs suffisent pour commettre le crime[103]. Dans cette perspective, bien que l'escroquerie informatique constitue un crime économique comme la fraude informatique, cette dernière a une portée beaucoup plus large, englobant toutes formes de manipulations de données informatiques.

L'escroquerie informatique peut être effectuée aux moyens de procédés techniques visant à usurper l'identité d'une personne, notamment l'usurpation d'adresse IP, le hameçonnage, l'envoi de pourriel, la prolifération de réseau de zombie, l'utilisation de logiciels malveillants, etc. La présente section étudiera les divers moyens dolosifs utilisés par le criminel pour commettre le crime plus spécifique de l'usurpation d'identité compris dans le crime plus général d'escroquerie informatique, comme crime connexe à la fraude informatique.

Ce crime peut être commis aux moyens d'outils technologiques visant à usurper délibérément l'identité d'une personne afin de commettre d'autres crimes économiques, tels la fraude sur les cartes de paiement[104]. Pour commettre ce délit informatique, l'usurpateur d'identité tente d'obtenir les renseignements personnels et financiers d'une personne dont le nom, l'adresse, le numéro d'assurance sociale, les numéros des cartes de crédit, dans l'intention d'accéder aux comptes de banque de la victime et y effectuer des opérations frauduleuses, comme par exemple, retirer de l'argent dans le compte de la victime pour faire l'achat de biens et services sur le réseau Internet.

Le vol d'identité qui est une forme d'escroquerie informatique ne fait pas l'objet d'une définition législative dans le *Code criminel*[105]. Même si les infractions portant sur la supposition de personne, la contrefaçon et la fraude fournissent une certaine aide pour sanctionner en partie cette forme d'escroquerie, ces infractions restent inefficaces lorsque prises isolément[106].

---

102 « J'avais lu beaucoup d'histoires, mais je ne croyais jamais que cela pourrait m'arriver…Hou la ! Cela peut vraiment arriver. N'importe qui pourrait se faire passer pour vous ». Ottawa Citizen, octobre 2005, victime d'une fraude d'identité : Gendarmerie Royale du Canada, *Protection des renseignements personnels et protection contre l'escroquerie-Guide pratique de l'étudiant*, p. 1, 1er mars 2006, http://www.rcmp-grc.gc.ca/scams/student_guide_f.pdf.

103 Rachel GRONDIN, *supra* note 31 à la page 156.

104 *ibid*.

105 L'ASSOCIATION DES BANQUIERS CANADIENS, *L'usurpation d'identité : la nécessité d'une politique en matière de prévention*, p. 2, http://www.cba.ca/fr/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20FRE.pdf.

106 *ibid*.

Divers acteurs dont l'association des banques du Canada[107] travaillent avec les forces policières et les gouvernements fédéraux et provinciaux sur l'élaboration d'une politique stratégique visant à mettre en œuvre des mesures préventives en matière d'usurpation d'identité et font pression sur le gouvernement canadien pour l'inclusion dans le droit pénal canadien d'une nouvelle infraction visant spécifiquement la répression du vol d'identité puisqu'ils sont conscients des risques que ce délit représente sur le développement du commerce électronique. Outre les répercussions économiques qu'il entraîne sur les institutions financières, les entreprises et les consommateurs[108], une perte de confiance dans les entreprises par les consommateurs peut également s'ensuivre en l'absence de tout contrôle législatif effectif sur ce délit informatique.

1. *IP spoofing* (usurpation d'adresse IP)

L'usurpation d'adresse IP constitue l'un des moyens utilisés par des criminels pour obtenir l'accès à des renseignements personnels de la victime à son insu en vue d'une utilisation délictueuse de ces informations. L'IP spoofing « consiste en une technique de hacking consistant à utiliser l'adresse IP afin d'usurper l'identité d'une personne »[109]. L'adresse IP qui est composée de 4 octets, allant de 0 à 255 et séparés par des points, sert à identifier de façon unique les périphériques du réseau dont l'ordinateur, l'imprimante, le lecteur de CD-ROM[110]. L'unicité des identificateurs du réseau IP est garantie lorsque le centre InterNIC attribue à chaque réseau connecté sur un réseau Internet public un identificateur du réseau officiel[111]. L'administrateur du réseau attribue ensuite un identificateur d'hôte unique à chacun des ordinateurs connectés au réseau local[112]. Une adresse IP peut être convertie sous un nom de domaines, une forme qui est plus accessible aux internautes[113].

Cette technique consiste à modifier l'en-tête de chaque paquet IP pour contenir une adresse IP différente de l'adresse IP source appartenant à une personne autre que l'usurpateur, pour ainsi créer plusieurs paquets IP[114]. Elle permet d'attaquer des réseaux en volant l'identité de quelqu'un d'autre[115]. L'usurpateur cible les services qui sont basés sur une relation de confiance dont la rsh pour accéder à l'adresse IP autorisée et se connecter à un serveur[116]. L'internaute qui utiliserait des services fondés sur la cryptographie (ssh) ou une authentification par mot de passe (rsa) serait

---

107 L'ASSOCIATION DES BANQUIERS CANADIENS, Fraude et sécurité, *Usurpation d'identité*, http://www.cba.ca/fr/section.asp?fl=4&sl=268&tl=276&docid=/.

108 PhoneBusters a indiqué que les pertes signalées par les victimes de vol d'identité s'élevaient à 21,8 millions de dollars pour l'année 2003 : Gouvernement du Canada, Service canadien de renseignements criminels, « Criminalité financière Vol d'identité » octobre 2005, http://www.cisc.gc.ca/annual_reports/annualreport2005/identity_theft_2005_f.htm

109 Wikipédia L'encyclopédie libre, *IP spoofing*, 11 janvier 2006, http://fr.wikipedia.org/wiki/IP_spoofing

110 Dicofr.com, Adresse IP, http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101000012.

111 *ibid*.

112 *ibid*.

113 De plus, « il existe deux types d'adresse IP : le format IPv4 (la version 4, historique, mais qui est encore très largement utilisée) et IPv6 (la version 6, récente et en cours de déploiement, qui doit remplacer à terme la version 4) ».Wikipédia L'encyclopédie libre, *Adresse IP*, 11 janvier 2006, http://fr.wikipedia.org/wiki/Adresse_IP.

114 Wikipédia L'encyclopédie libre, *Adresse IP*, 11 janvier 2006, http://fr.wikipedia.org/wiki/Adresse_IP.

115 *ibid*.

116 *ibid*.

moins exposé à ces attaques puisque ces services sont difficilement accessibles aux usurpateurs[117].

Dans cette perspective, l'usurpateur obtiendrait l'accès aux renseignements personnels de la victime pour commettre l'escroquerie informatique, par exemple en utilisant les données de sa carte de crédit pour faire des achats électroniques. Considérant que l'adresse IP sert à identifier une personne, le rôle du droit pénal serait d'interdire la possession et l'utilisation de multiples adresses IP par la même personne ainsi que la fabrication de nouvelles[118]. L'adoption d'une infraction en ce sens dissuaderait les criminels à utiliser une adresse IP différente de la sienne.

2. *Phishing* ou le hameçonnage

Le hameçonnage est une forme d'escroquerie basée sur l'usurpation d'identité. Il consiste en l'envoi massif de courriel non sollicité et trompeurs usurpant l'identité d'une institution financière ou d'un site commercial légitime, dans lequel les destinataires sont invités, sous de faux prétextes –tels qu'une panne du système informatique, une nouvelle législation, une modification des conditions d'utilisation, une actualisation des fichiers, une augmentation du niveau de sécurité, etc.–, à se rendre sur un faux site Web mais s'apparentant comme le site de l'institution financière pour qu'ils divulguent leurs coordonnées bancaires ou personnelles, dans l'intention de les utiliser pour commettre de l'escroquerie informatique[119]. Les clients des institutions financières sont directement touchés par le hameçonnage. Si aucun mécanisme de répression n'est prévu dans le droit pénal canadien, les usurpateurs continueront d'utiliser cette manœuvre dolosive et les institutions financières subiront non seulement des pertes financières mais perdront tout autant la confiance de leurs clients, ce qui est une conséquence qui est encore plus dévastatrice du point de vue financier.

L'Association des banquiers canadiens est d'avis que la répression de l'usurpation d'identité doit se faire par l'établissement de mesures préventives permettant d'assurer l'intégrité et l'authenticité des pièces d'identité[120]. Dans cette perspective, les institutions financières doivent demander le soutient du gouvernement fédéral et provincial pour procéder à la vérification des pièces d'identité émises par le gouvernement[121]. Une fois la vérification faite de l'identité des clients, la mise en place d'une infraction interdisant la possession de plusieurs pièces d'identité dissuaderait les criminels à commettre le hameçonnage. Le Groupe de travail anti-pourriel émet des recommandations en ce sens. Il suggère l'adoption d'une loi anti-pourriel visant à interdire plusieurs activités, notamment l'utilisation d'en-têtes ou de lignes de mention faux destinés à tromper le destinataire ou de contourner les filtres techniques et la construction d'adresses URL et de sites Web trompeurs dans le but de recueillir des renseignements personnels par

---

117 *ibid.*

118 L'ASSOCIATION DES BANQUIERS CANADIENS, *L'usurpation d'identité : la nécessité d'une politique en matière de prévention*, p. 2, http://www.cba.ca/fr/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20FRE.pdf.

119 Office québécois de la langue française, Bibliothèque virtuelle, *Vocabulaire d'Internet*, 1er mars 2006, http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/8869710.html.

120 L'ASSOCIATION DES BANQUIERS CANADIENS, *L'usurpation d'identité : la nécessité d'une politique en matière de prévention*, p. 3, http://www.cba.ca/fr/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20FRE.pdf.

121 *ibid.*

escroquerie[122]. En outre, l'insertion d'une signature électronique par l'institution financière dans le courriel envoyé au client permettrait d'authentifier que le courriel provient effectivement de celle-ci. Les dossiers doivent ensuite être conservés dans une base de données fiable et accessible à une entité digne de confiance[123]. Une campagne d'éducation doit également être effectuée auprès des consommateurs pour les sensibiliser à la menace que représente l'usurpation d'identité et à la nécessité de protéger leurs renseignements personnels.

3. Pourriel

Le pourriel est définit comme étant l'envoi massif et répété de « messages électroniques commerciaux non sollicités »[124]. Le problème lié au pourriel ne constitue plus un ennui mineur entraînant une perte de temps aux utilisateurs, il constitue un problème réel servant de moyen pour exercer des activités illicites sur le réseau Internet, notamment l'usurpation d'identité, le vol de renseignements personnels, la destruction des données informatiques, etc. En effet, il est démontré que la menace posée par le pourriel accroît à mesure que le nombre de pourriels augmente[125]. Même si les mesures de protection adoptées par les FSI ont contribué à diminuer le nombre de pourriels, la tendance à la hausse a persisté à cause de l'apparition d'autres formes de menaces liées à la sécurité d'Internet, telles que les logiciels espions, les virus, l'hameçonnage et les réseaux d'ordinateurs zombies[126]. Le pourriel est ainsi un moyen d'escroquerie informatique. Selon le Groupe de travail, « le pourriel menace directement la viabilité d'Internet comme moyen efficace de communication [et] la prospérité économique, à l'efficience des services publics au développement d'une cyberéconomie »[127].

Le Groupe d'experts émet une série de recommandations qui favorise une stratégie globale de lutte contre le pourriel[128]. Il propose entre autres l'adoption de lois et règlements spécifiques visant à interdire le pourriel et suggère de prévoir des infractions au titre d'une loi anti-pourriel spécifique pour les pratiques de multipostage abusif énumérées, telles que le défaut de se conformer à des procédures d'inclusion pour l'envoi de courriels non sollicités et la collecte, l'utilisation ou l'acquisition d'adresses de courriel sans consentement[129].

Nous nous enlignons sur cette recommandation puisque le fait de prévoir des infractions et sanctions sur le plan pénal dissuaderait effectivement les criminels à commettre l'usurpation d'identité. Cependant, l'approche étant une démarche globale de lutte contre l'usurpation d'identité, le pourriel et autres moyens d'escroquerie informatique, la sensibilisation et

---

122 Industrie Canada, Freinons le pourriel Créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel*, mai 2005, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317f.html.

123 *ibid*.

124 Industrie Canada, Freinons le pourriel Créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel*, mai 2005, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317f.html.

125 À la fin de l'année 2004, le pourriel représentait 80% du courriel global alors qu'en 2002, il en représentait 30% : *ibid*.

126 MessageLabs a fait rapport de 18 millions de courriels hameçons en 2004. L'étude *Online Safety Study* d'AOL®—National Cyber Security Alliance, publiée en octobre 2004, rapporte que 80 p. 100 des utilisateurs américains ont des logiciels espions ou publicitaires sur leurs ordinateurs et que 89 p. 100 d'entre eux en ignorent la présence : *ibid*.

127 *ibid*.

128 Industrie Canada, Freinons le pourriel Créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel*, mai 2005, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317f.html.

129 *ibid*.

l'éducation des utilisateurs sont toutes autant essentielles. Ainsi, le gouvernement fédéral et les intervenants doivent accroître une campagne de sensibilisation efficace auprès des utilisateurs en faisant circuler de l'information par l'intermédiaire de plusieurs médias, en maintenant à jour les informations pertinentes.

En somme, il est temps que le législateur pénal réagisse face aux problèmes toujours persistants de pourriels, tout comme d'ailleurs l'usurpation d'adresse IP.

4. Programme malveillant (*Malware*)

Un programme malveillant est un ensemble de programmes destiné à perturber, altérer ou détruire un système informatique à l'insu de l'utilisateur[130]. Ces logiciels constituent un moyen d'accès aux renseignements personnels des utilisateurs, donc un moyen d'usurper leur identité. Ces programmes peuvent prendre plusieurs formes, notamment des vers, des virus, des logiciels espions et des chevaux de Troie. Les vers sont des programmes qui se reproduisent de façon autonome sur des ordinateurs à l'aide d'un réseau informatique alors que les virus informatiques génèrent des copies d'eux-mêmes dont la propagation dépend des autres hôtes du réseau[131]. Un cheval de Troie est un type de programme malveillant contenant une fonction illicite cachée permettant de contourner les mécanismes de sécurité du système informatique pour s'introduire dans le système et modifier, altérer ou détruire les données informatiques[132]. Le système informatique peut être infecté en cliquant sur un message électronique ou en se rendant sur un site Web ou par le téléchargement des programmes infectés[133].

Les botnets forment des réseaux d'ordinateurs personnels infectés à l'insu de leur propriétaire par ces programmes malveillants et contrôlés à distance par des criminels à des fins de commettre des activités illicites, telles que le pollupostage, l'empoisonnement de DNS (Domain Name System), l'envoi de chevaux de Troie ou de virus pour faciliter la commission d'escroquerie en ligne[134]. Ainsi, la prolifération de ces réseaux de zombies dans le cyberespace renforcerait la commission de l'escroquerie informatique et la localisation de ces criminels serait difficilement réalisable en raison des caractéristiques du réseau, notamment l'anonymisation et la dématérialisation du réseau. Dans ce sens, ces réseaux de zombies, tout comme les programmes malveillants constituent une forme de menaces liées à la sécurité du réseau Internet et au développement du commerce électronique, comme l'indique le Groupe de travail[135].

Nous appuyons fortement leur recommandation à l'effet que le gouvernement fédéral devrait adopter un ensemble de règlements précis visant à interdire les logiciels espion et les réseaux de zombies[136]. De plus, en créant une infraction précise sur la possession de plusieurs pièces

---

130 Office québécois de la langue française, Le grand dictionnaire terminologique, *Programme malveillant*, 2005, http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/GDT_fiches/programme_malveillant.html.

131 Wikipédia L'encyclopédie libre, *Logiciel malveillant*, 15 février 2006, http://fr.wikipedia.org/wiki/Logiciel_malveillant.

132 Contrairement au virus, le cheval de Troie ne peut se reproduire de façon autonome : *ibid*.

133 Gendarmerie Royale du Canada, *Protection des renseignements personnels et protection contre l'escroquerie-Guide pratique de l'étudiant*, p. 6, 1er mars 2006, http://www.rcmp-grc.gc.ca/scams/student_guide_f.pdf.

134 Wikipédia L'encyclopédie libre, *Botnet*, 6 décembre 2005, http://fr.wikipedia.org/wiki/Botnet.

135 Industrie Canada, Freinons le pourriel Créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel*, mai 2005, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317f.html.

136 *ibid*.

d'identité et la mise en ligne de sites Web frauduleux, les menaces seraient aux mieux contrôlées. Les utilisateurs devraient entre autres prévoir des logiciels destinés à protéger pleinement le système informatique, tels que des antivirus, des pare-feux, des anti logiciels espions et les mettre à jour[137]. Ils peuvent acheminer des plaintes au PhoneBusters, un organisme central du Canada chargé de recueillir des renseignements sur les plaintes en matière de télémarketing, de lettres frauduleuses et en matière de vol d'identité[138].

Conclusion

La cybercriminalité économique constitue donc un problème préoccupant qui pourrait nuire au développement du commerce électronique si les mécanismes de répression contre la fraude, le vol et l'escroquerie s'avèrent inefficaces. L'élargissement de la notion de fraude a contribué à répandre la confusion et a entraîné une réelle difficulté à délimiter les éléments de faute de l'infraction. L'imprécision s'est également retrouvée dans l'actus reus et la mens rea de l'infraction du vol. L'inexistence dans le droit pénal canadien d'une infraction explicite visant la répression directe de l'usurpation du nom ou de l'adresse IP des utilisateurs d'Internet et du hameçonnage n'a pas découragé les criminels à émettre un comportement frauduleux. L'Architecture du cyberespace a permis de préserver leur anonymat après la commission de l'infraction. Le progrès de la technologie numérique a permis aux criminels de recourir à des dispositifs de plus en plus performants pour commettre des crimes économiques.
Il faut donc se tourner vers le législateur pénal pour qu'il redéfinisse les éléments de faute de la fraude, l'actus reus et le mens rea du vol et qu'il érige une infraction qui serait explicitement reconnue dans le *Code criminel* eu égard à l'usurpation d'identité. La répression sévère de « cette » nouvelle infraction découragerait les criminels et permettrait ainsi aux organismes d'application de la loi de les appréhender. Une des solutions étant le renforcement du cadre juridique des infractions économiques, existe-t-il d'autres pistes de solution pour combattre la cybercriminalité économique ?

---

137 Gendarmerie Royale du Canada, *Protection des renseignements personnels et protection contre l'escroquerie-Guide pratique de l'étudiant*, p. 6, 1er mars 2006, http://www.rcmp-grc.gc.ca/scams/student_guide_f.pdf.

138 *ibid*. à la page 8.

BIBLIOGRAPHIE

- **Monographies, recueils et articles de revues**

BOISVERT, A.-M., « La fraude criminelle : Sommes-nous allés trop loin? », (1995) 40 *Mcgill R.D.* 415-486.

COMMISSION DE RÉFORME DU DROIT DU CANADA, « Le vol et la fraude », *Document de travail 19*, Ottawa, Ministre des Approvisionnements et Services Canada, 1977, 136 p.

COMMISSION DE RÉFORME DU DROIT DU CANADA, « Le vol et la fraude », *Rapport n°12*, Ottawa, Ministre des Approvisionnements et Services Canada, 1979, 65 p.

COMMISSION DE RÉFORME DU DROIT DU CANADA, « Pour une nouvelle codification du droit pénal », *Rapport n°31*, Ottawa, Ministre des Approvisionnements et Services Canada, 1987, 233 p.

CÔTÉ-HARPER, G. et TURGEON, J., « Droit pénal canadien- Supplément », Cowansville, Éditions Yvon Blais, 1994, 171 p.

COURNOYER, G. et OUIMET, G., *Code criminel annoté 2005*, Cowansville, Éditions Yvon Blais, 2005, 2419 p.

EWART, J.D., « Criminal Fraud », Toronto, Carswell, 1986, 182 p.

GAGNÉ, J. et RAINVILLE, P., « Les infractions contre la propriété : le vol, la fraude et certains crimes connexes », Cowansville, Éditions Yvon Blais inc, 1996, 514 p.

GRONDIN, R., « Les infractions contre la personne et contre les biens », 5e éd., Montréal, Wilson & Lafleur ltée, 2003, 194 p.

HAMMOND, R. G., « Quantum Physics, Econometrics Models and Property Rights to Information », (1981), 27 *R.D. Mcgill* 47.

HENDERSON, M. B., « Commercial Crime in Canada », Toronto, Carswell, 2004, 15-25 p.

PROULX, M., « Le concept de la malhonnêteté dans la fraude pénale », dans *Droit pénal: Orientations nouvelles: Colloque du Service de la formation permanente du Barreau du Québec*, Cowansville (Québec), Yvon Blais, 1987, 209-234.

RAINVILLE, P., « Droit et Droiture : le critère de la malhonnêteté et la fraude criminelle», (1992) 33 *C. De D.*, 189.

STUART, D., « Canadian Criminal Law : A Treatise», 3e éd., Scarbough, Carswell, 1995, 672 p.

TRUDEL, P., ABRAN, F., BENYEKHLEF, K. et HEIN S., *Droit du Cyberespace*, Éditions Thémis, 1997, 1296 p.

- **Sites Internet**

L'ASSOCIATION DES BANQUIERS CANADIENS, *L'usurpation d'identité : la nécessité d'une politique en matière de prévention*, p. 2,

http://www.cba.ca/fr/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20FRE.pdf

Dicofr.com, *Adresse IP*, http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101000012

Gendarmerie Royale du Canada, *Protection des renseignements personnels et protection contre l'escroquerie-Guide pratique de l'étudiant*, p. 1, 1er mars 2006, http://www.rcmp-grc.gc.ca/scams/student_guide_f.pdf

Gouvernement du Canada, Service canadien de renseignements criminels, « Criminalité financière Vol d'identité » octobre 2005, http://www.cisc.gc.ca/annual_reports/annualreport2005/identity_theft_2005_f.htm

Office québécois de la langue française, Bibliothèque virtuelle, *Vocabulaire d'Internet*, 1er mars 2006, http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/8869710.html

Travaux publics et Services gouvernementaux Canada, « Commerce électronique, instaurer la confiance », novembre 2005, http://www.tpsgc.gc.ca/recgen/colloquium2005/presentations/group-1-peter-ferguson-f.html

Wikipédia L'encyclopédie libre, *IP spoofing*, 11 janvier 2006, http://fr.wikipedia.org/wiki/IP_spoofing

Wikipédia L'encyclopédie libre, *Botnet*, 6 décembre 2005, http://fr.wikipedia.org/wiki/Botnet

Wikipédia L'encyclopédie libre, *Logiciel malveillant*, 15 février 2006, http://fr.wikipedia.org/wiki/Logiciel_malveillant

- **Table de la législation**

Textes fédéraux

Code criminel, L.R.C. (1985), c. C-46 : art. 322 ; 342 ; 361 ; 380.

Textes internationaux

Convention sur la cybercriminalité, STE n° : 185, Budapest, 23 novembre 2001.

- **Table de la jurisprudence**

Abbas c. *La Reine*, [1984] 2 R.C.S. 526.

Adams c. *La Reine*, J.E. 95-106 (C.A.).

Coté c. *La Reine*, [1991] R.L. 110.

R. c. *Allsop* (1976) 64 Cr. App. R. 29 (C.A. Ang.).

R. c. *Bernard*, [1988] 2 R.C.S. 833.

R. c. *Bernston*, (2000) 145 C.C.C. (3d) 1 (C.A. Sask.), conf. par [2001] 1 R.C.S. 365.

R. c. *DeMarco*, (1974) 13 C.C.C. (2e) 369 (C.A. Ont.).

R. c. *Kirkwood*, (1983) 5 C.C.C. (3d) 393 (C.A. Ont.).

R. c. *Lacombe*, (1990) 60 C.C.C. (3e) 489 (C.A. Qué.).

R. c. *Libman*, [1985] 2 RCS 178.
R. c. *Littler*, (1975) 27 C.C.C. (2e) 234 (C.A. Qué.).
R. c. *DeMarco*, (1974) 13 C.C.C. (2d) 369.
R. c. *McLaughin*, [1980] 2 R.C.S. 331.
R. c. *Milne*, [1992] 1 R.C.S. 697.
R. c. *Olan*, [1978] 2 R.C.S. 1175.
R. c. *Pereira et Poulis*, [1990] J.Q. n° 2004 (C.A.).
R. c. *Sinclair*, (1968), 52 Crim. App. R. 618, [1968] 3 All. E.R. 241 (C.A.).
R. c. *Stewart*, [1988] 1 R.C.S. 963.
R. c. *Théroux*, [1993] 2 R.C.S. 5.
R. c. *Vaillancourt*, [1987] 2 R.C.S. 636.
R. c. *Zimmerman*, (1979) 4 W.C.B. 311 (C. cté Ont.).
R. c. *Zlatic*, [1993] 2 R.C.S. 29.
Re London & Globe Finance Co., [1903] 1 Ch. 728.
Sansregret c. *R*., [1985] 1 R.C.S. 570.
Vézina c. *La Reine*, [1986] 1 R.C.S. 2.