

Les voleurs d'identité

Profil d'une délinquance ordinaire

Benoît Dupont & Guillaume Louis

Note de recherche no. 2



Cette recherche a été entreprise grâce, en partie, au soutien financier du Programme des chaires de recherche du Canada et du Fonds Québécois de Recherche sur la Société et la Culture.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers. Elle collabore pour cela avec des organismes gouvernementaux et des entreprises.

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.edupont.net
Fax : +1-514-343-2269

© Chaire de recherche du Canada en sécurité, identité et technologie 2009

Faits saillants

Le vol d'identité a frappé 1,7 millions de personnes au Canada en 2008 et a fait 340.000 victimes au Québec l'année précédente. Malgré le volume significatif de cette forme émergente de criminalité, les connaissances dont nous disposons sur le sujet restent encore relativement limitées, particulièrement en ce qui concerne le profil des auteurs de ces crimes et leurs modes opératoires.

Le vol d'identité est souvent représenté dans les médias comme une forme de délinquance nécessitant des compétences techniques très développées et étroitement associée au crime organisé.

Cette recherche, qui s'appuie sur des sources secondaires provenant en grande majorité des États-Unis, permet de mieux comprendre la dynamique du vol d'identité et de démontrer qu'il s'agit en réalité d'une forme de délinquance très diversifiée englobant des stratagèmes dont la sophistication varie grandement.

Notre base de données est constituée à partir de 574 articles de presse recueillis de janvier à juin 2008. Elle contient 195 affaires de vol d'identité impliquant 422 délinquants.

Les femmes représentent près de 40% des délinquants. Cette forte présence s'explique selon nous par l'absence de violence inhérente à ce type de crime et par la possibilité de le commettre sans le soutien de pairs délinquants.

Les auteurs de vols d'identité sont relativement plus âgés que les autres délinquants, avec une moyenne de 33 ans. Le délinquant le plus âgé figurant dans notre base de données avait 67 ans.

Les délinquants ont agi seul dans une grande majorité des cas (64,6%), ce qui semble contredire la thèse d'une forte implication du crime organisé dans ce type de crime.

Concernant les techniques d'acquisition des identités, des moyens technologiquement rudimentaires comme le vol physique de portefeuille ou de sac à main et l'escroquerie représentent plus de la moitié des cas (53,4%). Il semble donc que les délinquants habituels exploitent les opportunités qui leurs sont fournies pour s'adonner au vol d'identité.

Par ailleurs, il est intéressant de noter que le second mode d'acquisition le plus répandu concerne des professionnels qui détournent à leur profit les renseignements personnels de clients, patients ou bénéficiaires qu'ils rencontrent dans le cadre de leur emploi (28,3%).

À l'étape de la fraude, Internet devient un outil privilégié des délinquants qui souhaitent extraire un bénéfice financier des identités volées, puisque 45,3% des cas impliquent l'achat de biens ou de services en ligne, ainsi que l'obtention de lignes de crédit via Internet.

Contrairement à l'image d'un crime faisant un grand nombre de victimes lors de chaque incident, notre échantillon n'identifie qu'une seule victime par affaire dans 57% des cas. Il est possible qu'un biais de sélection soit à l'origine de ce résultat surprenant.

Le montant médian des profits réalisés par les auteurs de vol d'identité est de 26.000 dollars US, ce qui fait du vol d'identité un crime relativement profitable au vu des faibles risques encourus.

Parmi les personnes arrêtées et condamnées, les peines infligées sont relativement lourdes, avec une peine moyenne de 54 mois de prison. Cette sévérité nous semble influencée par une volonté de dissuasion à l'égard de délinquants pouvant penser qu'ils jouissent en ce domaine d'une véritable impunité. Par contre, il semble que les affaires les plus complexes se règlent plus fréquemment par une peine assortie d'un sursis, en raison du pouvoir de négociation dont disposent les criminels à qui on demande de fournir des informations sur le mode opératoire utilisé.

Introduction

Le vol d'identité a frappé 6,7% de la population adulte canadienne en 2008, ce qui représente environ 1,7 millions de personnes (Sproule et Archer, 2008). Il a fait environ 340.000 victimes au Québec l'année précédente (Dupont 2008). Malgré le volume significatif de cette forme émergente de criminalité, les connaissances dont nous disposons sur le sujet restent encore relativement limitées, particulièrement en ce qui concerne le profil des auteurs de ces crimes et leurs modes opératoires. En effet, les principales études disponibles à ce jour prennent la forme de sondages menés auprès de victimes (Baum, 2006; ISIQ, 2007; Kim, 2007; Synovate, 2007; ITRC, 2008; Sproule et Archer, 2008), ce qui nous permet de mesurer la prévalence de ce crime, de comprendre l'usage qui est fait des informations dérobées et d'évaluer l'ampleur des préjudices subis. Cependant, l'une des principales limites des sondages de victimisation est que seule une minorité de victimes est en mesure de dire comment leurs informations personnelles se sont retrouvées entre les mains des délinquants, qu'elles sont par ailleurs rarement en mesure d'identifier. En effet, par nature, le vol d'identité et la fraude qui l'accompagne peuvent être commis sans que l'auteur et sa victime n'établissent un contact direct (contrairement aux agressions physiques par exemple).

Il est également difficile de s'appuyer sur les données policières pour analyser ce phénomène. En effet, les sondages mentionnés plus haut révèlent qu'une minorité seulement des victimes de vols d'identité déclarent ces derniers à la police. **Au Canada par exemple, seulement 13% des fraudes subies à la suite d'un vol d'identité ont été reportées à la police en 2007** (Sproule et Archer, 2008 : 25). Quant à la statistique criminelle, elle ne traite pas encore le vol d'identité comme une catégorie distincte, et il est par conséquent impossible de centraliser les données recueillies de manière hétérogène par les divers services de police.

Ce déficit de connaissances est problématique car il limite notre compréhension des modes opératoires privilégiés par les auteurs, qui représentent la clé de politiques et de stratégies de prévention efficaces. Il nous donc apparu utile de tenter de remédier à cette situation en analysant le profil d'un échantillon de voleurs d'identité constitué à partir d'affaires rapportées dans les médias nord-américains. Cette stratégie de recherche vise à dresser des comparaisons avec deux études semblables réalisées aux États-Unis en 2007 grâce au soutien du *Department of Justice* (Copes et Vieraitis, 2007; Gordon et al., 2007). Après avoir passé en revue la littérature scientifique limitée portant sur les voleurs d'identité et leurs méthodes, nous discutons la méthodologie employée ainsi que ses limites. Nous présentons ensuite les résultats de notre recherche en examinant plus particulièrement le profil socio-démographique des auteurs de vols d'identité, les méthodes employées, leurs liens avec les victimes, les profits réalisés et les condamnations leur étant imposées lorsqu'ils sont arrêtés et jugés.

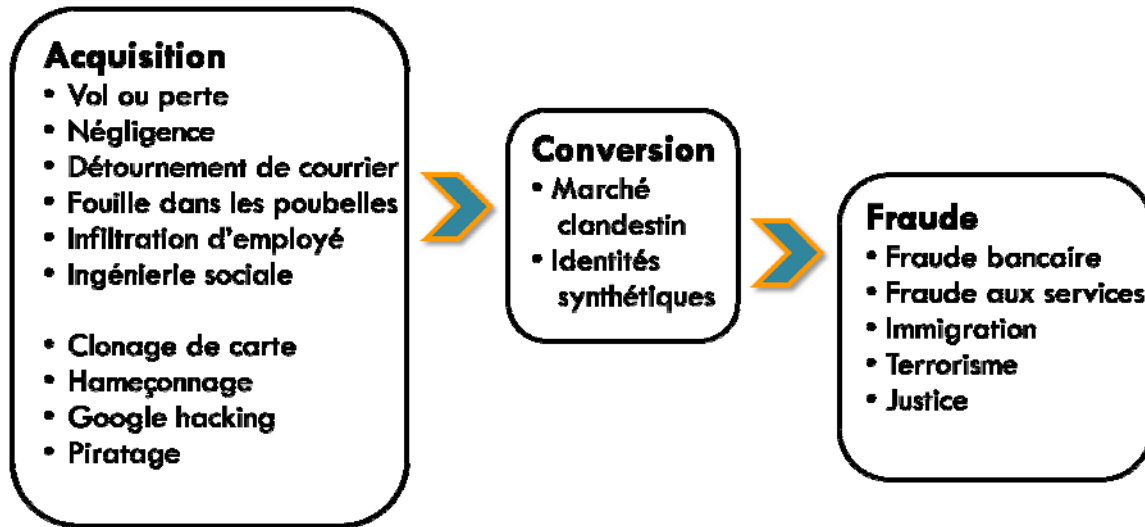
Recension de la littérature

Il est convenu d'affirmer que **le vol d'identité est l'un des crimes connaissant la plus forte croissance depuis quelques années** (Finklea, 2009). Toutefois, nous ne savons pas si cette augmentation relève d'une adaptation des délinquants habituels qui « migrent » vers ce type de crime en raison des risques moindres ou des profits accrus qui y sont associés, ou si elle reflète au contraire l'apparition de nouveaux délinquants aptes à exploiter les opportunités criminelles qui découlent du développement technologique des sociétés contemporaines.

Les grands médias, la presse spécialisée en sécurité informatique et les rapports publiés à intervalles réguliers par les vendeurs de solutions de sécurité rapportent l'existence de réseaux structurés de voleurs d'identités basés dans les pays d'Europe de l'Est mais opérant à l'échelle mondiale, liés au crime organisé et disposant de compétences techniques extrêmement avancées (voir à titre d'exemple Berinato, 2007; Symantec, 2008; Thibodeau, 2008). Ces délinquants de haut vol seraient en mesure d'exploiter sans peine les failles du cyberspace pour se procurer et monnayer de manière frauduleuse des millions d'identités, sans crainte d'être inquiétés par des forces de l'ordre impuissantes devant une telle sophistication. Sans vouloir remettre en question l'existence de ces marchés clandestins très spécialisés et profitables, nous avançons néanmoins l'idée que la manière dont ils sont représentés dans les médias et par les experts 'commerciaux' en sécurité informatique relève trop souvent de ce que le juriste Paul Ohm appelle « le mythe du super-utilisateur » (Ohm, 2008).

Le vol d'identité est en réalité une forme de délinquance très diversifiée englobant des stratagèmes plus ou moins sophistiqués. **On distingue dans la littérature scientifique trois grandes étapes du vol d'identité** (Sproule et Archer, 2007). **Dans un premier temps, l'acquisition d'identifiants appartenant à des personnes vivantes ou décédées** peut aussi bien prendre la forme d'un banal vol de sac à main ou de portefeuille que le piratage informatique d'une base de données protégée par des systèmes de sécurité devant être déjoués par des individus disposant d'une expertise et d'un équipement spécifique, comme ce fut le cas dans l'affaire TJX (magasins Winners et HomeSense). **Dans un deuxième temps, les identifiants volés vont être soit revendus sur des marchés clandestins en ligne** où la loi de l'offre et de la demande va permettre d'en déterminer la valeur d'usage (pour les fraudeurs), **soit être modifiés afin de créer des identités synthétiques**, c'est-à-dire des identités qui ne correspondent pas à des personnes réelles mais qui sont néanmoins crédibles aux yeux des institutions fraudées. **La troisième et dernière étape comprend la fraude proprement dite**, puisque dans de nombreuses juridictions, la possession d'éléments d'identification personnelle appartenant à des tiers ne représente pas une infraction à la loi. Cette fraude pourra avoir des objectifs pécuniaires, mais elle pourra aussi faciliter des crimes connexes liés à l'immigration clandestine, au terrorisme ou permettre au fraudeur de se soustraire à la justice en assumant l'identité d'une personne sans casier judiciaire. Le diagramme 1 détaille ces trois étapes.

Diagramme 1 : Les trois étapes du vol d'identité



On voit à travers ce diagramme que **les connaissances techniques requises de la part des délinquants varient de manière significative selon le mode d'acquisition, de conversion ou de fraude privilégié par ceux-ci**, qui n'hésitent d'ailleurs pas à opérer selon les principes de division du travail bien connus en économie. **Une autre distinction relative aux caractéristiques des voleurs d'identité concerne la fréquence de leurs actes.** Newman et McNally (2005 : 26) proposent ainsi une typologie des délinquants à 'faible' et à 'fort' volume. Dans le premier groupe, on retrouverait les personnes qui passent à l'acte une seule fois en réponse à une crise personnelle ainsi que les personnes qui exploitent les opportunités qui se présentent à elles (Gayer, 2003 : 13). Dans le second groupe, figureraient des individus qui recherchent activement des opportunités d'acquisition d'identifiants personnels ainsi que des délinquants ordinaires. Cette typologie est cependant dérivée de celles qui sont utilisées dans le domaine de la délinquance en col blanc et ne s'appuie que sur des données anecdotiques.

À ce jour, **seulement trois études menées aux États-Unis ont eu recours à des données empiriques pour analyser avec plus ou moins de détails le profil des personnes condamnées pour vol d'identité.** Une première étude, menée par Allison et al. (2005) dans une ville de Floride portait sur un échantillon de 52 délinquants. Ces derniers étaient en majorité de sexe féminin (63%), noirs (69%) et âgés en moyenne de 32 ans. On observe une certaine parité dans cet échantillon entre les délinquants sans emploi (53%) d'une part, et ceux qui sont salariés (41%) ou retraités (3%) d'autre part. Dans 60% des cas, aucun lien préalable n'existait entre la victime et le voleur, et 64% des délinquants opéraient seuls. Aucune information n'est disponible sur les techniques employées ou les profits accumulés par les auteurs.

La seconde étude, réalisée par Copes et Vieraitis (2007) porte sur 59 délinquants incarcérés dans des prisons fédérales, avec qui des entretiens semi-directifs ont été menés. Bien que cet échantillon ne soit pas représentatif, il nous permet de mieux comprendre les motivations et la diversité des méthodes employées par les répondants. L'échantillon est composé pour moitié de personnes dont le profil correspond à celui des petits délinquants de rue, et pour moitié d'individus qui ont utilisé leurs gains pour mener une vie « rangée » correspondant aux critères de la classe moyenne. **Le choix du vol d'identité est justifié en raison des faibles risques impliqués et de la facilité avec laquelle cette activité peut être menée.** Les deux tiers des répondants (63%) avaient déjà été arrêtés auparavant dans le cadre de crimes contre la personne, contre la propriété ou relatifs à l'usage et au trafic de stupéfiants. **Les techniques d'acquisition et de fraude les plus fréquentes sont relativement peu sophistiquées sur le plan technologique,** puisque les informations personnelles sont achetées auprès d'intermédiaires qui en manipulent de grandes quantités dans le cadre de leur emploi, récupérées dans les boîtes aux lettres et les poubelles des victimes, ou volées à des membres de la famille ainsi que des connaissances personnelles ou professionnelles. Les formes de fraude les plus répandues incluent l'émission de chèques contrefaits, l'obtention frauduleuse de cartes de crédit et la souscription d'emprunts bancaires sous des identités usurpées. **Parmi les compétences manifestées par les délinquants pour mener à bien leurs projets, les auteurs relèvent des compétences sociales, des compétences d'intuition, des compétences techniques et une bonne connaissance des modes de fonctionnement du système bancaire.**

La dernière étude fut menée par Gordon et al. (2007) avec le soutien du *Secret Service*, qui est l'une des principales organisations d'application de la loi fédérale engagée dans la lutte contre le vol d'identité aux États-Unis. Les analyses portent sur 517 affaires de vol d'identité traitées par le *Secret Service* de 2000 à 2006. Bien que l'échantillon soit beaucoup plus important que dans l'étude précédente (933 personnes mises en cause), **le profil des délinquants impliqués reste relativement diversifié** : les femmes constituent un tiers des accusés, les noirs sont surreprésentés (53,8%) mais les blancs restent nombreux avec 38,3% des mis en cause, et 71% des personnes interpellées dans le cadre de ces affaires n'étaient pas connues de la police. **Concernant l'implication du crime organisé, on peut affirmer qu'elle est minoritaire,** puisque 80% des accusés ont agi seuls ou avec un complice unique. On retrouve aussi dans cette troisième étude l'appât du gain comme facteur principal de motivation. Le préjudice financier médian par affaire se monte à 31.000 dollars US (et à 22.500\$ pour les affaires impliquant seulement un délinquant). Bien que les auteurs de l'étude aient quantifié le recours à l'Internet ou à d'autres technologies dans leurs analyses, le fait qu'ils n'aient pas distingué les stades de l'acquisition, de la conversion et de la fraude rend leurs résultats difficilement exploitables. Ainsi, lorsqu'ils avancent qu'Internet a joué un rôle dans 51% des affaires, cela inclut aussi bien le déploiement de logiciels malveillants que l'envoi de courriers électroniques à des complices. Ces informations restent donc trop fragmentaires pour en tirer des conclusions définitives sur le niveau de compétence technologique des délinquants. Finalement, **une minorité non négligeable d'affaires**

(34,1%) implique des employés malhonnêtes qui se procurent des identifiants personnels de clients ou d'usagers sur leur lieu de travail. Le secteur le plus affecté est celui du commerce de détail (43,8%), suivi du secteur bancaire et financier (23,8%).

Méthodologie

Contrairement aux trois études mentionnées dans les pages précédentes, notre recherche s'appuie sur des sources secondaires provenant de coupures de presse provenant de médias nord-américains, **l'objectif étant de constituer une base de données qui ne soit pas limitée à une zone géographique restreinte, à une institution particulière ou à un échantillon réduit de délinquants.**

Si le vol d'identité est devenu une préoccupation majeure pour l'opinion publique, cela ne garantit pas pour autant que les multiples affaires impliquant un vol d'identité soient couvertes par les grands organes de presse. Aussi, plutôt que de procéder à une recherche dans les archives de ces derniers, la stratégie retenue a été d'utiliser le système « Alertes Google », qui permet d'être informé quotidiennement des nouveaux résultats obtenus par le moteur de recherche en ligne *Google News*¹. Ce faisant, chaque fois que le mot-clef « Identity theft » était mentionné dans un article publié en ligne parmi les 4,500 sources d'information mises à jour en continu, nous en recevions le lien Internet. Cette alerte a été en fonction pendant 6 mois, soit de janvier à juin 2008.

Parmi l'ensemble des informations reçues, n'ont été retenues que celles relatant une affaire de vol d'identité. Ainsi, **nous disposons d'une base de données concernant 195 affaires et 422 délinquants constituée à partir de 574 articles de presse.** Les faits rapportés sont survenus, pour la quasi-totalité des affaires (190), sur le territoire américain.

Le contenu des articles de presse a été confronté à une grille d'analyse visant les points suivants : 1) source ; 2) date de publication ; 3) localisation géographique des affaires ; 4) identification des délinquants ; 5) sexe des délinquants ; 6) âge des délinquants ; 7) statut des délinquants face à la justice ; 8) sentence reçue le cas échéant ; 9) moyen d'acquisition de l'identité ; 10) utilisation de l'identité ; 11) motivation du délinquant ; 12) montant obtenu par le vol d'identité ; 13) nombre de victimes identifiées ; 14) sexe des victimes ; 15) liens entre les délinquants et les victimes.

Afin d'augmenter la validité des informations récoltées, nous avons systématiquement tenté de vérifier le contenu des articles originaux – transmis par l'alerte – en croisant les renseignements présentés avec une recherche spécifique pour chaque affaire. Malgré cela, pour 44 cas, nous ne disposons que d'une seule source. Néanmoins, dans plus d'un dossier sur deux, nous disposons d'au moins trois sources différentes. En outre, nous

¹ <http://news.google.com/>

sommes en mesure d'établir la fiabilité de nos données par leur comparaison avec celles de Gordon et al. (2007). Si certaines différences sont observables dans les résultats des deux études, les principales caractéristiques socio-démographiques des auteurs de vols d'identité sont comparables (courbe d'âge des auteurs de vols d'identité ainsi que la proportion homme/femme).

Avant de poursuivre, il est nécessaire de préciser que **ces données souffrent d'un important biais de sélection judiciaire et médiatique**. En effet, l'ensemble des sondages de victimisation réalisés sur le sujet démontrent que seulement une minorité des victimes décident de déclarer le crime à la police (de 10 à 20% selon les juridictions), et que les enquêtes menées ne concernent donc que cet échantillon déjà très réduit. Par ailleurs, pour que les médias puissent rapporter l'identité d'un voleur d'identité et les circonstances du crime pour lequel il a été arrêté, encore faut-il que la police puisse identifier un suspect. Or, il s'avère que le vol d'identité semble être le crime que la police a le plus de mal à élucider, une étude menée en 2002 faisant état d'un taux de résolution de 4% (Allison et al. 2005 : 24). Par ailleurs, les différents niveaux de juridiction se répartissent les affaires en fonction de leur degré de complexité. Ainsi, le FBI et le *Secret Service* se concentrent sur les groupes organisés et ayant des ramifications internationales, alors que les services municipaux, de comtés et les polices d'états traitent les vols d'identités « locaux » (Finklea 2009). Il est donc possible que notre échantillon principalement élaboré à partir de médias locaux surreprésente les affaires de faible envergure, même si notre alerte ne contenait à priori pas de distinction de gravité. Finalement, dans les juridictions fortement frappées par ce type de délinquance, on peut aisément imaginer que les journalistes vont concentrer leur attention sur les affaires les plus 'médiatiques', c'est-à-dire celles qui impliquent un préjudice financier élevé, un mode opératoire particulièrement audacieux ou des victimes singulièrement affectées par leur expérience. **Néanmoins, en l'absence de données statistiques de meilleure qualité, et au vu de la taille conséquente de notre échantillon, nous estimons qu'une telle analyse reste tout à fait valide** et pourra nous aider à mieux définir le profil des voleurs d'identité ainsi que de leurs tactiques.

Profil des auteurs

Parmi notre échantillon de voleurs d'identité, **les hommes sont certes toujours plus nombreux que les femmes mais ces dernières sont plus représentées dans ce délit que dans la plupart des crimes**, y compris ceux visant les biens. Une des raisons pour lesquelles **elles constituent pratiquement 40% des délinquants étudiés** réside dans le fait que les modes opératoires les plus répandus de vols d'identité ne font appel que très exceptionnellement à la violence, et qu'ils n'exigent pas une implication notable dans le monde interlope (et ce aussi bien au stade de l'acquisition de l'identité que de son utilisation frauduleuse).

Les auteurs de vol d'identité sont relativement plus âgés que les autres délinquants, avec une moyenne d'âge de 33 ans, et un 'vétérane' de 67 ans apparaissant dans notre échantillon. Cela dit, il se pourrait que la sous-représentation des jeunes (aucun auteur en dessous de 18 ans dans notre échantillon) soit attribuable à un biais médiatique résultant de l'interdiction légale de nommer les contrevenants mineurs dans de nombreux états et provinces, ou du désintérêt des reporters pour cette catégorie de délinquants. C'est donc dans la classe d'âge médiane que l'on retrouve le plus de délinquants. Une combinaison de facteurs permet d'expliquer ce constat. Tout d'abord, si le vol d'identité ne repose pas nécessairement sur l'Internet en ce qui a trait à l'acquisition proprement dite, l'identité volée, elle, est souvent mise à profit par le biais de ce média. Le vol d'identité étant assimilable à une forme de tromperie, de fausse représentation, encore faut-il être en mesure de duper l'interlocuteur. Cela s'avère fort compliqué pour un mineur ou un jeune majeur si l'identité est utilisée en personne et la protection assurée par l'intermédiaire d'Internet ne fonctionnera guère avec un minimum de contrôle parental – puisqu'il faudra donner une adresse de livraison. Aussi, il n'est guère surprenant que **la classe d'âge des 25 à 40 ans constitue 50% de notre échantillon.**

Notre échantillon couvre principalement les États-Unis et pratiquement tous les états sont représentés. Toutefois, plusieurs d'entre eux se distinguent par le nombre d'affaires de vol d'identité qui y ont été recensées par les organes de presse. Naturellement l'on retrouve parmi eux les états les plus peuplés (l'état de New York rassemble à lui seul 15% des cas, il est suivi de la Floride et de la Californie avec 8% chacun). Le Texas doit sa troisième place à sa situation face à l'immigration clandestine qui constitue une part non-négligeable des cas de vol d'identité.

Le vol d'identité est souvent associé dans la littérature scientifique et dans les médias au crime organisé local ou provenant d'Europe de l'Est (Newman et McNally, 2005; Deloitte, 2008; Winterdyk et Thompson, 2008). Pourtant, notre échantillon, confirmant en cela les résultats de l'étude de Gordon et al. (2007), ne vient pas appuyer cette relation. En effet, les affaires impliquant plus de 3 acteurs représentent moins de 14%. **Dans une très large majorité de cas, le délinquant a agi seul (64,6%).**

Mode opératoire et utilisation de l'identité

Le vol d'identité est-il ou non un crime technologique ? L'intérêt croissant porté à ce délit réside avant toute chose dans la crainte qu'effectivement, les innovations technologiques et la démocratisation des machines – miniaturisation, simplicité d'utilisation – soient à l'origine de son développement exponentiel. Dans l'étude réalisée par Gordon et al (2007), il apparaît que plus de la moitié des cas de vol d'identité impliquent le recours à un moyen technologique. Les auteurs précisent toutefois que, la plupart du temps, l'utilisation d'un outil technologique n'intervient que dans une seconde phase, c'est-à-dire après que le vol ait eu lieu. En effet, les auteurs distinguent l'acquisition des données personnelles d'identification – le plus souvent le

fruit d'une technique rudimentaire – et la reproduction de l'identité volée qui elle implique le recours à la technologie (scanner, appareil photographique numérique...). Cette distinction, fort pertinente, n'est malheureusement pas étayée de statistiques dans l'étude concernée, si bien qu'il nous est impossible de connaître la situation avec précision. Dans notre étude, il ne nous a pas été possible de produire cette distinction entre vol et reproduction. En revanche, nous en avons effectué une autre qui reflète mieux les trois étapes mentionnées dans la section introductive, et qui différencie l'acquisition de l'identité de la fraude rendue possible par l'utilisation de l'identité volée.

Ainsi qu'il est possible de l'observer dans le tableau 1, **des techniques rudimentaires ont été employées dans plus de la moitié des cas analysés** (vols physiques et escroqueries). Les vols physiques (vols à la tire, vols d'automobile, vols de poubelles, vols de courriers) constituent, de très loin, le principal moyen d'acquisition des identités volées. Il est d'ailleurs très intéressant de constater que parmi les quatre formes de vol présentées, les deux plus récurrentes ne sont pas du tout spécifiques au vol d'identité. En outre, nous avons parfois été en mesure d'observer que **plusieurs affaires de vol d'identité sont survenues sans être le motif premier du vol**. Les délinquants en possession d'un sac à main se sont aperçus qu'ils pouvaient profiter doublement de leur vol. **Il n'y a donc pas dans ces affaires de spécialisation dans le vol d'identité, mais plutôt l'exploitation par des délinquants « traditionnels » d'opportunités criminelles reliées à l'acquisition inattendue d'identifiants personnels**. Par ailleurs, les quelques cas d'escroquerie qui figurent dans notre échantillon impliquent tous la même méthode, la fausse représentation, et visaient principalement des personnes âgées ou frappées de déficiences.

Tableau 1 : Moyen d'acquisition de l'identité

	Nombre	Pourcentage
Vol physique	142	45,7%
Utilisation frauduleuse d'un fichier	88	28,3%
Internet	57	18,3%
Escroquerie	24	7,7%

Le deuxième mode opératoire le plus répandu est l'utilisation frauduleuse d'un fichier (qu'il s'agisse d'un fichier électronique ou sur support papier). On retrouve ici une majorité de **professionnels qui détournent à leur profit les renseignements personnels de clients, patients ou bénéficiaires qu'ils rencontrent dans le cadre de leur profession**. Dans de rares cas, le fichier utilisé relevait du domaine public (banque de donnée des personnes disparues, état civil). Dans ces derniers, la seule utilisation du fichier n'était pas suffisante et les délinquants ont également eu recours à des techniques de fausse représentation afin d'obtenir, dans un second temps, les documents nécessaires pour maintenir leur fausse identité.

Finalement, **le vol a été perpétré par le biais de l'Internet dans un peu moins de 20% des cas**. Il s'agit là de vols reposant sur des techniques plus sophistiquées (piratage,

hameçonnage ou ‘phishing’ et ‘pharming’, implantation de logiciels espions). En règle générale, on ne retrouve pas un degré d’organisation - s’agissant du nombre d’individus impliqués dans une même affaire - très important, à l’exception notable d’une affaire mettant en présence 38 personnes et disposant de ramifications internationales. Il nous semble qu’il existe une **corrélacion implicite entre le faible recours à la technologie et l’individualisme des délinquants**. En effet, les modes les plus sophistiqués de vol d’identité s’appuient sur une division du travail qui fait appel à des expertises complémentaires, alors que les délinquants opportunistes peuvent se permettre d’agir seuls, même si leur approche ‘artisanale’ limite proportionnellement leurs ‘profits’.

Il est clair que **le vol d’identité est avant tout un délit économique** puisque dans plus de 84% des cas, les criminels recherchaient un enrichissement direct. Toutefois, il ne faut pas négliger la problématique qui met en lien **vol d’identité et immigration clandestine**. En effet, pratiquement **16% des délinquants de notre échantillon se sont livrés au vol d’identité afin de couvrir l’illégalité de leur statut face aux services de l’immigration**.

Si l’Internet n’est pas aussi utilisé que nous l’envisagions à l’étape de l’acquisition, ce média est en revanche un outil fort apprécié par les délinquants à l’étape de la fraude. Ainsi que nous le présentons dans le tableau 2, **plus de 45% des cas impliquent le recours à Internet**. La facilité – parfois déconcertante – avec laquelle les délinquants de notre échantillon ont été capables d’utiliser des données personnelles pour acheter directement des marchandises ou, pire encore, obtenir des lignes de crédit dénote un **réel problème de contrôle des transactions en ligne**. Dans certains cas, les renseignements nécessaires afin d’obtenir un compte bancaire se réduisaient au nom de famille, au prénom et à la date de naissance du client potentiel.

Tableau 2 : Utilisation de l’identité

	Nombre	Pourcentage
Achat de biens et de services (carte présente)	105	27,3%
Crédit en ligne	96	25%
Achat de biens et de services en ligne	78	20,3%
Retrait et virement d’espèces	44	11,5%
Immigration	61	15,9%

Les victimes

Les caractéristiques des victimes figurent parmi les informations les moins rapportées par les médias. Cela est principalement attribuable au fait que dans une grande partie des cas, l’affaire n’en était qu’à ses débuts et que la police menait toujours ses investigations. Ensuite, le vol d’identité est un délit dans lequel on trouve fort souvent un flou considérable en ce qui a trait à l’identité et au nombre de victimes, notamment en raison de leur réticence à communiquer avec la police.

Parmi les 135 affaires dans lesquelles il nous a été possible d'établir certaines caractéristiques des victimes, nous obtenons une **quasi-parité entre les hommes et les femmes** (respectivement 44 et 47, dans 34 affaires ayant fait plusieurs victimes, ces dernières étaient à la fois des hommes et des femmes).

Le vol d'identité est souvent présenté comme une menace de grande ampleur du fait du nombre important de victimes que peut entraîner le vol d'un seul fichier. Nos données ne corroborent pas cette intuition. Si la moyenne de notre échantillon se situe à 135 victimes par affaires, la médiane, elle, permet de constater que **dans plus de la moitié des cas (57%), il n'y a qu'une seule victime identifiée.** En outre, cette moyenne est à n'en pas douter très largement affectée par nos sources qui font état des victimes potentielles et non des victimes avérées (dans une minorité d'affaires, le vol d'identité portait sur des bases de données sur lesquelles figuraient effectivement des milliers de personnes mais nous n'avons pas été en mesure d'identifier des victimes réelles).

Dans un peu plus de 40% des 157 cas pour lesquels nous disposions de suffisamment d'informations, il existait un lien entre victimes et délinquants. Le principal lien qui unit victimes et délinquants est lié à l'emploi de ces derniers. En effet, nous avons rencontré un nombre conséquent de cas dans lesquels des professionnels ont abusé de leur position pour usurper l'identité de leurs clients (25% de l'ensemble des cas). Les occasions dans lesquelles des données sensibles sont communiquées sont légion. Nous avons ainsi retrouvé plusieurs cas de vol d'identité impliquant du personnel médical, des aidants, des vendeurs d'automobiles ou des banquiers qui avaient utilisé frauduleusement les données personnelles de leurs patients ou de leurs clients.

Les profits

Le montant médian des profits réalisés par les auteurs de vol d'identité est de 26.000 dollars US. Il existe une grande disparité dans les gains puisque, selon nos données, le minimum obtenu est de 500 dollars et le maximum de 50 millions de dollars. Si de telles sommes sortent de l'ordinaire, force est de constater qu'au vu des efforts relativement modérés que demande un vol d'identité et l'utilisation frauduleuse de celle-ci, il s'agit d'un **délit ayant un très haut rendement, ce qui le rend d'autant plus attrayant.**

Poursuites pénales et condamnations

Au moment de notre étude, sur les 422 individus impliqués, 22 étaient recherchés par les forces de l'ordre (5%), 286 étaient inculpés (68%) et 114 avaient été condamnés (27%). Contrairement à l'idée reçue selon laquelle les crimes contre les biens – et spécialement ceux qui font intervenir l'Internet – sont peu poursuivis ou faiblement sanctionnés, nous avons pu relever que **le taux de condamnation des personnes**

arrêtées et la peine prononcée sont importants. En effet, si l'on soustrait les 39 individus déclarés coupables et en attente d'un jugement sur sentence, seulement cinq individus ont bénéficié d'un sursis. Pour ceux qui ont été condamnés à une peine d'emprisonnement, la sévérité des peines peut surprendre. En effet, **la peine moyenne est de 54 mois de prison et la peine médiane de 40 mois** (peine minimum de 4 mois et maximum de 228 mois). En l'absence d'explications alternatives, on peut supputer que cette relative **sévérité se veut dissuasive et cherche à compenser le sentiment d'impunité** qui pourrait naître parmi les délinquants en raison du très faible taux d'élucidation des infractions par la police. Toutefois, et bien que notre faible échantillon nous interdise de généraliser, **il semble aussi que les affaires les plus complexes mais également les plus coûteuses aient été réglées par une peine assortie d'un sursis.** Dans de tels cas, les autorités auraient été contraintes à négocier avec les délinquants afin que ces derniers leurs fournissent des informations capitales sur le mode opératoire employé.

Conclusion

Comme nous avons pu le démontrer à travers cette étude exploratoire du profil des voleurs d'identité, l'image relayée par les médias de délinquants informatiques surdoués capables de pirater les bases de données des institutions financières et les ordinateurs des particuliers afin de s'emparer de l'identité de milliers, voire de millions, d'individus ne reflète que très imparfaitement la réalité connue des services de police. Même si plusieurs réseaux très structurés de fraudeurs comme ShadowCrew, The Grifters, Cardersmarket ou DarkMarket ont pu être démantelés au cours des dernières années (Symantec, 2008), **la grande majorité des affaires contenues dans notre base de données implique des individus agissant seuls, utilisant des moyens rudimentaires, et faisant un nombre relativement limité de victimes.**

Ce décalage peut être interprété de deux manières très différentes. D'une part, on pourrait imaginer que les personnes arrêtées par la police et condamnées par les tribunaux ne constituent que le groupe le moins performant des voleurs d'identité, et que par le biais d'un mécanisme de sélection naturelle, les délinquants les plus prolifiques et les plus sophistiqués arrivent à se soustraire à la justice. En d'autres mots, on pourrait faire l'hypothèse que les organisations policières se focalisent sur les cas les plus simples et les moins organisés, laissant les institutions financières et les particuliers assumer le fardeau d'une délinquance endémique « tolérée » comme le prix à payer d'un système financier basé sur l'accessibilité du crédit et la fluidité des transactions marchandes. Cette explication nous semble difficile à justifier empiriquement, notamment en raison des arrestations à répétition mentionnées au paragraphe précédent. D'autre part, une interprétation moins catastrophiste mettrait plutôt l'accent sur la **nature tout à fait ordinaire du vol d'identité**, qui ne fait que refléter la prolifération des marqueurs d'identité (numéros d'assurance sociale, numéros de cartes de crédit, mots de passe, etc.) pouvant être aisément convertis en espèces sonnantes et

trébuchantes par des délinquants s'adaptant au même titre que les autres membres de la société à l'omniprésence de l'Internet comme moyen privilégié de communication et de consommation. Dans cette seconde interprétation, le vol d'identité ne serait que la plus récente manifestation d'un long processus de co-évolution entre délinquance et technologie. Dans un tel contexte, et comme semble l'illustrer notre échantillon, la police se trouvera de plus en plus fréquemment confrontée à des **formes hybrides de délinquance** combinant des pratiques traditionnelles telles que le vol ou l'escroquerie à des stratégies exploitant les nombreuses vulnérabilités des systèmes de gestion de l'identité et des transactions financières. Par ailleurs, comme l'a aussi confirmé cette étude, **une proportion non négligeable de salariés et de professionnels viennent grossir les rangs des voleurs d'identité**, réagissant ainsi à une convergence de facteurs tels que l'accès privilégié à des bases de données regorgeant d'informations personnelles, la facilité de monnayer ces informations et la perception que les risques de se faire prendre sont relativement faibles.

Afin de pouvoir être prise en compte efficacement par les organisations policières et le système pénal, de telles évolutions nécessiteraient d'indispensables adaptations, aussi bien au stade de la conception des programmes de prévention qu'à celui de la détection des affaires ou de l'organisation des enquêtes.

Références

Allison, Stuart; Schuck, Amie et Kim Michelle Lersch (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, vol. 33, no. 1, pp. 19-29.

Baum, Katrina (2006). *Identity theft 2004: First estimates from the National crime victimization survey*. US Department of Justice Bureau of Justice Programs: Washington DC.

Berinato, Scott (2007). *Who's stealing your passwords? Global hackers create a new online crime economy*. CIO.com: 17 septembre. Accessible en ligne à: www.cio.com/article/135500.

Deloitte (2008). *A report on cybercrime in Canada*. Canadian Association of Police Board: Ottawa.

Copes, Heith et Lynne Vieraitis (2007). *Identity theft : Assessing offenders' strategies and perceptions of risk*. University of Alabama: Birmingham.

Dupont, Benoît (2008). *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*. Ministère de la Sécurité Publique : Québec.

Finklea, Kristin M. (2009). *Identity theft: Trends and Issues*. Congressional Research Service: Washington DC.

Gayer, Jennette (2003). *Policing privacy: Law enforcement's response to identity theft*. CALPIRG Education Fund: Los Angeles.

Gordon, Gary; Rebovitch, Donald; Choo, Kyung-Seok et Judith Gordon (2007). *Identity fraud trends and patterns: building a data-based foundation for proactive enforcement*. Center for Identity Management and Information Protection: Utica College.

Identity Theft Resource Center (ITRC) (2008). *Identity theft: The aftermath 2007*. ITRC: San Diego.

Institut pour la Sécurité de l'Information (ISIQ) (2007). *Sondage auprès des citoyens branchés*. CRIM : Montréal.

Kim, Rachel (2007). *2007 Identity fraud survey report – consumer version*. Javelin Strategy & Research: Pleasanton.

Newman, Graeme et Megan McNally (2005). *Identity theft literature review*. National Criminal Justice Reference Service: Washington DC.

Ohm, Paul (2008). The myth of the superuser: Fear, risk and harm online. *UC Davis Law Review*, vol. 41, no. 4, pp. 1327-1402.

Sproule, Susan et Norm Archer (2008). *Defining identity theft*. Eight World Congress on the Management of eBusiness, 11-13 juillet: Toronto.

Sproule, Susan et Norm Archer (2008). *Measuring identity theft in Canada: 2008 consumer survey*, MeRC working paper no. 23. McMaster University: Hamilton.

Symantec (2008). *Symantec report on the underground economy July 07 – June 08*. Symantec: Cupertino.

Synovate (2007). *Federal Trade Commission: 2006 identity theft survey report*. Synovate: McLean.

Thibodeau, Patrick (2008). *Credit card thieves ran a polite, professional help desk*. Computerworld: 6 août. Accessible en ligne à: <http://www.networkworld.com/news/2008/080708-credit-card-thieves-ran-a.html>.

Winterdyk, John et Nikki Thompson (2008). Student and non-student perceptions and awareness of identity theft. *Revue Canadienne de Criminologie et de Justice Pénale*, vol. 50, no. 2, pp. 153-186.