Chapitre 11
Escroqueries par Internet

Quentin Rossy[1]
Betina Borisova[1, 2]

RÉSUMÉ

Si les escroqueries commises à l'encontre de personnes sont séculaires, Internet a profondément transformé leur ampleur pour différentes raisons qui sont discutées dans ce chapitre. La diversité et la complexité intrinsèque des schémas de tromperie sont mises en perspective avec d'autres formes de criminalité en ligne. En effet, les escroqueries sont bien souvent associées à des activités de vol de données et d'identités, ainsi que de blanchiment des biens soustraits. Le cœur de la discussion porte sur la nature des activités frauduleuses, la manière de les analyser et de les classifier, ainsi que sur les enjeux liés à l'évaluation de leur ampleur. Un modèle d'analyse qui soutient la description et la classification des cas est présenté. Il repose sur la décomposition du phénomène au regard d'un script général en quatre étapes : (1) la prise de contact, (2) la mise en confiance, (3) la remise de bien et (4) le maintien d'un lien distant.

Mots clés : fraude ; escroquerie ; Internet ; script ; classification.

11.1 INTRODUCTION

Ce chapitre aborde les transformations induites par Internet sur les fraudes commises à l'encontre de personnes. Les fraudes visant des États ou des organisations ne sont pas abordées. Les objectifs principaux de la discussion sont d'établir la diversité et parfois la complexité des schémas d'escroquerie par Internet et de présenter des modèles utiles pour les reconnaître et les analyser. La réflexion porte sur la nature des activités, la manière de les analyser et de les classifier, ainsi que sur les enjeux liés à l'évaluation de leur ampleur. La dimension humaine du problème, tant du point de vue des auteurs que des victimes, de même que la question des approches de

1 École des sciences criminelles, Université de Lausanne, Suisse.
2 Service forensique, Police neuchâteloise, Suisse.

mitigation sont abordées succinctement tout au long de la discussion sans être développées en détail. Quelques questions liées à la nature des fraudes sont analysées. Quelles activités sont regroupées sous les termes de « fraudes » ou « escroqueries » ? Comment Internet les a-t-il transformées et dans quelles proportions ? Quelles relations les fraudes entretiennent-elles avec d'autres formes de criminalité numérique ? Quels sont les modèles d'analyse existants pour reconnaître, décrire, distinguer et classifier les fraudes ?

11.1.1 Arnaques, fraudes ou escroqueries ?

Les notions de fraude et d'escroquerie sont très largement utilisées comme synonymes pour décrire un ensemble d'activités diverses. Contrairement à d'autres formes de criminalité contre le patrimoine et sérielle, telles que les cambriolages, la fraude commise à l'encontre de personnes regroupe une très grande variété de comportements déviants parfois peu visibles et pas toujours considérés comme criminels. « Fraude » vient du latin *fraus* (nom de la déesse romaine de la tromperie, de l'astuce et de la ruse), qui signifie « erreur et provocation à l'erreur ». La notion fait référence à une très grande diversité de problèmes : fraude fiscale, fraude à la loi, fraude documentaire, fraude à la carte bancaire, etc. La fraude regroupe également un ensemble d'actes qui cause des torts patrimoniaux à autrui par la tromperie (Samet, 2007).

Le terme de « fraude» ne se rapporterait pas spécifiquement à un problème de droit criminel. Il engloberait également des actes de déviance contraires à des normes sociales formelles ou non. Les fraudes peuvent ainsi prendre de nombreuses autres étiquettes moins dérangeantes, telles que « combine », « faute professionnelle » ou « rupture de contrat», et ainsi ne pas être considérées comme de « réelles » infractions (Button et Tunley, 2015).

D'un côté, un acte de moindre importance est considéré comme une *arnaque*. Il réfère alors à un comportement déloyal ou contraire à des normes sociales et éthiques ; par exemple une affaire conclue à un prix surfait. Généralement, l'arnaque consiste à exiger d'une personne mal informée qu'elle verse un montant excessif pour un conseil, un crédit, un abonnement ou un objet de valeur nulle ou faible. Elle ne constitue pas toujours un acte illégal aux yeux de la loi.

De l'autre côté, des schémas d'escroquerie, parfois complexes, peuvent causer des préjudices colossaux impactant le commerce global. L'*escroquerie* consiste à « tromper une personne physique ou morale en la déterminant à remettre un bien quelconque grâce à une entreprise frauduleuse » (Samet, 2007, p. 651). Elle est définie en droit suisse, français, canadien et belge notamment. Contrairement aux situations d'arnaque, les victimes d'escroqueries n'ont pas forcément la possibilité de se rendre compte par elles-mêmes de la supercherie et de s'en protéger. Des arnaqueurs détroussent quelques devises par astuce, alors que des escrocs

peuvent détourner des millions, par la mise en œuvre de carrousels de TVA, par exemple. Ainsi, l'ampleur et la gravité de l'action distingueraient les comportements frauduleux selon une échelle continue de l'arnaque à l'escroquerie. Des définitions juridiques francophones de l'escroquerie ressortent des éléments constitutifs intéressants pour qualifier la nature de l'activité. En droit suisse, l'enrichissement illégitime est obtenu par une « astuce qui induit en erreur». En droit français et belge, le fait est caractérisé par l'usage de « faux noms », « fausses qualités » ou l'emploi de « manœuvres frauduleuses » pour tromper. La manœuvre frauduleuse fait référence à une mise en scène préparée à l'avance pour tromper (Samet, 2007). Le Code criminel canadien décrit la spécificité du comportement par le recours à un « faux semblant». Ainsi, l'astuce déployée par les auteurs pour tromper implique l'usage d'une fausse qualité qui prend typiquement la forme d'un faux rôle (par exemple, faux vendeur, faux employeur ou faux propriétaire).

L'escroquerie pourrait être considérée comme un type particulier de fraude. Néanmoins, les usages varient. La Convention de Budapest de 2001 sur la cybercriminalité[3] définit la fraude informatique et non l'escroquerie informatique, par exemple. En anglais, le terme *swindle* (escroquerie) semble bien moins souvent utilisé que *fraud*. Button et Cross (2017) proposent notamment de considérer l'ensemble des comportements selon une échelle allant de l'arnaque (*scam*) à la fraude (*fraud*). Ainsi, les deux termes ont des usages divers suivant les contextes et il convient probablement d'admettre un emploi relativement interchangeable entre les notions de fraude et d'escroquerie.

11.1.2 Des escroqueries « sur » ou « par » Internet ?

La numérisation des processus de communication, combinée au développement des interactions par Internet, a conduit à de profondes transformations des activités au sein des sociétés modernes. Ainsi, une part importante, probablement dominante, des fraudes sont mises en œuvre par Internet. Si les ordres de grandeur du phénomène ont changé, les fraudes ont néanmoins une dimension atemporelle. Dans l'Antiquité par exemple, les malversations pouvaient porter sur les quantités et les qualités de biens en circulation. Les boissons, telles que le vin, constituaient un objet de fraude, de même que d'autres marchandises prisées (épices, parfums, tissus, etc.) (Samet, 2007). Actuellement des dizaines, voire des centaines de milliers de sites Web diffusent des contrefaçons de tous types. Par ailleurs, un bon nombre d'escroqueries en ligne sont le miroir d'actes perpétrés depuis de très nombreuses années par courrier postal. À titre d'exemple, avant d'être globalisée par l'usage de courriels, la fraude à la commission était perpétrée sous forme de lettre manuscrite (Buchanan et Grant, 2001 ;

3 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156d

Holt et Graves, 2007). Les cas les plus anciens documentés, tels que les cas dits du « prisonnier espagnol », remontent même au Moyen Âge. Un schéma analogue se retrouve dans les lettres de Jérusalem décrites par Vidocq à la fin du dix-huitième siècle. Ainsi, selon la typologie proposée par Wall (2005/2010), les fraudes exploitent les technologies comme moyen de développement d'opportunités (*crime using the machine*/*computer-assisted crime*). Le dispositif informatique n'est pas la cible, mais un outil au service de la réalisation de l'infraction (Alkaabi, Mohay, McCullagh et Chantler, 2010). Elles sont des infractions activées par Internet (*cyber-enabled crime*) et non dépendantes de son usage *(cyber-dependant crime*), selon la classification de McGuire et Dowling (2013).

S'il est plus fréquent de parler d'une escroquerie « sur » Internet que « par » Internet, la préposition « sur » renvoie néanmoins à une ambiguïté très commune. En effet, Internet est trop souvent confondu avec les espaces virtuels qui constituent le Web et qui sont accessibles par les navigateurs de nos ordinateurs, tablettes ou téléphones intelligents. Par exemple, le terme « site Internet » est très souvent utilisé pour décrire des espaces virtuels spécifiques du Web. Internet est un réseau, constitué à la fois d'une dimension physique (câbles et ondes) et d'une dimension logicielle (le protocole IP et des protocoles de transport de données), sur lequel des processus de communication sont mis en œuvre. Le Web n'est que l'une des nombreuses applications exploitées par le réseau Internet. Il forme un espace de partage de ressources (d'un texte, d'une image, d'une vidéo ou d'un fichier audio) localisées par des adresses URL (*Uniform Ressource Locator*) et rendues accessibles par des navigateurs. Ces ressources sont généralement intégrées dans des pages Web regroupées en sites Web localisés par leurs noms de domaine. Les courriels, les applications de messagerie instantanée et de partages de fichiers forment d'autres modes de communication reposant sur l'infrastructure d'Internet.

Ainsi, l'escroquerie ou la fraude en ligne doit être comprise comme un acte de tromperie qui conduit une victime, contactée par le réseau Internet dans un espace virtuel, à remettre un bien en profitant d'une fausse qualité ou d'une mise en scène mensongère. Le bien peut être directement de l'argent, mais également des données ou des produits.

11.2 ÉTENDUE DU PHÉNOMÈNE

11.2.1 Défis statistiques

Depuis plusieurs dizaines d'années, de nombreux pays industrialisés sont témoins d'une baisse des statistiques de leur criminalité. Selon certains criminologues (Farrell, Tseloni, Mailley et Tilley, 2011), ce déclin serait imputable à des changements économiques et sociaux, ou encore à une multiplication de mesures sécuritaires et de prévention ayant contribué à limiter les opportunités criminelles. Pour d'autres, la hausse des

dénonciations de crimes et délits par Internet serait le signe d'un changement profond, ayant transformé les comportements et opportunités criminels (Button et Cross, 2017 ; Caneppele et Aebi, 2017 ; Levi, 2017). En France, par exemple, presque les deux tiers des ménages victimes de fraudes (59 des effectifs cumulés entre 2009 et 2012) le sont par Internet (Benbouzid et Peaucellier, 2016). Ainsi, mesurer la prévalence de la criminalité en ligne, et en particulier des fraudes, est devenu un enjeu majeur (Côté, Bérubé et Dupont, 2016).

En 2004, Burns, Whitworth et Thompson (2004) ont réalisé une enquête auprès des 700 départements de police américains sur leur perception de la fraude par Internet. Plus de la moitié des agents de police (76,5) ayant pris part à l'étude considéraient que leur département et, plus généralement, les forces de l'ordre ne reconnaissent pas la fraude comme un problème d'importance. En effet, pendant longtemps, l'escroquerie en ligne a été marginalisée des statistiques officielles, faute de définition standardisée. La situation ne semble pas avoir beaucoup changé depuis (Button et Tunley, 2015 ; Dupont, 2016).

Ainsi, un délit financier commis par le biais d'Internet et rapporté aux autorités a encore de fortes chances d'être enregistré comme une infraction contre le patrimoine dite « traditionnelle » et non pas comme un délit numérique (CIPC, 2018). À titre d'exemple, un indicateur de mesure de la délinquance a été développé par le Federal Bureau of Investigation (FBI) – le *National Incident-Based Reporting System* (NIBRS) – pour permettre aux agences de préciser si le prévenu est suspecté d'avoir utilisé un ordinateur pour la commission de l'infraction, discriminant les actes perpétrés dans un espace virtuel de ceux pour lesquels l'ordinateur n'a été qu'un moyen pour arriver à ses fins. Néanmoins, les crimes commis par le biais d'Internet ne font pas partie des 40 catégories d'infractions prévues, si bien qu'ils doivent être reclassés par les opérateurs dans une des catégories préexistantes (Holt et Bossler, 2016). D'autres organismes recensent également des statistiques spécifiques à la fraude en ligne. C'est le cas aux États-Unis du Consumer Sentinel Network, un réseau d'échange d'information mis en place par la Commission fédérale du commerce. Les statistiques annuelles publiées par cet organisme sont basées sur des plaintes pour fraude enregistrées par une variété d'organismes policiers et judiciaires ainsi que par les services postaux. Entre 2,5 et 3 millions de fraudes et vols d'identités ont été recensés annuellement entre 2014 et 2017 pour une population d'environ 300 millions d'habitants. Environ 40 % des cas sont des fraudes et une perte financière médiane d'environ 400 $ US est relevée dans 20 d'entre eux (FDC, 2018).

Les défis ne se limitent néanmoins pas aux données policières. Les sondages de victimisation n'incluaient jusqu'à récemment que peu, voire pas du tout, de questions sur la victimisation de fraudes en ligne. Le National Crime Victimization Survey (NCVS) américain a, pendant longtemps,

ignoré la criminalité en ligne dans son instrument principal de mesure. Depuis 2004, il intègre des questions relatives à la prévalence du vol d'identité. Une recherche publiée en 2011 révèle que la proportion de ménages victimes de vol d'identité est passée de 5,5 en 2005 à 7 en 2010 (Langton, 2011). Ainsi, le NCVS a développé des études supplémentaires, périodiquement mises à jour, pour collecter des données sur le harcèlement en ligne (Nobles, Reyns, Fox et Fisher, 2014) et le vol de données (Holt et Bossler, 2016). En 2016, 10 des résidents américains disaient avoir été victimes de vol d'identité en ligne et 5 , d'une utilisation abusive de carte de crédit (Harrell, 2019). En Australie, l'Australian Bureau of Statistics entreprend régulièrement des sondages de prévalence de la victimisation de fraude. Le rapport 2016 révèle que dans les 12 mois précédant le sondage, 50 de la population âgée de 15 ans et plus avait été exposée à des fraudes en ligne ; 2,4 a déclaré avoir été victime au moins une fois d'un vol de données ou d'argent, contre 2,9 sur la période 2010-2011 (ABS, 2016).

En 2016, les fraudes par Internet et l'utilisation frauduleuse d'ordinateur sont intégrées dans le *Crime Survey* britannique. En sus des 6,3 millions déjà répertoriées, l'adjonction de ces deux nouvelles catégories a permis le recensement de 5,8 millions de nouvelles infractions. Sont alors recensées 2,6 millions de victimes de fraude avec perte financière et 2,4 millions de victimes de fraude n'ayant pas subi de pertes (tentatives) (ONS, 2016). En 2018, la tendance se confirme : 54 des incidents de fraude recensés par le sondage ont été perpétrés par le biais des technologies de l'information et de communication (soit 1,8 million d'incidents) (ONS, 2018).

Une étude récente de Reep-van den Bergh et Junger (2018) fait la synthèse de neuf sondages européens et conclut que la fraude en ligne touche entre 3 et 6 de la population. C'est de 1 à 3 des fraudes qui auraient lieu dans le commerce en ligne, 1 à 2 qui seraient liées à des opérations bancaires par Internet alors qu'environ 1 de la population serait victime d'autres types de fraudes, telles que les fraudes à la commission.

11.2.2 Faible taux de signalement des cas

Les données de victimisation révèlent globalement des taux de signalement à la police faibles, bien que la France semble faire figure d'exception (Benbouzid et Peaucellier, 2016). Les résultats du *Crime Survey* britannique de 2018 suggèrent, par exemple, que seulement 1 incident sur 8 (soit 13) a été rapporté aux autorités compétentes (ONS, 2018). Les raisons pouvant expliquer ces sous-estimations sont multiples (Holt et Bossler, 2016 ; Button et Cross, 2017). Premièrement, la victime doit avoir détecté la fraude. Elle peut parfois passer inaperçue, ne pas être reconnue ou admise comme telle. Deuxièmement, la décision de signaler le cas peut être subordonnée à l'importance du préjudice subi. En effet, si la somme dérobée est minimale, le lésé pourrait renoncer à porter plainte. Le manque de confiance en la police, en particulier en ses compétences pour traiter

effectivement les cas, pourrait également expliquer un faible taux de signalement. Ainsi, n'étant pas dans l'obligation de porter plainte, la victime serait réticente à dénoncer son cas. Parfois, elle ne trouve simplement pas le bon interlocuteur pour prendre sa plainte (Whitty, 2015b ; Cross, 2018). Finalement, certaines escroqueries peuvent mettre les victimes dans des situations de dépendance et de honte les conduisant à renoncer au signalement, d'autant plus que les fraudes et vols d'identité sont typiquement des infractions où la faute peut être imputée à la naïveté de la victime (Button et Cross, 2017 ; Button, Lewis et Tapley, 2014 ; Button et Tunley, 2015 ; Cross, Richards et Smith, 2016 ; Whitty, 2015b).

11.2.3 Plateformes de signalement en ligne : une nouvelle panacée ?

Bien que les taux de signalement à la police semblent encore relativement limités, des mécanismes de dénonciation en ligne se généralisent dans plusieurs pays du monde. Les sources de statistiques pourraient donc tendre à se développer. Bien que les types de cas intégrés varient, ils complètent utilement les chiffres produits par les sociétés commerciales impliquées dans le marché de la sécurité informatique qui sont entachés de biais et conflits d'intérêts majeurs (Dupont, 2016). Europol référence par exemple une vingtaine de sites pour les pays européens[4]. Aux États-Unis, l'Internet Crime Complaint Center (IC3) est un mécanisme de dénonciation central fondé conjointement par trois agences fédérales (le FBI, le National White Collar Crime Center [NWC3] et le Bureau of Justice Assistance). Le centre sert de structure de coordination dans la gestion des plaintes relatives aux crimes en ligne (Holt et Bossler, 2016).

De telles plateformes pourraient devenir des sources valides de données lorsque leurs existences seront bien connues des citoyens et que les victimes prendront l'habitude de les utiliser pour dénoncer les cas. Néanmoins, si la création de ces plateformes semble être un moyen intéressant pour diminuer le chiffre noir, leur démultiplication pourrait nuire à la vision d'ensemble (Cross, 2018). En France, par exemple, deux plateformes différentes ont été développées : PHAROS pour le signalement de contenus illicites et PERCEVAL pour les fraudes ayant conduit à des retraits frauduleux. De surcroît, les victimes d'un courriel indésirable sont invitées à rapporter leur cas sur le site signal-spam.fr. En effet, les autorités policières ne sont plus les seuls organismes qui relèvent les cas d'escroquerie en ligne. Les victimes peuvent parfois signaler un incident auprès d'organismes indépendants. En Australie, l'Australian Competition and Consumer Commission (ACCC) a développé la plateforme scamwatch.gov.au. Durant l'année 2017, 161 500 cas de fraudes, hameçonnages et autres vols d'identité ont été colligés pour une population d'environ 24,6 millions

4 https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

d'habitants (ACCC, 2018). Les autorités policières australiennes ont quant à elles mis en ligne une plateforme de signalement, l'Australian Cybercrime Online Reporting Network[5] (ACORN), qui recense 13 687 cas de crime en ligne, dont 52 de fraudes entre avril et juin 2018. Les données de l'ACCC montrent une image différente pour la même période, puisque 40 615 cas de fraude sont recensés. En Suisse, un formulaire de signalement est présent sur le site Web de la police fédérale, ainsi que sur le site de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Ce dernier renvoie les victimes vers les polices cantonales pour le dépôt de plainte. Un guichet en ligne a également été développé (suisse-epolice.ch). Il est décrit comme un « poste de police virtuel », mais il n'intègre pas les crimes en ligne. Une part importante de ces plateformes ne diffuse pas régulièrement leurs statistiques. Paradoxalement, cette prolifération d'initiatives pourrait ainsi tendre à complexifier la mesure du phénomène si des mesures d'intégration ne sont pas mises en œuvre, les victimes ne sachant plus vers quel organisme se tourner pour dénoncer les cas (Cross, 2018).

Globalement, mesurer l'ampleur des escroqueries en ligne demeure une gageure. Les sondages de victimisation semblent indiquer un taux de victimisation oscillant entre 3 et 6 de la population. Une part mineure des cas, probablement de l'ordre de 10 à 15 , est reportée aux autorités. Le développement de plateformes en ligne pour signaler les infractions pourrait conduire à une image plus complète du phénomène, mais il resterait encore à faire une mise en perspective des données colligées.

De plus, la diversité des modèles existants pour reconnaître, décrire et classifier les fraudes affecte tant les estimations de la prévalence, les comparaisons internationales, que la compréhension des modes opératoires et leurs conséquences. Une meilleure formalisation des types de fraudes est ainsi nécessaire, en particulier lorsqu'il s'agit de définir des stratégies de mitigation adéquates (Alkaabi *et al.*, 2010 ; Beals, DeLiema et Deevy, 2015 ; Reep-van den Bergh et Junger, 2018).

11.3 PORTRAIT DES ESCROQUERIES

11.3.1 Complexité et intrication des activités en ligne

La description et la classification des différents types de fraudes ont fait l'objet de nombreuses propositions fondées sur des dimensions très différentes. Les fraudes sont parfois catégorisées en fonction du moyen de communication exploité par les auteurs (ex. : fraudes en ligne, par courrier, par téléphone), en fonction du choix des victimes (ex. : fraudes de masse, fraudes ciblées), en fonction du type de victimes (ex. : fraudes contre les États, les entreprises, les particuliers), en fonction des stratégies de remise

5 https://www.acorn.gov.au/about-acorn

de bien (ex. : fraudes à l'avance de frais, fraudes aux surpaiements, hameçonnage), ou encore en fonction du type de bien recherché (ex. : fraudes financières, vol des données bancaires, vol d'identité) (Button, Lewis et Tapley, 2009 ; Beals *et al.*, 2015). Certaines typologies intègrent plusieurs dimensions, comme la classification de Wall (2007) qui distingue les fraudes tant sur le type de cibles, les modes de remise de bien et les types d'espace virtuel.

De surcroît, le vol d'identité, le piratage et l'hameçonnage sont des comportements souvent mis en perspective de schémas d'escroqueries comme infractions connexes, sans toutefois expliciter clairement leurs relations (Holt et Graves, 2007 ; Levi, 2008 ; Whitty, 2015b). En effet, les modes opératoires développés par les auteurs impliquent une succession d'étapes qui laissent entrevoir l'intégration d'activités criminelles diverses dans un tout parfois difficile à détecter et à reconstruire. Comprendre l'ensemble de l'activité est essentiel pour reconnaître et distinguer les types de cas, mettre en œuvre des dispositifs de suivi et établir des mesures de mitigation adéquates, qu'elles soient répressives ou préventives. Afin de mieux situer l'enjeu de l'*intrication des activités*, prenons l'exemple de la fraude à la demande de soutien décrite dans le paragraphe qui suit.

Par l'envoi de courriels d'appel à l'aide, le fraudeur endosse la fausse qualité d'un proche de la victime pour lui soutirer de l'argent en prétextant une situation d'urgence, typiquement pendant un voyage à l'étranger durant duquel il aurait prétendument perdu son argent et ses documents de voyage. Il demande alors un virement d'argent par un service de transfert de fonds international. Pour réaliser une telle escroquerie, l'escroc doit voler l'identité d'un proche de la victime. Une méthode classique consiste à exploiter directement le compte courriel d'une autre victime en envoyant le message frauduleux à l'ensemble de ses contacts. Ainsi le schéma de fraude implique une étape initiale de vol des informations d'accès à des boîtes courriel. Le vol d'identité peut être commis par le piratage d'ordinateurs avec un logiciel malveillant ou par hameçonnage (*phishing*) qui conduit les victimes à transmettre leurs données sur des sites contrefaits. Le piratage de téléphone mobile permet également aux fraudeurs de contacter les victimes par messagerie instantanée.

Dans cet exemple, la fraude implique une chaîne d'activités individuellement reconnues comme des infractions, comme l'hameçonnage et le piratage conduisant à des vols de données. En aval de l'escroquerie, des activités de blanchiment peuvent également être mises en œuvre. Si elles sont détectées par la police, le lien avec le schéma d'escroquerie initial n'est pas toujours facilement établi. L'activité de blanchiment peut porter directement sur le produit financier. Dans ce cas, des passeurs d'argent ou mules financières (*money mule*) transfèrent, via leur compte personnel, les gains liés à l'escroquerie. Dans d'autres cas, les biens achetés avec des données volées sont transférés par l'intermédiaire de passeurs de paquets

(*package mule*). En l'occurrence, ces activités de blanchiment sont bien souvent commises par des personnes ayant répondu à des annonces frauduleuses d'offre d'emploi (*job opportunity scam*). Les escrocs publient en effet des annonces en adoptant la fausse qualité de sociétés crédibles et sollicitent ensuite les personnes pour des activités de passeurs contre une commission. Au passage, leurs données personnelles peuvent être volées pour commettre d'autres fraudes. Décrire et classifier les escroqueries implique de reconnaître qu'elles peuvent être formées d'une succession d'étapes parfois complexes. Si chacune d'elles est considérée individuellement comme un cas distinct, les chances de reconstruire l'activité globale sont minimes.

11.3.2 Vers une réorganisation des auteurs de fraudes ?

L'intrication des activités de piratage, de vol de données, de mise en œuvre de schémas de tromperie et de blanchiment soulève des questions sur le niveau d'organisation des acteurs (Leukfeldt, Kleemans et Stol, 2017). Internet semble en effet avoir reconfiguré les interactions entre les criminels qui peuvent se rencontrer virtuellement dans des *espaces de convergence* en ligne, tels que des forums, et ainsi partager, échanger et vendre leurs services (Soudijn et Zegers, 2012). L'activité criminelle devient un service (*crime-as-a-service*) mis à disposition d'autres criminels (Sood et Enbody, 2013). Les pirates informatiques disposent de compétences techniques pour voler des données, puis les vendent à des fraudeurs capables de les monétiser (Dupont, 2013). Ces derniers exploitent finalement des passeurs afin de transférer les biens et de blanchir les produits financiers. Une telle succession se retrouve typiquement dans le schéma de fraudes au commerce de biens en ligne connu sous le nom de *triangulation*, où l'escroc vend à prix cassé sur un site un bien qu'il aura acheté avec des données volées sur un site légitime (Gregg et Scott, 2008).

Ainsi, l'interconnexion globalisée des technologies numériques par le réseau Internet a grandement facilité les activités transnationales des auteurs de fraudes (Grabosky, 2004 ; Levi, 2008). Ces derniers peuvent prendre contact avec un nombre croissant de victimes potentielles, profiter des services d'autres criminels pour mener à bien leurs schémas de fraudes et tabler sur les difficultés des systèmes policiers et judiciaires à s'organiser pour traiter les cas. Certains types de fraudes demeurent néanmoins très fréquemment associés à des régions précises du monde. Par exemple, le Nigéria, et plus récemment les pays de l'Afrique de l'Ouest, ont été associés aux fraudes à l'avance de frais (Bogui, 2010 ; Button et Cross, 2017 ; Edwards *et al.*, 2018 ; Park, Jones, McCoy, Shi et Jakobsson, 2014). D'autres régions du monde sont également souvent associées à des crimes en ligne. Les cas d'hameçonnage sont typiquement liés à des groupes criminels en provenance de l'Europe de l'Est, notamment la Russie, la Lituanie et la Roumanie (Levi, 2008). Bien que l'origine des auteurs puisse être bien plus diverse, l'association entre certains types de fraudes et des

régions du monde a des effets stigmatisants (Bogui, 2010). Edwards et ses collègues (2018) soulignent que, si une part importante d'auteurs de fraudes aux sentiments semble provenir des pays de l'Afrique subsaharienne, la Malaisie et l'Afrique du Sud réunissent une part non négligeable d'auteurs de fraudes (près de 20). Globalement, le niveau d'organisation des auteurs de fraudes, leur origine géographique et la proportion de réseaux transnationaux restent des questions ouvertes.

11.3.3 Script et types des fraudes

Afin de décrire les schémas d'escroquerie dans un tel contexte, une approche par script est proposée pour mieux cerner et situer la diversité des modes opératoires développés par les auteurs de fraudes. Un script est un modèle d'analyse qui formalise la séquence des étapes entreprises avant, pendant et après une activité criminelle (Cornish, 1994). Une telle approche a notamment été proposée par Levi (2008) pour décrire les interactions dans les réseaux de fraudeurs, par Whitty (2015a) pour décrire les fraudes aux sentiments, ainsi que par Choi, Lee et Chun (2017) pour les fraudes par téléphone.

Le modèle d'analyse des escroqueries proposé ici repose sur la décomposition du phénomène au regard d'un script général en quatre étapes : (1) la prise de contact, (2) la mise en confiance, (3) la remise de bien, et (4) le maintien d'un lien distant. Plusieurs typologies de comportements peuvent alors être mises en perspective à chacune des étapes. Ce script porte sur l'escroquerie en elle-même, qui se combine parfois avec des activités de vol de données en amont et des activités de blanchiment en aval, qui ne sont pas détaillées.

Prise de contact. La première étape consiste pour l'escroc à trouver des proies potentielles et à prendre contact avec elles. Internet devient alors le vecteur de la rencontre entre le fraudeur et la victime en tant que gardien de la cible convoitée (son argent, ses données). La rencontre, virtualisée, évite les contacts physiques, sources potentielles de risques, rend les déplacements inutiles, ce qui limite les efforts, s'abstrait de limites spatiales devenues redimensionnables, car virtuelles, et étend ainsi le nombre d'opportunités et les gains potentiels. Internet permet des contacts indirects (par le biais d'avatars) et asynchrones qui facilitent le maintien d'un lien distant, ainsi que l'anonymat en cas de détection. La prise de contact peut se faire à travers divers canaux de télécommunication : par messagerie instantanée, par téléphone, dans un réseau social, par courriel.

Divers espaces de rencontre virtuels sont en effet exploités par les fraudeurs avec des approches de plusieurs genres, et le mode d'exposition en ligne semble façonner la structure des opportunités (Pratt, Holtfreter et Reisig, 2010). Par analogie au modèle des triangles de mobilité, initialement proposé par Burgess (1925), la rencontre virtuelle peut se conceptualiser en trois types: la *convergence*, l'*intrusion* et l'*hameçonnage*. Chacun fait

référence à des modes de rencontre impliquant des déplacements virtuels entre les espaces virtuels de l'auteur de la fraude, de la victime ou d'un tiers. D'abord, lors d'une convergence, l'auteur de la fraude et le gardien (la victime) se rencontrent dans un espace tiers d'activités routinières en ligne. Les fraudes sont commises sur des plateformes en ligne comme les sites de petites annonces, de ventes, de jeux ou de rencontres amoureuses. Parmi ces espaces de convergence, les espaces de vente de produits illicites sont particulièrement touchés par les fraudes. En effet, les victimes ne vont pas dénoncer une fraude pour une transaction commerciale elle-même initialement frauduleuse. Ensuite, lors d'une intrusion, l'auteur de la fraude intègre directement l'espace dédié du gardien. Les fraudes par faux services de support informatique appartiennent à cette catégorie. En effet, les auteurs de fraudes obtiennent l'accès à l'ordinateur de la victime par tromperie. Enfin, dans les cas d'hameçonnage, le gardien abusé transmet ses données dans l'espace dédié de l'auteur, typiquement par le biais d'un faux site d'une société de services (ex. : une banque) ou un faux magasin en ligne.

Pour déployer leurs scénarios frauduleux, les auteurs de fraudes vont également faire le choix de cibler des proies spécifiques ou au contraire d'atteindre un maximum de victimes non profilées à priori. Les fraudes sont dites « ciblées » (*targeted fraud*) ou « de masse » (*mass-marketing fraud*) (Whitty, 2015b). Les fraudes ciblées impliquent de réunir des informations personnelles sur la victime afin de déployer un scénario trompeur spécifiquement adapté à la situation de la personne. Tel est le cas, par exemple, des fraudes au président. Il s'agit de fraudes où l'escroc vole l'identité d'un patron d'entreprise pour tromper un employé (ciblé) et l'amener à verser une forte somme d'argent sur un compte sous prétexte d'une affaire commerciale urgente et importante, par exemple. Dans les cas de fraudes aux sentiments, les auteurs vont prendre contact avec des célibataires potentiellement en manque de compagnie pour les escroquer. Dans le cas des fausses loteries, en revanche, des courriels sont envoyés à un maximum de personnes dans l'espoir que certaines répondront à la tromperie. En général, le contact de masse conduit à une accumulation de gains de faible importance, souvent inférieurs à mille francs/euros/dollars, alors que les contacts ciblés peuvent mener à des gains substantiels de plusieurs dizaines, voire centaines de milliers de francs/euros/dollars. Pour Jakobsson (2016), la frontière entre escroqueries ciblées et de masse est relativement floue. D'une part, les courriels de masse pourraient être volontairement mal écrits pour cibler les plus naïfs. D'autre part, certains schémas de fraudes peuvent être mis en œuvre de façon ciblée ou non (comme l'hameçonnage) ou concerner des groupes d'individus caractéristiques (en recherche d'emploi, de logement, etc.). Globalement, l'évolution des modes opératoires tend vers un ciblage accru (Jakobsson, 2016). En effet, les schémas de fraudes ciblées semblent générer les profits les plus élevés. L'Australian Competition and Consumer Commission (2018) relève, pour l'année 2017, que les fraudes aux sentiments sont responsables de plus de 40 millions de

dollars de perte, alors que l'hameçonnage, le vol d'identité et les fausses factures, qui sont les crimes les plus souvent rapportés, auraient généré un profit de 4,7 millions de dollars canadiens.

Mise en confiance. L'étape de mise en confiance ou le « jeu de confiance » (*confidence game*) constitue le cœur de toute escroquerie. Elle repose sur la capacité du fraudeur à induire la victime en erreur, à user de persuasion pour la tromper et l'amener dans un second temps à lui remettre de l'argent ou un bien. Popularisé par la nouvelle de Hermann Melville *The Confidence-Man: His Masquerade* publiée en 1857, le terme d'artiste de la confiance (*confidence*/*con artist*) est parfois utilisé pour décrire les auteurs de ce type de fraude, tant la tromperie peut relever d'une ingénieuse, voire artistique mise en scène trompeuse. Le terme remonte, en fait, à la manchette du *New York Herald* du 8 juillet 1949, « Arrest of the Confidence Man», qui référait à William Thompson, arrêté le 7 juillet à New York (Bergmann, 1969), et qui fut reprise quelques semaines plus tard par *The National Police Gazette* sous le terme *confidence game*. Thompson, adoptant la fausse qualité d'une ancienne connaissance, appréhendait des passants dans la rue qui n'arrivaient évidemment pas à se souvenir de lui, et obtenait qu'ils lui donnent leur montre ou de l'argent. Si Thompson n'est pas le premier escroc de ce type, la notion de confiance lui est associée en raison de la phrase qu'il disait à ses victimes : « Have you confidence in me to trust me with your watch until tomorrow? » Le cas de Thompson a été rendu célèbre par sa couverture médiatique de l'époque et l'ironie de la situation : un « petit arnaqueur» avait volé quelques montres à des financiers de Wall Street, escroquant potentiellement des millions (en réalité, le profil des victimes était plus large). La simplicité et la faible portée du mode opératoire de Thompson cachent une variété d'autres modes opératoires parfois beaucoup plus sophistiqués. Le *confidence man* demandait la confiance, là où d'autres créent des situations de confiance (Braucher et Orbach, 2015).

Le jeu de confiance repose sur la capacité du fraudeur à placer sa victime dans une situation de mauvaise prise de décision en induisant des biais cognitifs, émotionnels ou moraux (Lea, Fischer et Evans, 2009 ; Whitty, 2013 ; Braucher et Orbach, 2015 ; Kahneman 2011). Les fraudeurs adoptent une fausse qualité pour créer une situation de confiance (un proche, un partenaire commercial), de peur induite par une figure d'autorité (un patron, la police, etc.), et/ou d'engagement lié à des valeurs (devoir une faveur, rendre service, faire un don, appartenir à une communauté, adopter un courant de pensée). La fraude repose ainsi sur des vulnérabilités particulières qui peuvent être très diverses (Holtfreter, Reisig et Pratt, 2008). Les escrocs exploitent les difficultés (financières, amoureuses), les attentes (cupidité, avarice), la peur et les croyances (valeurs, mythes) des victimes pour arriver à leur fin. De surcroît, l'escroc va bien souvent placer la victime dans une apparente situation d'urgence et va user de pression pour l'empêcher de prendre une décision raisonnée (Atkins et Huang, 2013 ; Braucher et Orbach, 2015).

La diversité des situations possibles rend la classification des scénarios très complexe. Beals, DeLiema et Deevy (2015) décrivent une liste impressionnante de scénarios qui sont classifiés au regard du bénéfice attendu par la victime de la fraude. Les schémas de fraudes se distingueraient alors en fonction de vulnérabilités particulières des gardiens (les victimes) sur lesquelles les auteurs « jouent » pour établir une relation de confiance par l'usage de fausses qualités spécifiques. Le tableau 11.1 résume les types de fraudes et en donne quelques exemples fréquents.

Tableau 11.1 Typologie des escroqueries par Internet selon le type de bénéfice attendu par la victime

Types de fraudes	**Bénéfice attendu (vulnérabilité)**	**Fausse qualité**	**Description**
Fraudes à l'investissement	Rendement financier (cupidité, appât du gain)	Faux investissement	Fausses promesses de rendements financiers élevés en échange d'investissements. Les fraudes varient en fonction du contexte de prise de contact (faux courtier, faux paris sportifs, faux logiciel de placements, etc.).
Fraudes au gain d'argent	Gain d'argent (cupidité, appât du gain)	Fausse loterie	Faux gain de loterie ou faux concours (pour un voyage, par exemple).
		Fausse commission	Fausse commission sur un gain important selon différents scénarios : héritage, orphelin, réfugié, décès d'un riche client, recherche de partenaire commercial, etc.
Fraudes au commerce de biens	Transaction commerciale (avarice, rapacité ou besoin financier)	Faux produit	Vente de produits contrefaits ou sans valeur.
		Faux vendeur	Vente de produits inexistants, ainsi que des animaux, des organes, etc. La fraude peut prendre la forme de fausses annonces sur des plateformes de commerce en ligne ou de faux magasins en ligne.
		Faux acheteur	Faux achat conduisant à de fausses confirmations de paiements et parfois à des avances de frais pour débloquer le paiement.
		Triangulation	Revente d'un produit acheté sur un autre espace avec des données bancaires volées.

Tableau 11.1 Typologie des escroqueries par Internet selon le type de bénéfice attendu par la victime

Fraudes au commerce de services	Service (crédulité, ignorance, situation précaire)	Faux service	Accord pour un service qui implique des offres trompeuses ou qui n'est pas fourni du tout : inscription dans un registre commercial, assurances, vacances, aide à l'immigration, adoption, fausses croyances (bonne fortune, malédiction, etc.).
	Prêt d'argent (difficulté financière)	Faux prêt	Également nommé « prêt à l'avance de frais », fausses offres de prêts ou de bourses d'études.
	Logement (difficulté à en trouver)	Fausse location	Les fraudes à la location sont de deux types. Elles visent, d'une part, les personnes habitant dans des zones particulièrement touchées par la pénurie de logements, d'autre part, sur les locations de vacances.
Fraudes à l'emploi	Emploi (difficulté à en trouver)	Faux emploi	Fausses opportunités de travail qui nécessitent peu de compétences ou de qualifications, mais prétendent fournir des récompenses financières supérieures à la moyenne. La fraude conduit à une activité illégale de blanchiment pour la victime.
Fraudes aux sentiments	Compagnie et bonheur (solitude et vide affectif)	Fausse romance	Fausse histoire d'amour pour obtenir de l'argent en prétextant des difficultés ou une situation d'urgence une fois la confiance établie.
Fraudes à la demande de soutien	Satisfaction d'avoir aidé (compassion, amitié)	Fausse charité	Usurpation de l'identité d'une association caritative ou fausse association créée pour détourner des dons.
		Faux ami	Souvent par usurpation de l'identité d'un proche, fausse demande d'aide d'une connaissance en situation difficile à l'étranger et sans ressources.

Tableau 11.1 Typologie des escroqueries par Internet selon le type de bénéfice attendu par la victime

Fraudes à l'autorité	Évitement d'un problème/tort potentiel (peur de l'autorité)	Fausse facture ou dette	Fausse facture/dette non payée avec menace de frais.
		Faux problème de sécurité/technique	Usurpation de l'identité d'un service d'assistance technique pour résoudre un problème de sécurité sur la machine du lésé.
		Fausse infraction	Fausse amende pour une infraction en ligne, par l'usurpation de l'identité d'une autorité.
		Faux partenaire commercial	Usurpation de l'identité d'un partenaire commercial pour changer le destinataire d'une facture.
		Faux patron	Faux patron demandant un virement bancaire en prétextant une affaire commerciale urgente.

Source : Adapté de Beals *et al.*, 2015.

Remise de biens. En règle générale, la fraude a pour cible l'argent de la victime, mais dans certains cas, les escrocs profitent de la situation de confiance pour dérober des informations personnelles qu'ils pourront exploiter dans d'autres scénarios de fraudes, par exemple, ou voler des coordonnées bancaires avec lesquelles ils réaliseront des achats ou des virements. Si le mode opératoire de remise de bien varie en fonction du scénario de confiance exploité par l'auteur de la fraude, des stratégies transversales peuvent être identifiées. Au moins trois types généraux sont exploités par les escrocs : (1) les remises de bien délibérées, (2) à l'insu de la victime ou (3) par l'usage d'un moyen de contrainte. Les techniques sont multiples et peuvent se combiner selon des séquences qui vont débuter par une mise en confiance amenant le lésé à transmettre délibérément de l'argent et finir par des menaces conduisant à des extorsions.

La majeure partie des fraudes repose sur une stratégie de remise des biens consciente de la part des victimes qui pensent obtenir un bénéfice en retour (le bien ou le service prévu). Le mode opératoire principal exploité par les escrocs est celui de l'*avance de frais*. Le fraudeur demande de l'argent au lésé prétextant des frais avant de pouvoir remettre la somme d'argent, la prestation ou le produit attendu par la victime. À tort, ce schéma d'escroquerie est parfois appelé « fraude à la commission ». En réalité, les fraudes à la commission portent sur une fausse promesse de commission, c'est- à-dire un pourcentage sur une prétendue fortune à disposition de l'escroc. Les fraudes qui exploitent le mode opératoire de l'avance de frais sont

beaucoup plus vastes. Les faux frais annoncés par les auteurs de fraudes pour obtenir des versements peuvent être très divers :

- lors de fraudes à la commission ou de fausses loteries, les frais portent sur le déblocage du gain (frais de succession en cas de scénario d'héritage, ouverture de compte en banque, frais de notaire, etc.) ;
- lors de fausses offres de logement, les frais peuvent consister en un paiement de caution, un loyer d'avance, ou un droit de visite ;
- dans les cas de faux vendeurs, des frais de transport sont demandés ;
- s'il s'agit d'un faux acheteur, de fausses confirmations, suspensions ou rétentions de paiement sont envoyées pour réclamer des frais de déblocage du paiement; des frais de transport sont parfois également réclamés pour venir chercher la marchandise ;
- dans les cas de demande de faux amis, la demande d'aide porte sur des frais de transport ou de logement, par exemple ;
- lors de fraudes aux sentiments, les explications peuvent être multiples : des frais médicaux, des difficultés financières personnelles, un projet de développement ou un voyage.

Certains scénarios de fraudes n'impliquent pas forcément des avances de frais tout en reposant sur une remise de bien délibérée. Dans le cas des fraudes au faux partenaire commercial, le fraudeur amène le lésé à réaliser un paiement sur le compte du fraudeur qui a usurpé l'identité d'un créancier de l'entreprise. Les escroqueries dans le commerce en ligne reposent entre autres sur l'habitude du paiement d'avance. Le faux vendeur obtient le paiement d'avance pour un produit ou un service qu'il ne livrera tout simplement pas. Le faux acheteur arrive à obtenir la marchandise en simulant une fausse confirmation de paiement. Une fausse annonce de blocage du paiement par l'intermédiaire financier peut également être envoyée (par exemple, dans l'attente de la confirmation de livraison). Certains auteurs exploitent également des stratégies de paiement en excès. La confirmation de paiement indique un montant supérieur à celui prévu. Le fraudeur demande alors à la victime de lui verser l'excédent. Lorsque la victime réalise que le paiement initial n'a pas eu lieu, elle a déjà remboursé l'excédent à ses frais. De telles stratégies sont notamment mises en œuvre par l'envoi de chèques qui prennent quelque temps avant d'être invalidés. Un faux acheteur déclare ne pas pouvoir venir chercher la marchandise, mais il annonce envoyer une société de transport. Le faux acheteur verse au vendeur un chèque couvrant le montant du bien et le paiement du transport qui sera réalisé par le vendeur dupé (Jones et McCoy, 2014). L'escroc récupère alors par la fausse qualité de transporteurs le montant des frais de livraison.

La remise de bien peut également avoir lieu au détriment du lésé sans qu'il ait conscience d'avoir transmis de l'argent. Les fraudes au faux problème technique ou de sécurité sont de ce type. Les fraudeurs appellent les

victimes, prétextant une faille de sécurité, la détection d'un virus sur leur ordinateur ou un autre problème technique, et les amènent à installer un logiciel de prise de contrôle à distance de l'ordinateur. Après avoir invité la victime à saisir ses coordonnées bancaires pour payer une solution logicielle (un antivirus, une mise à jour, etc.) ou à se connecter directement à leur banque en ligne, les escrocs vont réaliser des versements à son insu. D'autres escroqueries conduisent les lésés à s'inscrire involontairement à des services de SMS ou d'appels surtaxés ou encore à remplir des formulaires en ligne par lesquels ils souscrivent à des services payants non désirés.

Finalement, les fraudeurs peuvent user de moyens de contrainte pour faire du chantage et extorquer de l'argent au lésé. Dans les cas de fausses relations amoureuses, la victime amenée à se dénuder devant sa caméra va subir des menaces de publication en ligne de la vidéo. Dans les cas de fraudes à l'autorité, la fausse qualité adoptée par le fraudeur lui permet de faire pression sur le lésé qui verse l'argent non pas parce qu'il est en confiance, mais parce qu'il a peur du tort qui pourrait lui être causé. Dans les cas de fausses amendes, l'escroc usurpe l'identité d'une police pour menacer le lésé de poursuites judiciaires en cas de non-paiement de l'amende d'ordre (clémente) reçue. Dans les cas de fraudes au faux patron, le fraudeur ne manque pas d'user de sa position hiérarchique pour menacer l'employé de licenciement s'il ne réalise pas le virement d'argent nécessaire à la réalisation d'une affaire commerciale capitale pour l'entreprise.

Maintien d'un lien distant. Les gains engendrés sont en général de moyenne importance. Par exemple, la technique de l'avance de frais est réputée engendrer des revenus médians de quelques centaines, voire quelques milliers de francs/euros/dollars avant que la victime ne réalise la tromperie et décide de stopper les envois d'argent (FDC, 2018 ; Levi, 2017). Néanmoins, certains lésés vont payer à plusieurs reprises et perdre de très importantes sommes d'argent, ce qui peut les conduire à la ruine, voire au suicide. Comment expliquer que des victimes se retrouvent dans de telles situations ?

Globalement, la technique repose sur la stratégie commerciale du « doigt dans l'engrenage » (*foot-in-the-door technique*). Les fraudeurs débutent par des demandes peu coûteuses, puis augmentent les demandes au fil du temps. Un phénomène d'engagement est alors observé qui favorise la poursuite des paiements (Freedman et Fraser, 1966). Les fraudeurs développent des stratégies de pression pour maintenir le lien avec leur victime tout en gardant de la distance afin d'éviter d'être détectés, identifiés et localisés. Ils vont user de persuasion pour convaincre les victimes de continuer à payer en exploitant les vulnérabilités liées au scénario de confiance mis en œuvre (Atkins et Huang, 2013). Dans les cas de fausses ventes d'animaux, par exemple, l'escroc va par exemple prétexter des frais de vétérinaire, des frais de transport et finalement des frais de blocage en

douane. Si la victime refuse de payer, l'escroc ne manquera pas de rappeler à sa proie que le pauvre animal est bloqué dans une cage à la douane. Il joue alors sur les sentiments de compassion et de culpabilité. Les fraudes à la fausse commission sur un gain hypothétique reposent sur un mécanisme analogue. Les auteurs vont démultiplier les barrières (argent bloqué, frais administratifs, recours à un notaire, etc.) entre la promesse initiale et l'obtention du gain afin de maintenir le lien. Dans les cas de fausses romances, l'escroc va créer une situation de dépendance avec ses victimes en leur envoyant des messages régulièrement, jour et nuit. Pour créer cette relation de proximité tout en minimisant les risques de détection, les auteurs vont très rapidement demander aux victimes de quitter l'espace de convergence en ligne (typiquement un réseau social) pour communiquer par courriel ou par téléphone. Ainsi, les messages et les faux profils peuvent être supprimés et échapper à une hypothétique surveillance de la plateforme. Le jeu de confiance se transforme progressivement en situation de dépendance et de pression. Les victimes se retrouvent finalement dans des situations de déni, de honte ou de crainte, ce qui réduit les risques de dénonciation si elles réalisent leur erreur. L'escroquerie devient alors un cercle vicieux.

11.4 CONCLUSION

L'escroquerie ou la fraude en ligne doit être comprise comme un acte de tromperie qui conduit une victime, contactée par le réseau Internet dans un espace virtuel, à remettre un bien, et ce, en profitant d'une fausse qualité ou d'une mise en scène mensongère. Le bien peut être de l'argent, mais également des données ou des produits. L'ampleur du problème ne fait plus aucun doute. La majorité des fraudes commises à l'encontre des personnes semble maintenant être liée à Internet. À l'instar des vols et des cambriolages dans l'espace physique, elles constituent la part majoritaire des crimes contre le patrimoine sériels et véhiculés par des espaces virtuels. Si les schémas de fraudes existent depuis de très nombreuses années, Internet a fondamentalement transformé les mécanismes de rencontre. Les auteurs de fraudes peuvent prendre contact avec un nombre croissant de victimes potentielles, profiter des services d'autres criminels pour mener à bien leurs schémas de tromperie et tabler sur les difficultés des systèmes policiers et judiciaires à s'organiser pour traiter les cas. Les changements de volumes augurent de profondes transformations pour détecter, analyser et mitiger les problèmes. La complexité intrinsèque des fraudes implique également de repenser les modèles. Dans ce chapitre, un modèle d'analyse des escroqueries commises par le réseau Internet a été proposé. Il repose sur la décomposition du phénomène selon un script général en quatre étapes : (1) la prise de contact, (2) la mise en confiance, (3) la remise de bien, et (4) le maintien d'un lien distant. Globalement, les problèmes demeurent souvent mal compris par les victimes, les acteurs de la sécurité

et la recherche. Ils peinent donc à être reconnus. Les difficultés à détecter, à décrire et à classifier les fraudes affectent alors tant les estimations de leurs prévalences et les comparaisons internationales que la compréhension des modes opératoires et de leurs conséquences. L'ampleur du problème a néanmoins bien été établie et de nombreuses initiatives voient le jour à travers le monde pour mieux cerner le problème et améliorer les pratiques.

RÉFÉRENCES

ABS (Australian Bureau of Statistics). (2016). *4528.0 – Personal fraud, 2014-15*. Récupéré de http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4528.0Main%20Features152014-15?opendocument&tabname=Summary&prodno=4528.0&issue=2014-15&num=&view=

ACCC (Australian Competition and Consumer Commission). (2018). *Targeting scams: Report of the ACCC on scams activity 2017*. Récupéré de https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF

Alkaabi, A., Mohay, G., McCullagh, A. et Chantler, N. (2010, octobre). Dealing with the problem of cybercrime. Dans *Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime*, 4 au 6 octobre 2010, Abu Dhabi, Émirats arabes unis. Récupéré de https://eprints.qut.edu.au/38894/1/c38894.pdf

Atkins, B. et Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(03), 23-32.

Beals, M., DeLiema, M. et Deevy, M. (2015). *Framework for a taxonomy of fraud*. Longevity Center/FINRA Financial Investor Education Foundation/Fraud Research Center, Washington, DC : Stanford. Récupéré de http://162.144.124.243/~longevl0/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf

Benbouzid, B. et Peaucellier, S. (2016). L'escroquerie sur internet : la plainte et la prise de parole publique des victimes. *Réseaux, 3*(197-198), 137-171.

Bergmann, J. (1969). The original confidence man. *American Quarterly, 21*(3), 560-577.

Bogui, J.-J. (2010). La cybercriminalité, menace pour le développement. Les escroqueries Internet en Côte d'Ivoire. *Afrique contemporaine, 2*(234), 155-170.

Braucher, J. et Orbach, B. (2015). Scamming: The misunderstood confidence man. *Yale Journal of Law and the Humanities*, 27(2), 249-292.

Buchanan, J. et Grant, A. J. (2001). Investigating and prosecuting Nigerian fraud. *United States Attorneys' Bulletin*, *49*, 39-47.

Burgess, E. W. (1925). Can neighborhood work have a scientific basis? Dans R. E. Park, E. W. Burgess, et R. D. McKenzie (dir.), *The City: Suggestions for investigation of human behaviors in the urban environment* (p. 142-155). Chicago, IL: University of Chicago Press.

Burns, R. G., Whitworth, K. H. et Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32*(5), 477-493.

Button, M. et Cross, C. (2017). *Cyber frauds, scams and their victims*. Londres, GB : Routledge.

Button, M., Lewis, C. et Tapley, J. (2009). *Fraud typologies and the victims of fraud: Literature review*. Londres, GB: National Fraud Authority. Récupéré de http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-typologies-and-victims.pdf

Button, M., Lewis, C. et Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Button, M. et Tunley, M. (2015). Explaining fraud deviancy attenuation in the United Kingdom. *Crime, Law and Social Change*, *63*(1-2), 49-64.

Caneppele, S. et Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66-79.

Choi, K., Lee, J. L. et Chun, Y. T. (2017). Voice phishing fraud and its modus operandi. *Security Journal*, *30*(2), 454-466.

CIPC (Centre international pour la prévention de la criminalité). (2018). *Prévention de la criminalité et sécurité quotidienne: prévenir la cybercriminalité*. 6e Rapport international. Montréal, Canada. Récupéré de http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Report/CIPC_Rapport_2018.pdf

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, *3*, 151-196.

Côté, A. M., Bérubé, M. et Dupont, B. (2016). Statistiques et menaces numériques : comment les organisations de sécurité quantifient la cybercriminalité. *Réseaux*, *197-198*(3), 203-224.

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1-12.

Cross, C., Richards, K. et Smith, R. G. (2016). *Improving responses to online fraud victims: An examination of reporting and support*. Report to the Criminology Research Advisory Council. Canberra, Australie. Récupéré de https://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf

Dupont, B. (2013). Skills and trust: a tour inside the hard drives of computer hackers. Dans C. Morselli (dir.), *Illicit Networks* (p. 195-217). Londres, GB : Routledge.

Dupont, B. (2016). Des effets perturbateurs de la technologie sur la criminologie. *Revue internationale de criminologie et de police technique et scientifique*, *69*(3), 305-322.

Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., Whitty, M. (2018). The geography of online dating fraud. *Workshop on technology and consumer protection*. San Francisco, CA: IEEE. Récupéré de https://www.ieee-security.org/TC/SPW2018/ConPro/papers/edwards-conpro18.pdf

Farrell, G., Tseloni, A., Mailley, J. et Tilley, N. (2011). The crime drop and the security hypothesis. *Journal of Research in Crime and Delinquency*, *48*(2), 147-175.

FDC (Federal Trade Commission). (2018). *Consumer Sentinel Network Data Book 2017*. Récupéré de https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf

Freedman, J. L. et Fraser, S. C. (1966). Compliance without pressure: The foot- in-the-door technique. *Journal of Personality and Social Psychology*, *4*(2), 195-202.

Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime*, *6*(1), 146-157.

Gregg, D. G. et Scott, J. E. (2008). A typology of complaints about eBay sellers. *Communications of the ACM*, *51*(4), 69-74.

Harrell, E. (2019). Victims of identity theft, 2016. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Récupéré de https://www.bjs.gov/content/pub/pdf/vit16.pdf

Holt, T. J. et Bossler, A. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Londres, GB: Routledge.

Holt, T. J. et Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

Holtfreter, K., Reisig, M. D. et Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220.

Jakobsson, M. (dir.). (2016). *Understanding social engineering based scams*. New York, NY: Springer.

Jones, J. et McCoy, D. (2014). The check is in the mail: Monetization of Craigslist buyer scams. Dans *2014 APWG Symposium on Electronic Crime Research* (p. 25-35).

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Langton, L. (2011). *Identity theft reported by households, 2005-2010*. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Washington, DC: U.S. Department of Justice. Récupéré de https://www.bjs.gov/content/pub/pdf/itrh0510.pdf

Lea, S., Fischer, P. et Evans, K. (2009). *The psychology of scams: Provoking and committing errors of judgement*. Office of Fair Trading. Récupéré de www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

Leukfeldt, E. R., Kleemans, E. R. et Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704-722.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, *8*(4), 389-419.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

McGuire, M. et Dowling, S. (2013). *Cyber crime: A review of the evidence. Summary of key findings and implications*. Home Office Research Report, 75. [Londres, GB] : Home Office.

Nobles, M. R., Reyns, B. W., Fox, K. A. et Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, *31*(6), 986-1014.

ONS (Office for National Statistics). (2016). *Crime in England and Wales: Year ending Mar 2016*. Récupéré de https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingmar2016

ONS (Office for National Statistics). (2018). *Crime in England and Wales: Year ending June 2018*. Récupéré de https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2018

Park, Y., Jones, J., McCoy, D., Shi, E. et Jakobsson, M. (2014). Scambaiter: Understanding targeted Nigerian scams on Craigslist. *System*, *1*, 1-15.

Pratt, T. C., Holtfreter, K. et Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Reep-van den Bergh, C. M. et Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*(1), 5.

Samet, C. (2007). La fraude et l'escroquerie. Dans E. Béaur (dir.), *Fraude, contrefaçon, contrebande de l'Antiquité à nos jours* (p. 639-660). Genève, CH : Librairie Droz.

Sood, A. K. et Enbody, R. J. (2013). Crimeware-as-a-service – A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

Soudijn, M. R. J. et Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*, 111-129.

Wall, D. S. (2005). The Internet as a conduit for criminals. Dans A. Pattavina (dir.), *Information Technology and the Criminal Justice System* (p. 77-98). Thousand Oaks, CA : Sage. Révisé en mars 2010. Récupéré de https://www.researchgate.net/publication/228199078_The_Internet_as_a_Conduit_for_Criminal_Activity

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden, MA : Polity Press.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665-684.

Whitty, M. T. (2015a). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

Whitty, M. T. (2015b). Mass-marketing fraud: A growing concern. *IEEE Security & Privacy*, *13*(4), 84-87.