

Université de Montréal

Mécanismes d'entraide en ligne des victimes de fraude amoureuse

D'un registre amoureux à un registre frauduleux

Par

Pascale-Marie Cantin

École de criminologie

Faculté des Arts et des Sciences

Travail dirigé présenté en vue de l'obtention du grade de *Maîtrise ès sciences* (M. Sc) en
Criminologie, option Criminalistique et Information

Août 2021

© Pascale-Marie Cantin, 2021

Résumé

Le développement de nouvelles technologies de communication se conjugue avec l'essor des crimes facilités au moyen d'Internet. Partie intégrante des sociétés occidentales, le cybermonde simplifie la vie et le travail des particuliers et des entreprises. Toutefois, cet outil comporte un lot de risques, particulièrement en matière de fraudes et d'arnaques. La présente recherche fait part de cet oxymore en s'intéressant à la façon dont les victimes d'escroqueries sentimentales utilisent le cybermonde afin de s'entraider à la suite d'une expérience frauduleuse commise dans le monde virtuel. Pour ce faire, nous avons analysé trois forums de discussion en ligne destinés aux victimes de fraude amoureuse afin d'établir les mécanismes d'entraide utilisés par ces dernières pour faire suite à leur expérience. En outre, nous avons extrait une portion d'informations identifiantes disponibles à travers ces forums de façon à révéler ce qu'elles comportent en termes de traces numériques. Les résultats indiquent entre autres qu'une importante proportion de victimes utilisent ces forums pour raconter leur récit, trouver du soutien et recevoir des conseils, mais aussi pour accompagner d'autres victimes potentielles ayant un doute sur la relation qu'elles entretiennent en ligne. De plus, ces plateformes servent de moyen de lutte afin d'exposer et de lutter contre les cybercriminels, puisqu'elles sont en partie destinées au partage d'informations identifiantes, de photographies et de modes opératoires liés aux arnaqueurs sentimentaux. Les victimes se servent également des forums de discussion afin de sensibiliser et d'informer les internautes généraux quant aux stratagèmes utilisés par les fraudeurs et de fournir les noms des institutions et organismes à contacter s'ils sont un jour ou l'autre confrontés à une possible arnaque amoureuse. Cette étude met en exergue la pertinence de combiner la criminalistique et la criminologie afin d'aborder des phénomènes cybercriminels et l'importance de s'attarder au caractère transfrontalier des fraudes amoureuses afin de mieux les prévenir et de mieux les contrer.

Mots-clés :

Fraude amoureuse ; Stratagème de rencontre ; Arnaque/Escroquerie sentimentale ; Mécanisme d'entraide en ligne ; Forums de discussion en ligne ; Traces numériques ; Informations identifiantes

Abstract

The development of new communication technologies is combined with the rise of crime facilitated by the Internet. As an integral part of Western societies, the cyberworld simplifies the life and work of individuals and businesses. However, this tool carries a lot of risks, especially in terms of frauds and scams. This research addresses this oxymoron by looking at how victims of sentimental scams use the cyberworld to help each other after a fraudulent experience has been committed in the virtual space. To this end, we analyzed three online discussion forums intended for victims of romance fraud in order to establish the self-help mechanisms used by the latter to follow up on their experience. In addition, we extracted a portion of the identifying information available through these forums in order to reveal what they contain in terms of digital traces. The results show, among other things, that a significant proportion of victims use these forums to tell their story, to find support and advice, and to accompany other potential victims who are unsure about their online relationship. In addition, these platforms serve as a means to expose and combat cybercriminals, as they are partly intended for sharing identifying information, photographs and modus operandi related to romance scammers. Victims also use chat rooms to educate and inform general Internet users about the schemes used by fraudsters, and the institutions and organizations to contact if they are ever confronted with a possible romance scam. This study highlights the relevance of combining forensic sciences and criminology in order to address cybercriminal phenomena as well as the importance of focusing on the cross-border nature of romance frauds in order to better prevent and counter them.

Keywords:

Romance scam ; Self-help mechanisms ; Online discussion forums ; Digital traces ; Identifying information

Table des matières

| | |
|--|------|
| Résumé..... | iii |
| Abstract..... | iv |
| Table des matières..... | v |
| Liste des tableaux..... | viii |
| Liste des figures et des cartes..... | ix |
| Remerciements..... | x |
| Introduction..... | 1 |
| Chapitre 1 : Revue de littérature | 3 |
| 1. L'implication du cyberspace dans l'escroquerie sentimentale..... | 3 |
| 1.1. Le romantisme dans le cyberspace | 3 |
| 1.2. Les traces numériques générées par les rencontres en ligne | 7 |
| 1.3. L'entraide en ligne..... | 9 |
| 2. Les arnaqueurs sentimentaux..... | 10 |
| 2.1. Organisation et typologie de fraudeurs..... | 10 |
| 2.2. Ingénierie sociale et techniques de persuasion des fraudeurs..... | 13 |
| 2.3. Script criminel (anatomie) de la fraude amoureuse..... | 16 |
| 3. Les victimes | 18 |
| 3.1. Caractéristiques des victimes..... | 18 |
| 3.2. Conséquences de l'arnaque amoureuse sur les victimes..... | 20 |
| Chapitre 2 : Problématique | 21 |
| Chapitre 3 : Méthodologie | 25 |
| 3.1. Choix de la méthode et procédure employée..... | 25 |
| 3.2. Les spécificités du terrain d'étude | 29 |

| | |
|---|-----|
| 3.2.1. Le vocabulaire employé sur les forums de discussion..... | 29 |
| 3.2.2. L'émotion par l'écrit..... | 30 |
| 3.3. Considérations éthiques particulières à cette étude | 31 |
| 3.4. Limites de l'étude | 32 |
| Chapitre 4 : Analyse et interprétation des résultats | 32 |
| 4.1. Les forums de discussion : un soutien et une voix pour les victimes | 33 |
| 4.1.1. Le témoignage écrit : une forme de libération et de soutien moral | 33 |
| 4.1.2. L'identification à son semblable : un moyen pour briser l'isolement | 36 |
| 4.1.3. L'accompagnement : un mécanisme pour se reconstruire..... | 38 |
| 4.2. Les forums de discussion : une lutte contre les cyberarnaqueurs | 39 |
| 4.2.1. Le signalement et le partage de profils frauduleux : une abondance de traces numériques..... | 39 |
| 4.2.2. Le partage du contenu des conversations entre un fraudeur et une victime : reconstruction de modus operandi fondé sur les traces numériques..... | 42 |
| 4.3. Des plateformes d'informations et de sensibilisation | 44 |
| 4.3.1. Les astuces pour démasquer une arnaque | 45 |
| 4.3.2. Les astuces pour couper le contact avec un cyberarnaqueur | 46 |
| 4.3.3. Les institutions et les organismes à contacter | 47 |
| Chapitre 5 : Discussion | 50 |
| 5.1. Les forums de discussion : un outil permettant aux victimes de retrouver les bienfaits du monde en ligne..... | 51 |
| 5.2. Le signalement en ligne : un registre qui gagne à être étendu internationalement | 52 |
| 5.3. Considérations à prendre dans l'interprétation des forums de discussion | 53 |
| Chapitre 6 : Dimension intégrative | 54 |
| Conclusion | 57 |
| Références bibliographiques..... | xii |

Annexes..... xix

Liste des tableaux

| | |
|--|----|
| Tableau 1. Présentation des forums de discussion sélectionnés abordant la fraude amoureuse | 27 |
| Tableau 2. Terminologie des forums de discussion en ligne | 30 |
| Tableau 3. Procédés sémio-discursifs de l'émotion sur les forums de discussion en ligne | 30 |
| Tableau 4. Nombre moyen de réponses et de vues sur les forums de discussion..... | 38 |
| Tableau 5. Les mécanismes d'entraide entre les victimes de fraude amoureuse..... | 48 |

Liste des figures et des cartes

| | |
|--|----|
| Carte 1. Provenance des numéros de téléphone signalés, Signal-Arnaques..... | 51 |
| Figure 1. Nombre de fois qu'un réseau social est mentionné dans une publication d'origine, ScamWarners, 2013 à 2021 | 43 |
| Figure 2. Nombre de fois qu'un fournisseur de service courriel est mentionné dans une publication d'origine, ScamSurvivors, 2013 à 2021..... | 44 |

Remerciements

La présente étude n'aurait pu être menée sans l'aide et le soutien de nombreuses personnes. Malgré un parcours ébranlé par les enjeux liés à l'actuelle pandémie, celles-ci ont su m'accompagner et faire une réelle différence dans la réalisation de ce projet et dans la cadre du programme de maîtrise en criminologie, option criminalistique et information dans son ensemble. Merci pour votre soutien, vos conseils et le précieux temps que vous m'avez accordés au cours des deux dernières années.

Premièrement, je souhaite dédier ce travail à la mémoire de Diane Casoni, qui fut la première à croire en mon sujet en démontrant un enthousiasme contagieux à son égard et à la recherche en général. Merci de m'avoir rassurée durant mon premier trimestre à la maîtrise et d'avoir cru en moi.

Deuxièmement, je tiens sincèrement à remercier mon directeur de recherche, Benoît Dupont, pour sa grande disponibilité, son soutien, ses conseils et le travail incroyable qu'il effectue auprès de tous les étudiants qu'il accompagne aux cycles supérieurs. Merci de nous avoir octroyé une bourse d'études de la Chaire de recherche en prévention de la cybercriminalité durant la dernière année pour nous aider à mieux faire face au confinement et aux cours en ligne. Merci d'avoir cru en moi et de m'avoir encouragée tout au long de mon parcours.

Merci également à Quentin Rossy pour ses conseils et son aide concernant la dimension criminalistique de ce travail. Ce dernier n'aurait été possible sans les cours donnés en ligne à partir de l'Université de Lausanne et l'aide que vous m'avez fournie pour l'extraction de données. Je vous remercie de votre temps, de votre disponibilité et de vos encouragements.

Merci beaucoup à l'École de criminologie de m'avoir octroyé une bourse de rédaction durant l'été. Cette bourse a été un réel soutien durant cette période.

Je souhaite également remercier le Centre international pour la prévention de la criminalité qui m'a permis d'approfondir mon sens de la recherche au cours de la dernière année et de me concentrer sur mes études durant mon dernier trimestre.

Merci à toutes les personnes de l'École de criminologie, professeurs et étudiants, avec qui j'ai pu échanger et qui ont contribué à faire de ce parcours universitaire une expérience exceptionnelle.

Finalement, j'adresse un grand merci à mes proches et à ma famille qui ont toujours cru en moi, qui ont relu mes nombreux travaux et qui m'ont fourni un soutien incroyable tout au long de mon parcours universitaire, tant au baccalauréat qu'à la maîtrise.

Introduction

L'émergence des moyens de communication numériques a certainement modifié la façon dont les individus correspondent entre eux. De nombreux avantages sont tirés du cyberspace, le premier étant la facilitation des échanges à distance entre deux ou plusieurs personnes. Toutefois, les progrès liés à la sphère numérique s'accompagnent d'une part, d'un déplacement de la criminalité vers le monde en ligne et, d'autre part, d'une nouvelle catégorie de crimes émergents directement de ce monde virtuel. En d'autres mots, les activités criminelles provenant du monde réel s'adaptent et évoluent en fonction de cet environnement, puis de nouvelles activités déviantes naissent à travers les opportunités créées par celui-ci. L'une des spécificités qui distinguent le cyberspace du monde réel est le nombre vertigineux de cibles qu'il permet d'atteindre en minimisant grandement les risques liés aux activités déviantes, ce qui le rend propice aux répétitions criminelles. Ces activités impliquent notamment une variété de fraudes, qui demandent de nouvelles formes d'interventions et de réponses (Dupont, 2017 ; Rossy et Ribaux, 2020 ; Ribaux et Souvignet 2020).

Parmi ces formes de fraude, l'arnaque sentimentale (ou fraude amoureuse), phénomène peu rapporté par les individus qui en sont victimes, devient progressivement courante. De plus en plus, les individus se tournent vers les sites de rencontre en ligne afin de vivre de nouvelles expériences romantiques sans limites spatio-temporelles. Récemment, les arnaques qui s'y rattachent se sont multipliées avec l'utilisation accrue des réseaux sociaux par les utilisateurs. En 2018, le Centre antifraude du Canada rapportait environ 760 plaintes relatives aux arnaques sentimentales, ayant fait l'objet d'une perte financière d'approximativement 22,5 millions de dollars dans sa totalité (Gendarmerie royale du Canada, 2019). Par ailleurs, on considère qu'il s'agit de la dixième fraude la plus courante chez les Canadiens, et la deuxième engendrant le préjudice financier le plus important derrière le harponnage (Centre anti-fraude du Canada, 2019). Notons également que les enjeux liés à la pandémie de la COVID-19, telle l'utilisation accrue d'Internet et des médias sociaux durant cette période ainsi que le sentiment d'isolement, ont engendré une recrudescence significative de plusieurs types de fraudes en 2020, dont le stratagème amoureux (Gouvernement du Canada, 2021).

Jusqu'à présent peu analysée en termes de recherche, cette fraude se particularise et se démarque par la double conséquence qu'elle engendre : une perte financière généralement importante et une déception amoureuse non négligeable dans la plupart des cas. La majorité des recherches portant sur le sujet traitent des réseaux frauduleux et des conséquences pour les victimes, mais peu s'attardent à la dimension forensique et aux enjeux de cybersécurité qui se rattachent aux arnaques sentimentales en ligne. En outre, jusqu'à présent, aucune étude ne s'est expressément attardée à la façon dont les victimes de fraude amoureuse se reconstruisent et s'entraident ultérieurement à leur expérience. La plupart des écrits portant sur l'entraide en ligne concernent les domaines de la santé et de l'éducation. Notre cadre conceptuel est d'ailleurs fondé sur cette idée selon laquelle certains individus vivant des réalités semblables solliciteraient de l'aide et en fourniraient sur des forums de discussion en ligne destinés à leur problématique. De ce fait, la présente étude cherche à mettre en relation ces axes manquants ou ceux qui pourraient être approfondis. Elle s'intéresse d'abord aux mécanismes d'entraide générés par les victimes de fraude amoureuse sur les forums de discussion en ligne, puis à la façon dont ceux-ci comportent et génèrent des traces numériques pertinentes laissées par les fraudeurs dans leur mode opératoire.

Le présent travail est composé de six chapitres. Le premier fait un survol des écrits présentant les principales entités liées aux arnaques sentimentales, tels le cybermonde, les fraudeurs et les victimes. Ce chapitre fait également un bref survol de la littérature relative à l'entraide en ligne. Ensuite, le second chapitre porte sur la problématique de recherche du présent travail en abordant plus précisément les connaissances manquantes du phénomène pour mieux justifier la pertinence et la contribution de notre étude. Le troisième chapitre présente la méthodologie employée, laquelle porte sur l'analyse de trois forums de discussions et sur l'extraction de données pertinentes. Le quatrième chapitre présente les résultats obtenus, et le cinquième lance une discussion relativement à ces derniers. Finalement, le dernier chapitre concerne la pertinence d'intégrer la criminalistique et la criminologie dans le cadre d'études portant sur la fraude amoureuse.

Chapitre 1 : Revue de littérature

La présente recension des écrits cherche à contextualiser la fraude amoureuse de façon à mettre en exergue les principales entités qui interagissent entre elles pour la composer, soit le cybermonde, les fraudeurs et les victimes. Pour ce faire, nous procéderons du général au particulier, en débutant par la présentation de l'espace social et technologique dans lequel cette arnaque prend forme. Nous aborderons notamment les écrits concernant l'entraide en ligne, qui constituent un important cadre théorique pour la présente recherche, considérant qu'ils nous ont permis d'orienter les choix concernant la nature des données à collecter ainsi que l'analyse et l'interprétation qui peuvent en être faites. Ensuite, nous présenterons les caractéristiques et les techniques des fraudeurs, et finaliserons en traitant du profil des victimes et des impacts d'une telle fraude sur ces dernières.

1. L'implication du cyberspace dans l'escroquerie sentimentale

Cette première section fait part des différents rôles que peut jouer le cyberspace à travers une expérience de fraude amoureuse. Avant tout, il est nécessaire de définir ce terme, que nous qualifierons également de cybermonde, de monde numérique ou de monde en ligne au cours de la présente étude. Au cours des dernières décennies, plusieurs définitions ont vu le jour et ont évolué parallèlement avec l'émergence de nouveaux cybercrimes. Aujourd'hui, on peut désigner le cyberspace comme étant « un système global de structures informatiques interconnectées comprenant le matériel, les logiciels, les données et les utilisateurs ainsi que les relations logiques entre elles, peu importe la manière dont elles s'établissent [notre traduction] » (DPCM, 2013, cité par Ning et al., 2018, p. 1845). Ainsi, cette section abordera, d'une part les études ayant contribué aux connaissances liées au romantisme dans le cyberspace, à savoir les interactions sociales numériques et, d'autre part, les enjeux se rattachant aux rencontres en ligne. Ensuite, elle traitera des études relatives aux traces numériques générées par celles-ci, puis terminera en abordant l'entraide entre internautes prenant forme à travers le monde numérique.

1.1. Le romantisme dans le cyberspace

1.1.1. Les interactions sociales sur les sites de rencontre

Les premiers sites de rencontre en ligne sont apparus au cours des années 1990 et se sont multipliés depuis (Brooks, 2011). L'omniprésence des technologies au sein du grand public (téléphones mobiles, Internet, etc.) et la numérisation des institutions et de la société occidentale en général ont fait croître la popularité des sites de rencontres au cours des dernières années (Phan et al., 2021). En 2021, 36 % des Canadiens célibataires sont inscrits à un site ou une application de rencontre, puis entre 60 % et 90 % (dépendamment du groupe d'âge) utilisent régulièrement les réseaux sociaux (Eharmony, 2021 ; Schimmele et al., 2021). Une grande partie de nos activités sociales se déroulent de plus en plus en ligne et sont fondées sur des discours numériquement construits grâce à des dispositifs logiciels d'écriture du web (Paveau, 2019). Les relations sociolinguistiques construites sur ces sites impliquent notamment des stratégies de *flirt*, combinant des aspects linguistiques, paralinguistiques et non verbaux (par exemple, des insinuations, des questions, des références, des sourires et des rires, des contacts visuels, des façons de communiquer, etc.). Ces stratégies sont des moyens qui servent à construire, à exprimer et à négocier un ou des désirs romantiques entre les utilisateurs (Cameron et Kulick, 2006).

Ainsi, les sites de rencontre impliquent un jeu de séduction dans lequel les utilisateurs cherchent d'abord et avant tout à plaire à l'autre (Qeis, 2016). Par ailleurs, les représentations photographiques et le langage utilisé sur les sites de rencontre peuvent avoir un rôle prééminent sur la façon dont les individus interprètent le profil d'un abonné. Concrètement, Fiore et al. (2008) ont démontré que les photos et les images présentées constituent le principal prédicteur d'attractivité d'un profil sur un site ou une application de rencontre. Les textes de présentation auraient également une importante incidence sur la perception positive d'un utilisateur vis-à-vis un autre. En ce qui a trait aux profils masculins, les textes démontrant de l'extraversion, de la confiance et une certaine forme de sensibilité seraient perçus comme étant plus attrayants aux yeux des utilisatrices. Quant aux profils féminins, ce serait principalement les photographies qui mettent la féminité en exergue qui auraient une forte incidence sur la perception positive d'un profil de la part des abonnés masculins (Fiore et al, 2008). L'étude de Del Teso Craviotto (2006) a pour sa part démontré que l'humour était l'une des stratégies les plus couramment employées par les hommes pour engager une conversation affectueuse. La reproduction à l'écrit d'expressions et de prononciations de la vie courante (à l'oral) donnerait une impression

de familiarité et serait souvent associée à un sens de l'humour permettant d'améliorer le courant d'une conversation. Les applications et les sites de rencontre créeraient ainsi un *simulacrum*, à travers duquel les utilisateurs construiraient une réalité imaginaire basée sur une interaction sociale numérisée (Qeis, 2016).

En outre, le langage représente un élément clé pour comprendre la manière dont les gens construisent leurs désirs et interagissent en fonction de leur identité sexuelle à travers des sites ou des applications de rencontre (Del Teso Craviotto, 2006). Pour bâtir ces interactions, les utilisateurs d'un site de rencontre doivent échanger et s'appuyer sur un ensemble d'idées communes afin de permettre une communication cohérente dans le cybermonde, tels un langage, des règles de conversation et des mécanismes d'inférence communs (Del Teso Craviotto, 2006). Dans le même ordre d'idées, Sabela (2014) suggère que les sites de rencontre s'apparentent à une communauté qui instaure des règles et des normes permettant aux utilisateurs de converser de façon harmonieuse. Ces règles et ces normes seraient propres à chaque site ou application de rencontre. La même étude suggère qu'en interagissant en ligne, les individus découvrent la portée de la représentation d'eux-mêmes, notamment à travers les commentaires écrits de leurs abonnés. Le contact social réalisé en ligne avec d'autres peut produire un niveau élevé de satisfaction chez les participants (Del Teso Craviotto, 2006). Dans le cas d'une arnaque sentimentale et de la présente recherche, ces éléments sont particulièrement pertinents pour mieux comprendre la façon dont les fraudeurs produisent et reproduisent des profils réalistes qui paraissent légitimes aux yeux des utilisateurs en fonction de la plateforme de rencontre employée. Ceci pourrait, entre autres, nous donner des indications quant aux modes opératoires des cybercriminels qui ajusteraient leur profil en fonction des normes du réseau social en question. Les individus « étudieraient » les sites et modifieraient leur présentation et leur façon de faire en fonction des normes associées à ceux-ci (Sabela, 2014). Comme mentionné précédemment, les hommes et les femmes ne sont pas attirés par le même genre de profils sur les sites de rencontre, indiquant que les cybercriminels pourraient possiblement adapter leurs techniques frauduleuses en fonction de l'individu ciblé.

1.1.2. Les risques et la criminalité liés aux réseaux sociaux

Bien qu'ils facilitent les rencontres et la communication, les réseaux sociaux¹ génèrent des risques associés à la violence et aux crimes de nature économique et sexuelle (Phan et al., 2021). L'utilisation accrue des plateformes et des applications web permet aux cybercriminels d'avoir accès à un ciblage de victimes potentielles exigeant peu d'efforts (Cross, 2020). Par ailleurs, une étude réalisée aux États-Unis suggère qu'environ 66 % des utilisateurs d'Internet considèrent que les sites et les applications de rencontre sont dangereux (Madden et Lehnart, 2006, cité par Couch et al., 2012).

Jusqu'à présent, les études réalisées sur les risques associés aux sites de rencontre traitent pour la plupart des violences sexuelles. Certaines d'entre elles (Cali et al., 2013 ; Scannell, 2019 ; Australian Institute of Criminology, 2020) se sont penchées sur les dangers liés aux rencontres en personne organisées à partir d'un site de rencontre. D'autres (Australian Institute of Criminology, 2020 ; Snaychuk et O'Neill, 2020 ; Zhong et al., 2020) se sont intéressées aux crimes liés à la notion de *Technology-Facilitated Sexual Violence* (TFSV), une notion qui réfère à un comportement sexuel inapproprié et non désiré étant communiqué et transmis par des moyens numériques. Ces comportements incluent le harcèlement en ligne, le harcèlement sexuel et la violence sexuelle véhiculée en ligne (Snaychuk et O'Neill, 2020 ; Zhong et al., 2020). Cette forme de violence serait davantage dirigée vers les femmes (Powell et Henry, 2015 ; Anderson et al., 2020). L'étude de Zhong et al. (2020) suggère que les réseaux sociaux et les plateformes web faciliteraient et exacerberaient les violences sexuelles, notamment en raison d'une désinhibition prononcée des utilisateurs interagissant sur ceux-ci.

En ce qui concerne les crimes économiques commis à travers les sites de rencontre, la littérature renvoie abondamment à l'usurpation d'identité et aux escroqueries sentimentales, dont la fraude amoureuse et la sextorsion. Ces deux phénomènes peuvent s'apparenter. Toutefois, dans le cadre du présent travail, nous préférons différencier ces

¹ Certains réseaux sociaux sont expressément destinés aux rencontres romantiques en ligne. C'est le cas notamment des applications Tinder, Bumble, Hinge, etc. D'autres n'ont pas été développées dans le but de faciliter les rencontres romantiques, mais celles-ci peuvent tout de même prendre forme à travers ces applications, en raison notamment des profils publics (ou non) et de la facilité de communication qui les caractérise. C'est le cas notamment d'Instagram et de Facebook. Notons également que Facebook dispose d'une fonction vouée aux rencontres romantiques. Étant donné qu'une arnaque sentimentale peut prendre forme sur l'une ou l'autre de ces formes de réseaux, les sites de rencontre sont ici considérés comme des réseaux sociaux au même titre qu'une application impliquant un profil non destiné à une quête amoureuse.

deux formes d'escroquerie, puisqu'elles se distinguent à certains égards et n'impliquent pas nécessairement les mêmes enjeux et modus operandi. En effet, la sextorsion se définit comme étant une forme de chantage, qui consiste en l'extorsion d'images de nature sexuelle à travers Internet ou les réseaux sociaux (Ashurst et McAlinden, 2015). Dans certains cas, les cyberintimidateurs vont menacer de publier les images envoyées par les victimes à leur entourage si une somme d'argent ne leur est pas remise dans une période donnée (Boisseau et Legros, 2020). Ainsi, le phénomène de la sextorsion se différencie de la fraude amoureuse puisqu'elle implique une forme de chantage et de menace particulière. Dans le second phénomène, la victime envoie volontairement une somme d'argent à son fraudeur puisqu'elle considère leur relation comme étant légitime.

Par ailleurs, le délit de la sextorsion touche davantage et plus spécifiquement la population adolescente (Ashurst et McAlinden, 2015). D'après Machimbarrena et al. (2018), les adolescents coconstruisent leur environnement en mettant en relation les mondes en ligne et hors ligne. Ainsi, les réseaux sociaux sont souvent utilisés dans le but de développer certains aspects propres à l'adolescence, dont l'intimité relationnelle. Étant donné la quête d'identité et les nombreux changements qui surviennent à l'adolescence, les individus seraient psychologiquement plus vulnérables à ce type d'escroquerie durant cette période de leur vie (Machimbarrena et al., 2018).

1.2. Les traces numériques générées par les rencontres en ligne

Les réseaux sociaux et les plateformes web sont des outils débordant d'informations pouvant permettre de retracer un individu ou de l'identifier (Powell et Haynes, 2020). Dans le cadre d'une investigation cherchant à détecter les traces numériques d'un crime commis à l'aide de moyens informatiques, il faut savoir distinguer les cas où l'on utilise un ordinateur (ou un téléphone intelligent) pour commettre une infraction de ceux pour lesquels l'infraction a pour objet un ordinateur (Buquet, 2011). Dans le cadre de la présente étude, nous nous intéressons aux premiers cas puisque les escroqueries sentimentales consistent en une manipulation facilitée au moyen d'un ordinateur et non d'une attaque ciblant un réseau ou un système informatique. Notons qu'une trace est définie comme étant « une marque ou un signal apparent, pas nécessairement visible à l'œil nu [représentant] le vestige d'une présence ou d'une action » (Margot, 2014, p.74). Elle est porteuse

d'information sur sa source et sur l'activité à son origine. Dans un cadre numérique, une trace est constituée « d'empreintes numériques laissées volontairement, ou non, dans l'environnement informatique » (Galinon-Méléneec et Zlitni, 2013, p.115). Internet constitue un environnement informatique, mais peut aussi être considéré comme un environnement informatisé, si l'on considère, à l'évidence, les êtres humains comme acteurs du Web (Galinon-Méléneec et Zlitni, 2013). En d'autres mots, les traces numériques sont des données laissées de manière active et passive par des individus et elles désignent les informations qu'un dispositif numérique enregistre sur les actions ou l'identité de ses utilisateurs. Prises de façon isolées, ces traces n'ont parfois guère de sens. Toutefois, une fois combinées et traitées, elles peuvent révéler des informations significatives permettant de profiler des individus et de faire du ciblage comportemental (Sogliuzzo, 2013). Les traces numériques concernant les escroqueries sentimentales sont généralement plus abondantes à travers les moyens de communication utilisés pour assurer les échanges entre la victime et l'arnaqueur. Ces traces peuvent constituer, par exemple, des photographies, des numéros de téléphone, des dates des échanges, des pseudonymes, du contenu, des moyens de paiements, des adresses courriel, des adresses IP, des localisations, etc. La collecte de traces se fait en partie par l'exploitation de l'ordinateur ou des comptes de la victime ayant porté plainte (Taylor et al., 2014). En outre, on peut également avoir accès à certaines données en en faisant la demande à la compagnie responsable du réseau social concerné (Powell et Haynes, 2020).

Les réseaux sociaux contiennent des données et des métadonnées souvent abondantes pouvant épauler les enquêteurs. En effet, ceux-ci détiennent souvent de nombreuses informations sur les suspects, les victimes et les témoins, grâce aux données comme les messages, les listes d'amis, les géolocalisations, les vidéos et les informations démographiques. Les réseaux possèdent également des métadonnées qui peuvent s'avérer pertinentes, tels que des adresses courriel, des adresses IP, des logs de connexion, etc. (Karyda et Mitrou, 2007 ; Arshad et al., 2019). Toutefois, plusieurs obstacles peuvent entraver le processus d'enquête visant les traces numériques, à savoir les méthodes d'anonymisation (VPN, Proxy, etc.) et les enjeux légaux et transfrontaliers qui régissent les fournisseurs de service (Karyda et Mitrou, 2007). L'utilisation de traces numériques comme preuve dans le cadre d'un procès est encadrée par des lois sévères et le droit pénal

tire de l'arrière compte tenu de l'évolution rapide des technologies dans la majorité des pays (Powell et Haynes, 2020). Dans le cas d'une fraude amoureuse, une mise en accusation est rarement concrétisée, principalement en raison des complexités pénales transfrontalières (Baillif et Ducret, 2018).

1.3. L'entraide en ligne

Cette section traite de l'entraide en ligne, et plus précisément des forums de discussion dédiés à une certaine forme d'assistance. Ce soutien constitue un cadre conceptuel important pour notre étude puisque le fondement s'appuie sur la façon dont les victimes d'arnaque sentimentale échangent entre elles ultérieurement à leur expérience frauduleuse à travers le monde en ligne.

1.3.1. Les forums de discussion d'aide

Avec l'avènement d'Internet, les forums de discussion font désormais l'objet d'analyse linguistique et empirique afin d'étudier certains phénomènes. Originellement, ce terme latin faisait référence à un lieu de discussions et d'échanges. De nos jours et dans le monde numérique, il est employé pour désigner, entre autres, un outil de communication asynchrone visant l'échange de messages télématiques entre des internautes (Duthoit et al., 2011). Son caractère asynchrone assure sa temporalité relativement longue et sa persistance dans le cybermonde. Pour Pélissier et Mailles-Viard Metz (2010), l'aide désigne tout espace de dialogue impliquant une interaction entre un individu « plus connaissant » et un « moins connaissant » qui s'inscrit dans une perspective visant à résoudre un problème pour favoriser l'état d'une situation particulière.

Jusqu'ici, les études portant sur les forums de discussion d'entraide concernent majoritairement le domaine de la santé (p. ex. : Smith-Merry et al., 2019 ; Berthelot-Guiet et Charbonneaux, 2020) ou le domaine scolaire (p. ex. : Duthoit et al., 2011 ; Puustinen et al., 2015). Parmi celles-ci, l'étude de Berthelot-Guiet et Charbonneaux (2020) aborde l'entraide numérique intergénérationnelle sur les forums de discussion entre des individus atteints d'un glioblastome. Leur recherche a notamment démontré que les malades utilisaient les forums afin de faire part de leur « récit », c'est-à-dire une description des péripéties associées à la maladie. Les forums produisent collectivement des savoirs expérientiels en raison des échanges entre les internautes. L'étude de Greiner (2018) a pour

sa part démontré que les usagers des forums portant sur l'usage du cannabis publient des messages à thématiques différentes selon leur genre et leur implication quantitative sur une plateforme numérique. En outre, l'étude suggère qu'il y existe deux formes de soutien sur les forums, soit le soutien émotionnel et celui visant à fournir de l'information. Finalement, l'étude réalisée par Smith-Merry et al. (2019) suggère que les forums de discussion en ligne destinés aux individus atteints d'un problème de santé mentale permettent aux internautes de développer des relations sociales manquantes dans leur vie quotidienne, et à la fois de trouver et de fournir des conseils pratiques. Du côté du domaine scolaire, l'étude de Puustinen et al. (2015) suggère que les interactions sociales et les échanges entre les élèves et leur professeur tendent à différer dans le monde en ligne, ceux-ci étant abrégés et parfois sans conclusion dans le cybermonde (à l'inverse de la communication en face à face). Notons toutefois que la participation aux forums scolaires était obligatoire pour les étudiants, ce qui n'était pas dans les cas des forums étudiés dans le domaine de la santé.

Les études portant sur l'entraide en ligne démontrent qu'une importante part d'individus concernés par une problématique se tournent vers les forums de discussion afin de partager leur expérience, de recevoir du soutien et/ou de trouver ou de fournir des informations pertinentes. Toutefois, peu, voire aucune, d'entre elles ne se sont attardées à l'entraide entre les victimes d'un phénomène criminel. La contribution de ces études demeure intéressante pour notre cadre conceptuel, fondé sur l'entraide sur les forums de discussion.

2. Les arnaqueurs sentimentaux

2.1. Organisation et typologie de fraudeurs

La littérature fait part de plusieurs types d'arnaqueurs sentimentaux caractérisés par des différences culturelles et organisationnelles. L'étude d'Edwards et al. (2018) est l'une des rares études ayant analysé les traces numériques laissées par les cybercriminels dans un délit relatif à une fraude amoureuse. L'étude s'est penchée sur la provenance des adresses IP de certaines arnaques et sur la réutilisation d'éléments respectifs à certains profils. Elle suggère entre autres que la majorité des arnaqueurs sentimentaux exécuteraient leur crime depuis des pays d'Afrique de l'Ouest, employant des proxy pour cacher leur géolocalisation. D'autres études (Rege, 2009 ; Enoch, 2008) suggèrent que les

cybercriminels responsables des cas de fraude amoureuse opèrent généralement à travers une forme d'organisation criminelle, dans laquelle ils travaillent ensemble afin de créer des cercles de partage de données et de meilleures stratégies frauduleuses. Les prochaines lignes traiteront plus en profondeur de ces études et de ce qu'elles suggèrent en matière d'organisation et de typologies de fraudeurs.

2.1.1. Le fraudeur solitaire

D'une part, le premier type de fraudeur réfère à l'individu qui agit seul. Celui-ci est reconnu pour être patient et avoir une approche routinière, par laquelle il gagnera tranquillement la confiance de sa victime. Au point de vue technique, l'arnaqueur qui agit seul détient des connaissances informatiques de base et utilise de fausses images afin de créer des profils frauduleux. Il ne démontre pas d'empathie envers celui ou celle qu'il a fraudé et évite les conséquences pénales en gardant son anonymat (Rege, 2009). L'étude d'Edwards et al. (2018) suggère entre autres que les fraudeurs utilisent fréquemment des serveurs proxy, qui servent d'intermédiaires entre le trafic Internet d'un internaute et le site web qu'il consulte. L'individu n'est donc jamais en contact direct avec les sites qu'il fréquente et cela lui permet de préserver son anonymat (Ghimiray, 2021). En outre, Aransiola et Asindemade (2011) considèrent qu'une importante part des cybercriminels au Nigéria exécutent leurs crimes dans des cybercafés de façon à conserver leur anonymat. Edwards et al. (2018) suggère qu'environ 30 % des arnaqueurs sentimentaux se situeraient dans cette région du monde. Ceux-ci créeraient davantage de faux profils masculins, d'hommes âgés d'environ 50 ans et prétendant être divorcé ou veuf (également vrai pour la Malaisie et l'Afrique du Sud). Les arnaqueurs agissant depuis les Philippines, l'Ukraine et le Sénégal créeraient pour leur part, plus de faux profils féminins, de femmes âgées d'environ 30 ans. Par ailleurs, les fraudeurs adapteraient la présentation de leur faux profil en fonction de la culture du pays dans lequel il cible leurs victimes potentielles (Edwards et al. 2018).

2.1.2. Les fraudeurs œuvrant en petit groupe

D'autre part, Rege (2009) fait part de fraudeurs qui agissent en petit groupe. Les individus le composant sont alliés et solidaires les uns envers les autres. Ils détiennent chacun un rôle précis dans la concrétisation de la fraude, en passant par les organisateurs,

aux exécuteurs, puis à ceux responsables des transferts d'argent. Les organisateurs sont les arnaqueurs les plus déterminants dans une fraude amoureuse puisqu'ils déterminent la nature et la portée de cette dernière (Lemieux, 2003, cité par Rege, 2009). Les exécuteurs, pour leur part, ont comme objectif de répondre aux attentes des organisateurs. C'est eux qui composent les lettres d'amour, qui parlent plusieurs langues et qui entretiennent des échanges avec les victimes (Rege, 2009). Les responsables des transferts d'argent sont ceux qui collectent les sommes des victimes puis les exportent à l'entreprise criminelle à travers des sites comme WesterUnion ou MoneyGram (Rege, 2009 ; Whitty, 2013). Ces fraudeurs détiennent généralement les mêmes compétences techniques que les individus agissant seuls. Toutefois, ils utilisent des bases de données sur les victimes potentielles qu'ils partageront entre eux ainsi que des exemples de types de lettres ou de courriels d'amorce. L'étude d'Edwards et al. (2018) suggère d'ailleurs que les cybercriminels réutilisent des textes descriptifs et des images pour créer des profils frauduleux. Les fraudeurs partagent internationalement des images et des textes, mais auraient plus tendance à partager ce genre de contenu avec des individus œuvrant depuis le même pays qu'eux (Edwards et al. 2018). Ils échappent aux autorités par l'anonymat et par une réorganisation flexible et dynamique de leur groupe criminel.

2.1.3. Le large réseau criminel

Enfin, on retrouve également les fraudeurs qui agissent à travers un large réseau. Ils entretiennent de faibles liens entre eux et opèrent via une structure transitoire et décentralisée. Tout comme dans les petits groupes, le large réseau est composé d'organisateurs, d'exécuteurs et de transféreurs d'argent. Toutefois, le réseau est également composé d'extendeurs, d'*enforcer* et de *crossovers* (Rege, 2009). Les extendeurs réfèrent aux arnaqueurs responsables d'élargir le réseau criminel. Ils recrutent entre autres de nouveaux membres et encouragent la collaboration avec d'autres entreprises illégitimes. Ce que Rege (2009) qualifie d'*enforcer* fait référence aux individus protégeant le réseau en prenant les mesures nécessaires afin d'assurer l'amadouement des victimes. Quant aux *crossovers*, ils représentent les personnes faisant partie du réseau criminel qui œuvre également au sein du gouvernement ou d'une entreprise légitime. Ces arnaqueurs fournissent des documents légitimes afin d'amadouer plus facilement les victimes. En outre, ils donnent un accès aux informations internes, facilitant le bon fonctionnement du

réseau criminel. Le large réseau se distingue par sa forte culture frauduleuse, à travers le partage d'informations, de données, de ressources et de formations qui sont quotidiennement mises de l'avant et diffusées massivement. Ces cybercriminels échappent aux conséquences pénales grâce à leurs techniques d'anonymat (serveurs proxy, VPN, Tor, cybercafés, etc.), leur réorganisation flexible et dynamique, l'autonomie de leurs opérations et par l'exposition de sous-groupes frauduleux (Rege, 2009). En effet, selon Yoo (2005), le large réseau est davantage à l'abri du contrôle social que les petits groupes ou que l'individu qui agit seul puisqu'il arrive à demeurer intact même si certains des fraudeurs qui le composent sont exposés aux forces de l'ordre.

2.2. Ingénierie sociale et techniques de persuasion des fraudeurs

Il a été démontré que les cyberfraudeurs présentent des caractéristiques et utilisent des techniques de persuasion similaires (Whitty, 2013). Afin d'amadouer leur victime et de concrétiser leur fraude, les cyberarnaqueurs opèrent à travers des techniques d'ingénierie sociale, c'est-à-dire qu'ils manipulent les individus afin d'obtenir des informations confidentielles (Ferreira et al., 2015 ; Anesa, 2020). Dans une situation impliquant une arnaque sentimentale, les fraudeurs manipulent les utilisateurs des sites de rencontre en leur offrant ce qu'ils recherchent, c'est-à-dire, une relation amoureuse (Whitty, 2013).

L'objectif ultime de cette manipulation peut être le gain financier direct ou l'obtention d'informations bancaires. Pour ce faire, les fraudeurs utilisent des techniques de persuasion visant à exploiter les faiblesses psychologiques des utilisateurs de sites ou d'applications de rencontre (Archer, 2017). Cialdini (2007) a mis l'accent sur six principes psychologiques souvent employés par les individus cherchant à obtenir la conformité d'autrui. Ces techniques sont souvent retrouvées chez les fraudeurs d'arnaque sentimentale (Whitty, 2013 ; Archer, 2017).

2.2.1. Réciprocité

Le premier principe réfère à la réciprocité. Celui-ci s'inspire de l'idée selon laquelle les individus seraient plus susceptibles de se conformer à une demande lorsqu'ils se sentent redevables ou ressentent une certaine obligation envers le demandeur (Cialdini, 2007). D'après Whitty (2013), certains arnaqueurs sentimentaux utilisent cette technique en

envoyant des fleurs ou des petits cadeaux à leur victime en espérant qu'elle se sente redevable et cède plus facilement à la demande d'argent future.

2.2.2. Engagement et cohérence

Le second principe consiste en l'engagement et en la cohérence. Après avoir pris une décision ou un engagement initial, les individus seraient davantage portés à prendre des décisions similaires ou conformes à cet engagement afin de justifier leur action antérieure (Cialdini, 2007). Dans certains cas, certains individus continuent d'agir conformément à leurs décisions antérieures puisqu'ils ont déjà beaucoup investi à travers celles-ci et croient qu'ils approchent de leur objectif ultime. Dans le cas du phénomène de la fraude amoureuse, certaines victimes vont continuer d'envoyer des sommes d'argent croyant qu'elles seront prochainement récompensées avec une relation amoureuse légitime (Whitty, 2013).

2.2.3. Preuve sociale

Ensuite, Cialdini (2007) propose le principe de la preuve sociale (consensus), qui consiste en l'idée selon laquelle les gens seraient enclins à concevoir un comportement comme normal s'ils perçoivent que les autres agissent également dans ce sens. En d'autres mots, l'individu a tendance à agir comme les autres s'il perçoit qu'ils sont nombreux à agir ainsi. Ce principe est moins évident dans le cas d'une fraude amoureuse, mais peut tout de même survenir. Par exemple, certains fraudeurs font semblant d'avoir été victimes d'un grave accident et demandent une aide financière à leur victime. Afin de convaincre ces dernières, les cybercriminels mentionneront que d'autres personnes lui ont déjà envoyé des fonds, mais que cette aide n'est toujours pas suffisante (Archer, 2017).

2.2.4. Affection

Le principe suivant est particulièrement influent dans une situation d'arnaque sentimentale puisqu'il fait référence à l'affection. Ce principe s'appuie sur l'idée selon laquelle les gens seraient plus susceptibles d'être persuadés par quelqu'un qu'ils affectionnent ou avec qui ils partagent des points communs (Cialdini, 2007). Dans la plupart des cas de fraude amoureuse, les individus éprouvent des sentiments amoureux vis-à-vis le fraudeur, ce qui les motive à leur remettre des sommes d'argent (Whitty, 2013). Les cybercriminels développent petit à petit une relation amoureuse avec leur victime, en

la séduisant au moyen de compliments et de promesses de projets communs. La recherche d'affection, étant souvent l'objectif principal des individus s'inscrivant sur des sites de rencontre, agit dès lors comme une susceptibilité facilitant le transfert d'argent et la concrétisation de l'arnaque pour le fraudeur.

2.2.5. Autorité

On retrouve ensuite le principe de l'autorité, qui s'appuie sur l'idée selon laquelle les individus se conformeraient davantage à une demande si le demandeur occupe une position d'autorité par rapport à eux (Cialdini, 2007). Dans la majorité des arnaques sentimentales, le fraudeur prétend être une personne influente occupant des fonctions importantes, comme un homme d'affaires, un soldat ou un médecin œuvrant pour une organisation internationale, se donnant ainsi un certain statut valorisé par plusieurs (Whitty, 2013).

2.2.6. Rareté

Finalement, le principe de la rareté est le dernier concept développé par Cialdini (2007). Celui-ci sous-entend que les individus seraient davantage portés à prendre une décision sur une situation donnée s'ils considèrent qu'elle représente une opportunité unique et limitée dans le temps. En d'autres mots, les individus sont plus susceptibles de vouloir ce qu'ils pensent ne pas pouvoir avoir à un autre moment. Dans les cas d'arnaqes sentimentales, les fraudeurs prétendent souvent avoir besoin d'argent de manière urgente. Ainsi, les victimes, craignant de fragiliser leur relation si elles refusent la demande, ont tendance à remettre une somme pécuniaire au fraudeur en raison de l'urgence de la fausse situation. En outre, il se peut également que ces victimes aient peu d'opportunités amoureuses sur les sites qu'elles fréquentent, rendant unique la relation qu'elles entretiennent avec le fraudeur. Ainsi, la perte de ce contact privilégié peut également être perçue dans cette dynamique de rareté.

Chaque situation impliquant une fraude amoureuse détient son lot de particularités. Toutefois, les techniques de persuasion employées par les cybercriminels peuvent servir d'indices permettant d'identifier une fraude (Ferreira et Lenzini, 2015). Les études de Whitty (2013) et d'Archer (2017) ont permis de démontrer en quoi les techniques de persuasion de Cialdini (2007) permettent de discerner une arnaque d'une relation amoureuse légitime issue du cybermonde.

2.3. Script criminel (anatomie) de la fraude amoureuse

Quelques études (Whitty, 2013 ; Shaari et al. 2019) ont mis l'accent sur le processus de concrétisation des fraudes amoureuses. Cette forme d'escroquerie se développerait à travers des étapes distinctes visant à amadouer les utilisateurs des sites de rencontre. Ceci rappelle l'approche d'analyse de scripts criminels proposée par Cornish (1994, cité par Rossy, 2016), à travers laquelle il définit la décomposition des activités délictueuses selon une séquence d'épisodes organisés par une structure procédurale de comportements et de routines.

2.3.1. Épisode premier : la création du profil frauduleux

Pour Whitty (2013) et Shaari et al. (2019), le premier stade consiste en l'élaboration du profil frauduleux. Dans la majorité des cas, l'initiateur mentionne être un professionnel d'origine américaine ou européenne, travaillant à l'étranger (Anesa, 2020). Le profil est généralement composé d'une ou de plusieurs photos démontrant un style de vie luxueux (Shaari et al. 2019). Chez les profils frauduleux féminins, les photos empruntées appartiennent généralement à de jeunes femmes désirant devenir mannequins ; elles publient celles-ci dans l'objectif de décrocher un emploi dans le domaine (Whitty, 2013). Chez les hommes, les photos sont généralement empruntées des réseaux sociaux les plus utilisés et représentent des hommes vêtus d'un uniforme d'armée (Whitty, 2013). De plus, selon l'étude de Shaari et al. (2019), les profils frauduleux ont généralement une courte liste d'amis, ce qui constitue l'un de leurs défauts pouvant indiquer une intention malveillante.

2.3.2. Épisode second : conditionner une potentielle victime

Ensuite, le second stade consisterait au *grooming*, c'est-à-dire à l'amadouement de la victime en développant un lien de confiance et en amplifiant l'intimité relationnelle avec cette dernière (Whitty, 2013 ; Shaari et al. 2019). En termes de temps, cette étape peut varier de quelques semaines à quelques mois (Whitty, 2013). Le fraudeur va généralement employer des mots ou des expressions avec des connotations religieuses, qui indiquent une fiabilité et un sentiment de confiance, qui expriment un désir pour la victime et des expressions qui priorisent la victime, puis la fait sentir importante (Shaari et al. 2019). Par ailleurs, c'est normalement au cours de cette étape que le fraudeur va déclarer son amour

pour la victime et lui proposer d'utiliser d'autres moyens de communication (autre que le site de rencontre ou le réseau social où ils ont fait connaissance) (Whitty, 2013). De façon à construire une relation de plus en plus intime, le fraudeur communiquera avec sa victime par téléphone, par clavardage direct ou par messages vocaux. Il lui promettra une vie romantique et amoureuse à long terme, puis lui indiquera que leur rencontre doit être reportée pour des raisons souvent de nature professionnelle (Whitty, 2013). En général, c'est au cours de cette étape que la victime partagera des informations personnelles sur sa vie et commencera à développer des sentiments amoureux pour celui ou celle qui tente de la frauder (Whitty, 2013). Toutefois, selon Whitty (2013), à ce stade, la victime n'est pas prête à envoyer des fonds.

2.3.3. Troisième épisode : les demandes graduelles d'aide pécuniaire

Pour Whitty (2013) et Shaari et al. (2019), le troisième stade arrive lorsque le fraudeur tente tranquillement de convaincre sa victime de lui envoyer une certaine aide financière. En général, le langage employé par le fraudeur devient plus agressif et insistant (Shaari et al. 2019). Certains scénarios pour soudoyer la victime sont plus communs que d'autres. Par exemple, les criminels diront qu'un membre de leur famille est atteint d'une maladie grave et qu'il nécessite des soins coûteux, qu'ils ont des problèmes avec l'immigration pour rejoindre la victime dans son pays, qu'ils ont eu un accident ou encore qu'ils sont forcés de payer une compensation (Shaari et al. 2019). De manière générale, le fraudeur commence à demander de petites sommes, puis augmente avec le temps si la victime collabore (Anesa, 2020).

2.3.4. Quatrième épisode (facultatif) : humiliation et abus cybersexuel

Dans certains cas plus rares, le stade suivant porte sur l'abus sexuel (Whitty, 2013). Cette situation se produit parfois lorsque le fraudeur a déjà commis un crime financier envers sa victime et désire l'humilier davantage en demandant à cette dernière d'accomplir des actes sexuels devant sa caméra. D'après Whitty (2013), le fraudeur agit ainsi dans le but d'utiliser le contenu pour faire chanter la victime ou pour son simple plaisir. Cette étape peut ainsi s'apparenter au phénomène de la sextorsion mentionné précédemment.

2.3.5. Dernier épisode : la découverte de l'arnaque

Enfin, la dernière phase consiste en la révélation du crime (Whitty, 2013 ; Shaari et al., 2019). D'après Shaari et al. (2019), à ce stade, les échanges font presque uniquement l'objet de transactions financières et l'utilisation de mots ou d'expressions romantiques disparaît graduellement. Le langage employé est plus agressif. C'est alors que la victime prendra connaissance du crime commis à son égard, soit par le biais du fraudeur, par les autorités ou par elle-même (Whitty, 2013). En outre, c'est durant cette phase que la victime sera confrontée à des sentiments ambivalents, balançant entre son amour et sa haine pour celui qui l'a fraudée. Elle sera par la suite confrontée à une double conséquence, à la fois pécuniaire et émotionnelle. Dans certains cas, le stade de la révélation ne met pas nécessairement un terme à la fraude. Il arrive que le fraudeur avoue son crime à la victime, mais tente tout de même de lui faire croire que ses sentiments amoureux sont réels. Ainsi, une deuxième vague d'escroqueries peut survenir. En outre, la victime devient parfois complice de l'arnaqueur, de façon plus ou moins volontaire, notamment lorsqu'elle accepte d'agir comme mule pour les transferts d'argent. (Whitty, 2013).

3. Les victimes

3.1. Caractéristiques des victimes

Plusieurs études (Whitty, 2018 ; Sorell et Whitty, 2019 ; Buttons, Nicholls, Kerr et Owen, 2014) ont mis l'accent sur les caractéristiques des victimes d'arnaque en ligne et les raisons pour lesquelles ces dernières sont tombées dans un piège frauduleux. Ces caractéristiques réfèrent aux conditions socio-économiques des individus ainsi qu'à leurs traits de personnalité.

3.1.1. Âge et éducation

Des chercheurs (Titus et Gover, 2001 ; Whitty, 2018) ont analysé les facteurs de vulnérabilité pouvant influencer un individu à tomber dans un piège frauduleux. L'étude de Whitty (2018) a démontré que les individus d'âge moyen seraient les plus touchés par le phénomène. Les individus appartenant à cette tranche d'âge auraient plus de revenus que les individus plus jeunes ou très âgés et seraient davantage à la recherche d'une relation amoureuse sérieuse, ce qui peut en partie expliquer cette tendance (Whitty, 2018). En outre, les résultats de l'étude ont démontré que les individus éduqués et instruits seraient plus vulnérables aux fraudes amoureuses que les personnes moins scolarisées. Titus et Gover

(2001) suggèrent également que les individus instruits seraient plus à risque d'être victime d'une fraude. Deux hypothèses peuvent expliquer ces résultats. D'une part, Whitty (2018) indique que les individus éduqués utiliseraient davantage les sites de rencontre, expliquant pourquoi ils seraient plus nombreux à être victimes de fraude amoureuse. D'autre part, Fisher et al. (2013) suggèrent que les individus instruits auraient tendance à avoir un excès de confiance menant à un sentiment d'infaillibilité en matière d'escroquerie. Ainsi, dans le cas d'une fraude amoureuse, les individus très confiants négligeraient les signes précurseurs de l'arnaque, facilitant sa concrétisation.

3.1.2. Impulsivité et faible maîtrise de soi

Whitty (2018) a analysé les caractéristiques psychologiques des victimes de fraude amoureuse en comparant leur personnalité avec celles d'individus n'étant pas tombés dans un piège frauduleux. Les résultats de l'étude ont démontré que les victimes d'arnaque sentimentale sont généralement impulsives et ont une maîtrise d'elles-mêmes présentant des vulnérabilités. Cette caractéristique expliquerait notamment pourquoi ces individus seraient plus susceptibles d'être persuadés par le principe de la rareté de Cialdini (2007), présenté préalablement (Whitty, 2018). Par ailleurs, les individus avides et à la recherche de sensations fortes, ce qui constitue une forme d'impulsivité, seraient plus vulnérables aux cyberfraudes (Zuckerman, 2013, cité par Modic et Stephen, 2012). Block (1995) considère qu'un individu avec une personnalité impulsive aura généralement tendance à adopter des comportements à risque. En outre, les résultats de l'étude de Langenderfer et Shimp (2001) sur les facteurs de vulnérabilité des victimes d'escroquerie ont démontré que ces dernières sont souvent à la recherche d'une forme de fantaisie, les rendant ainsi plus vulnérables à tomber dans un piège frauduleux. Ce résultat est conforme à l'idée de Qeis (2016), mentionné précédemment, selon laquelle les individus auraient tendance à créer des relations simulacres en ligne pour répondre à leurs désirs.

3.1.3. Crédulité

Les études de Whitty (2018), Teunisse et al. (2020) et Whitty (2019) ont démontré que les victimes d'arnaque sentimentale ont une grande facilité à croire autrui. Les victimes elles-mêmes auraient tendance à se qualifier d'individus naïfs et ayant facilement confiance aux propos des autres, favorisant ainsi leur attachement au fraudeur (Whitty, 2019). Dans

le même ordre d'idées, l'étude de Langenderfer et Shimp (2001) a démontré que les victimes de fraude sont généralement plus crédules et naïves que les personnes non victimisées. Cette caractéristique relève d'une tendance perçue dans la majorité des phénomènes variés du monde en ligne (Langenderfer et Shimp, 2001).

3.2. Conséquences de l'arnaque amoureuse sur les victimes

3.2.1. Conséquences émotionnelles

Comprendre les impacts d'une fraude constitue une nécessité afin de lutter contre les arnaques en ligne (Modic et Anderson, 2015). Les conséquences d'une fraude amoureuse varient d'une victime à une autre. En effet, Modic et Anderson (2015) ont démontré que les traits de personnalité peuvent influencer la façon dont un individu interprétera et vivra les impacts négatifs relevant d'une escroquerie. Toutefois, l'étude de Buchanan et Whitty (2014) a relevé que les arnaques sentimentales engendrent des conséquences émotionnelles toutes aussi importantes chez les victimes financières que chez les victimes non financières, c'est-à-dire celles n'ayant pas succombé aux demandes d'argent du fraudeur. Suite à l'escroquerie, plusieurs impacts psychologiques, comme le stress, la honte, la perte d'estime de soi, la colère et le bouleversement sont ressentis par les victimes de fraude en général (Button, Lewis et Tapley, 2014). L'isolement, l'état de choc et un sentiment d'inquiétude persistant sont également des conséquences émotionnelles soulevées par les victimes de fraude (Cross, Richard et Smith, 2016).

Plusieurs individus indiquent avoir été confrontés à une détérioration de leur santé mentale suite à la fraude (Button, Lewis et Tapley, 2014). Dans le même ordre d'idées, l'étude de Cross, Richard et Smith (2016) a démontré que l'arnaque subie s'avère être un événement critique et dévastateur pouvant changer la vie des victimes. D'autres ont déclaré être encore plus affectées par la perte de la relation amoureuse que par la perte financière associée au crime, et ce, peu importe l'ampleur des montants irrécupérables (Whitty, 2015). En effet, les études antérieures ont démontré que pour de nombreuses victimes, l'expérience frauduleuse engendre des conséquences durables et entraînent des changements dans le comportement de ces dernières. Par exemple, l'étude de Button et al. (2009) a démontré que la victimisation engendre un changement dans les comportements des individus, comme le fait d'être plus prudent et méfiant.

Par ailleurs, une fois le crime révélé, certains individus ressentiraient un profond sentiment de honte et d'humiliation, les démotivant à signaler la fraude aux autorités (Whitty, 2015). La fraude peut également engendrer des impacts négatifs affectant les relations de la victime avec son entourage (Button, Lewis et Tapley, 2014). Certains membres de la famille sont confrontés à une détresse et à un stress important lorsqu'ils tentent de décourager la victime de transférer des sommes d'argent à l'arnaqueur (Button, Lewis et Tapley, 2014).

3.2.2. Conséquences financières

Les avancées technologiques des dernières années ont facilité la concrétisation de diverses formes de fraude financière. Internet et les réseaux sociaux sont devenus l'outil principal pour les fraudeurs afin de rentrer en contact avec des victimes et de soutirer de l'argent à partir de plateformes sécurisées permettant de garder leur anonymat (Cross, Richard et Smith, 2016). L'étude de Cross, Richard et Smith (2016) a démontré que les victimes de fraude en ligne ont de la difficulté à indiquer précisément les sommes pécuniaires perdues, puisque les pertes ont été subies sur une longue période. Dans d'autres cas, les victimes ont indiqué avoir simplement perdu la trace des montants envoyés. Par ailleurs, plus la somme d'argent perdue est importante, plus les victimes ont tendance à vivre certaines conséquences émotionnelles, comme le stress (Cross, Richard et Smith, 2016). La perte financière engendre également plusieurs conséquences en termes de conflits familiaux (Button, Lewis et Tapley, 2014). En matière de fraude amoureuse, la Gendarmerie royale du Canada (2018) estime qu'environ 760 victimes se sont fait détrousser plus de 22,5 millions de dollars à l'échelle du pays durant l'année. Ces pertes dépassent toute autre forme d'escroqueries et de fraudes signalées en 2018. On considère qu'il s'agit d'un crime répandu sur Internet évoluant conjointement avec les diverses plateformes de rencontre en ligne, qui mérite une attention empirique particulière.

Chapitre 2 : Problématique

La revue de littérature a permis de démontrer que l'utilisation accrue des réseaux sociaux et des nouvelles technologies de communication a contribué à l'émergence de nouveaux types de crimes impliquant des modes opératoires spécifiques au monde en ligne. Les sites de rencontre constituent d'ailleurs une méthode facilitant un bon nombre

d'escroqueries, telles l'usurpation d'identité, la sextorsion et l'escroquerie sentimentale. Bien qu'on reconnaisse la prise d'ampleur de ces arnaques, il est toutefois difficile d'en estimer la prévalence (Coat, 2020).

En ce qui concerne plus précisément la fraude amoureuse, les écrits ont démontré qu'il existe plusieurs typologies d'arnaqueurs sentimentaux, œuvrant seuls, en petit groupe ou à travers un large réseau. Ceux-ci s'entraident, partagent leurs techniques frauduleuses et développent ainsi leurs intentions malveillantes en fonction des nouvelles technologies et plateformes de rencontre. La littérature aborde également les principaux modes opératoires employés par les cyber fraudeurs pour commettre une arnaque sentimentale ainsi que les techniques de persuasion utilisées. Une grande partie des arnaqueurs sentimentaux exécuteraient leur crime depuis l'Afrique de l'Ouest (Yen et Jakobsson, 2016), complexifiant le processus d'enquête en raison des enjeux transfrontaliers accompagnant une demande d'entraide internationale (Baillif et Ducret, 2018).

La littérature aborde également l'expérience victimaire d'une fraude amoureuse. En effet, de façon à cibler les différents facteurs de risque pouvant avoir une incidence sur la victimisation, plusieurs études (Buttons et al., 2014, Whitty, 2018 ; Sorell et Whitty, 2019) ont abordé les principales caractéristiques des victimes de fraude amoureuse. D'autres (Buchanan et Whitty, 2014 ; Modic et Anderson, 2015) ont plutôt mis l'accent sur les conséquences émotionnelles et financières associées à l'expérience victimaire. Les victimes sont rarement, voire jamais indemnisées, puis sont pour la plupart bouleversées à long terme (Button et al., 2014).

Les études citées dans la revue de littérature comprennent cependant un lot de limites. D'une part, la majorité des études portant sur les victimes sont issues de la littérature anglo-saxonne et ont été menées dans des pays tels l'Australie ou au Royaume-Uni. Ainsi, il apparaît pertinent de combler la littérature en s'attardant davantage aux fraudes amoureuses ayant impliqué des victimes s'exprimant en langue française ou résidant dans un État francophone. D'autre part, une importante part des études se sont attardées à l'expérience victimaire, sans toutefois aborder la façon dont les victimes se reconstruisent et font preuve de résilience à la suite de leur expérience frauduleuse. Notons que certaines études (voir entre autres Smith-Merry et al., 2019 ; Berthelot-Guiet et Charbonneaux, 2020) ont analysé

l'entraide en ligne, mais qu'aucune n'a expressément mis l'accent sur les victimes de fraude amoureuse.

Par ailleurs, les études portant sur les arnaqueurs sentimentaux traitent principalement de la façon dont ils mettent leur fraude à exécution. Celles-ci se concentrent davantage sur les modes opératoires de façon générale, sans s'attarder à ce qu'ils révèlent, notamment, en termes de traces numériques. En effet, on observe, à travers la littérature, que peu d'études se sont penchées sur la dimension forensique et sur les enjeux de cybersécurité liés aux applications et aux sites de rencontre. En effet, peu de recherches ont traité des artefacts numériques pouvant être collectés au moyen des applications ou des téléphones mobiles ayant été impliqués dans une escroquerie. Certaines (Karyda et Mitrou, 2007 ; Arshad et al., 2019) se sont intéressées aux traces générées par les réseaux sociaux de façon générale, mais peu, voire aucune, ne traitent explicitement des traces numériques découlant d'une fraude amoureuse. Dans le cas d'un crime commis sur Internet, il nous semble essentiel de considérer l'espace à travers duquel une fraude est commise et d'identifier ce qui le compose ainsi que les failles qui lui sont associées.

La fraude amoureuse est un crime caractérisé d'une part, par une dynamique relationnelle particulière alimentée par une forme de manipulation du fraudeur envers sa victime et, d'autre part, par un espace numérique composé d'une panoplie de données et d'entités rendant l'arnaque possible. Ainsi, il semble essentiel d'établir une codisciplinarité entre les champs d'expertise pouvant être utiles afin d'étudier l'un et l'autre des mécanismes visant à mieux comprendre ce phénomène criminel, à savoir la criminologie et les sciences forensiques fondées sur les traces numériques. Combiner ces deux sciences permet d'avoir une perspective plus large de ce qui compose les crimes commis à travers Internet.

Comme nous l'avons mentionné précédemment, les études citées dans la revue de littérature ont traité des mécanismes d'entraide entre les fraudeurs, mais n'abordent pas ceux qui existent entre les victimes afin de leur permettre de se reconstruire suite à l'expérience frauduleuse. L'étude de Bastiaensens (2019) a démontré qu'un bon nombre d'individus contraient la cyberviolence en offrant et en recevant du soutien à travers

Internet. Ainsi, à partir de ce postulat et tout en cherchant à combler les autres limites mentionnées préalablement, l'objectif principal de la présente recherche est de mieux comprendre comment les victimes s'entraident en ligne à la suite d'une arnaque sentimentale. Cette première étape est essentielle pour la poursuite du second objectif qui vise à détecter, grâce aux mécanismes d'entraide, les traces numériques laissées par les fraudeurs et recueillies par les victimes pouvant servir à les identifier ou à établir des liens entre elles. Identifier les types de traces laissées par les cybercriminels dans leur mode opératoire et déterminer comment y avoir accès à partir des victimes permettra notamment de guider le travail d'investigation lié à cette forme d'escroquerie.

Afin d'atteindre ces objectifs, notre étude prendra la forme d'une recherche hybride, impliquant une portion qualitative plus importante, mais empruntant toutefois des méthodes quantitatives visant à faciliter l'interprétation des traces numériques. Ceci nous permettra de mettre davantage en relation la criminologie et les sciences forensiques et de démontrer en quoi la combinaison de ces deux champs d'expertise est nécessaire afin de traiter des enjeux liés à une fraude amoureuse.

Les résultats de notre étude permettront ainsi de développer les savoirs liés à la façon dont les victimes s'entraident à la suite d'une expérience frauduleuse, et comment ces mécanismes peuvent contribuer au travail d'investigation visant ultimement à produire du renseignement criminel. Concrètement, afin de répondre à l'objectif principal visant à identifier les mécanismes d'entraide et à l'objectif plus spécifique aux traces numériques, notre étude vise à répondre aux questions suivantes :

Question principale : Quels sont les mécanismes d'entraide en ligne développés par les victimes d'arnaque sentimentale suite à leur expérience et quelles fonctions remplissent-ils à leur égard ?

Question secondaire : Que révèlent ces mécanismes quant aux traces numériques laissées par les fraudeurs dans leur mode opératoire et quelle est leur pertinence ?

Chapitre 3 : Méthodologie

3.1. Choix de la méthode et procédure employée

Pour répondre au mieux aux questions soulevées dans le cadre de cette étude, les données ont été collectées à travers une démarche méthodologique hybride, dont les principales composantes sont de nature qualitative, mais dont certains aspects empruntent des éléments propres aux méthodes quantitatives. La combinaison de ces méthodes est complémentaire et permet d'aborder un sujet sous plusieurs aspects (Laplace, 2013).

Ainsi, de façon à mieux comprendre la façon dont les victimes de fraude amoureuse s'entraident en ligne, nous avons privilégié une procédure inductive fondée sur les forums de discussion publics. Cette méthode est employée dans le but de réaliser une théorisation ancrée se basant sur le contenu de ces forums. Notre observation est dite « non participante », puisque nous analysons le discours des utilisateurs des forums sans toutefois intervenir ou interagir avec eux. Cette forme d'observation est avantageuse, d'une part, puisqu'elle n'a pas d'impact sur les données collectées et, d'autre part, puisque nous n'avons pas besoin de nous faire observer par les participants, ce qui nous permet d'avoir une plus grande objectivité et de garantir une absence de désirabilité sociale de la part des personnes observées (Pastinelli, 2011). Par ailleurs, puisque nous utilisons des forums de discussion publics, il n'y a pas d'évaluation éthique nécessaire à réaliser auprès des utilisateurs des plateformes.

Afin de concrétiser cette démarche, nous avons réalisé une observation préliminaire sur Internet. Cette étape nous a permis d'identifier les divers espaces de travail, de nous imprégner des différents forums et de prendre connaissance du vocabulaire employé. Nous avons également fait un survol du type de contenu disponible de façon à identifier les éléments exploitables. À la suite de cette première étape, nous avons pris connaissance de nombreux forums portant sur la fraude amoureuse. Nous en avons sélectionné trois à analyser dans le cadre de la présente étude, à savoir ScamWarners, ScamSurvivors et Signal-Arnaques (voir l'Annexe 1 pour le format des forums). Les deux premiers sites sont de langue anglaise, alors que le dernier est en français. La grande majorité des forums de discussion portant sur la fraude amoureuse et présentant une abondance de données sont rédigés en anglais, à l'exception du site Signal-Arnaques. Comparer les résultats issus des

sites anglophones et de ce site francophone nous permettra ainsi de déterminer s'il existe des différences entre les mécanismes d'entraide en ligne en fonction de la langue employée dans les forums de discussion. Ces trois forums ont été principalement sélectionnés en raison de l'abondance et de la pertinence de leur contenu.

En outre, étant donné la quantité de données disponibles et de façon à mieux traiter l'information relative aux traces numériques, nous avons extrait les données issues de ces forums (p. ex. : titre, contenu du message, date de publication, nombre de vues, nombre de réponses, numéro de téléphone fourni par le fraudeur et sa provenance, adresse courriel du fraudeur, pseudonymes du fraudeur et de l'auteur de la publication, etc. [voir Tableau 1]) dans des bases de données Excel et avons désagrégé des informations avec des fonctions disponibles sur le logiciel. Dans le cadre de cette recherche, Internet permet d'augmenter la puissance statistique des résultats en favorisant l'accès à notre population cible (les victimes de fraude amoureuse), souvent éloignée. L'extraction permet de diminuer le coût des erreurs lors du transfert de données, puisque la collecte est déjà informatisée par les forums de discussion (Laplace, 2013).

Pour ce faire, toutes les pages (accessibles sans *login*) issues des forums ont été téléchargées avec un programme développé à l'École des sciences criminelles de l'Université de Lausanne par le professeur Q. Rossy et son équipe (T. Pineau et J. Bourquenoud). Le programme, développé en python 3, se fonde sur la librairie *Selenium* qui permet d'automatiser l'utilisation d'un navigateur. Le processus a été réalisé sur *Windows* en exploitant le navigateur *Chrome*. Toutes les pages ont été parcourues en désactivant l'affichage des images, afin de limiter la bande passante pour le serveur. Les requêtes ont été réalisées à un rythme d'environ 10 pages par minute, de façon à limiter la charge du serveur et ainsi ne pas réaliser une opération pouvant s'apparenter à un déni de service. Toutes les pages ont été enregistrées au format HTML. Ensuite, toutes les pages portant sur les sections d'intérêt ont été parcourues, puis les liens vers chacun des sujets ont été extraits selon le même processus. En ce qui concerne le traitement des pages, la librairie *lxml* a été utilisée et des fonctions de recherche (*parsing* et *xpath*) ont été employées afin de structurer le contenu. Enfin, les données ont été enregistrées dans des fichiers textes au format CSV (Rossy, 2021). Cette étape nous a permis de faciliter l'identification des données pertinentes et de mieux analyser les traces numériques qui nous

intéressent dans le cadre de notre étude. Le tableau 1 présente les trois forums sélectionnés et leurs caractéristiques.

Tableau 1. Présentation des forums de discussion sélectionnés abordant la fraude amoureuse

| ScamWarners | |
|--|--|
| Description | Ce site est composé de forums et de fiches d'informations visant à sensibiliser la population aux fraudes. Les principaux objectifs sont d'informer la population, d'identifier les individus à risque d'être victime d'une fraude, d'offrir du soutien aux victimes et d'aider les individus à mieux se protéger des escroqueries. |
| Origine de la création | Initiative publique |
| Langue employée | Anglais |
| Pays d'origine | Royaume-Uni |
| Nombre d'informations² extraites dans la base de données | 25 151 |
| Type de données disponibles | <ul style="list-style-type: none"> - Titre de la publication³ - Contenu de la publication - ID de la publication - Nom d'utilisateur de l'abonné - Nombre de publications publiées par l'abonné - Localisation de l'abonné - URL de l'abonné - Date de création du compte - Date de création de la publication - Date de la dernière réponse à la publication - Nombre de vues sur la publication - Nombre de réponses à la publication |
| ScamSurvivors | |
| Description | Ce site comporte des forums de discussion, des fiches d'information, un blogue, une galerie et des questionnaires visant à identifier un fraudeur. Ils traitent de tous les types de crimes, mais plus particulièrement de la sextorsion et de la fraude amoureuse. Les principaux objectifs de la plateforme sont de sensibiliser et d'éduquer la population, d'exposer les |

² Ici, on qualifie d'informations toutes données ayant pu avoir été extraites en fonction du forum concerné. Il peut s'agir d'informations relatives aux internautes participant au forum (pseudonyme, date de publication du message, adresse courriel, etc.) ou d'informations relatives au fraudeur dénoncé (adresse courriel, pseudonymes utilisés, numéro de téléphone, etc.). Se référer à la case suivante du tableau 1 pour voir les types de données disponibles sur les forums concernés.

³ Sur ce site, le pseudo de l'arnaqueur présumé fait parfois l'objet du titre de la publication. Ainsi, nous avons accès à cette trace numérique à partir de certains titres affichés.

| | |
|--|---|
| | fraudeurs et d'aider les victimes à se reconstruire à la suite d'une escroquerie. |
| Origine de la création | Initiative communautaire fondée par des bénévoles |
| Langue employée | Anglais |
| Pays d'origine | Royaume-Uni |
| Nombre d'informations extraites dans la base de données | 8274 |
| Type de données disponibles | <ul style="list-style-type: none"> - Titre de la publication⁴ - Contenu de la publication - ID de la publication - Nom d'utilisateur de l'abonné - Nombre de publications publiées par l'abonné - Localisation de l'abonné - URL de l'abonné - Date de création du compte - Date de création de la publication - Date de la dernière réponse à la publication - Nombre de vues sur la publication - Nombre de réponses à la publication |
| Signal-Arnaques | |
| Description | Signal-Arnaques.com est un site communautaire de signalement qui permet de référencer les escroqueries commises sur Internet. Le site permet d'informer ou d'aider un individu victime d'une arnaque. Les signalements sont réalisés à partir d'un formulaire et se distinguent en douze catégories, soit les arnaques de site d'annonces, financières, téléphoniques, de loterie, aux sentiments, d'emploi, de dons, l'hameçonnage (<i>phishing</i>), les arnaques sur les réseaux sociaux, les arnaques via PayPal, les sites internet frauduleux et les autres escroqueries. |
| Origine de la création | Initiative communautaire, fondée par une entreprise |
| Langue employée | Français, anglais, espagnol, italien et allemand ⁵ |
| Pays d'origine | France |
| Nombre d'informations extraites dans la base de données | 3786 |
| Type de données disponibles | <ul style="list-style-type: none"> - L'ID de la publication - Date de publication |

⁴ Sur ce site, le pseudo de l'arnaqueur présumé fait souvent l'objet du titre de la publication. Ainsi, nous avons accès à cette trace numérique à partir des titres affichés.

⁵ Sur ce site, il est possible de sélectionner la langue de préférence. Par conséquent, le contenu rédigé dans la langue choisie est disponible. Dans le cadre de notre étude, nous avons sélectionné la langue française, ayant ainsi accès aux publications uniquement rédigées dans cette langue.

| | |
|--|---|
| | <ul style="list-style-type: none"> - Le contenu de la publication partagée par la victime - Adresse courriel de l’arnaqueur - Pseudo de l’arnaqueur - Le numéro de téléphone de l’arnaqueur - Le type de téléphone - L’opérateur de téléphone - Le pays d’origine du numéro de téléphone - L’URL du faux profil - Arnaques similaires connexes |
|--|---|

Étant donné l’abondance des publications sur certains forums, particulièrement sur ScamWarners, nous avons dû sélectionner, pour mieux comprendre les mécanismes d’entraide en ligne des victimes de fraude amoureuse, certaines publications qui feraient l’objet d’une analyse qualitative plus approfondie afin de répondre à cet axe de notre recherche. Ainsi, nous avons choisi environ 1 000 messages⁶ (près de 335 dans chacun des forums de discussion) qui ont fait l’objet d’une analyse de contenu. Ces messages ont été sélectionnés en fonction de la longueur de la publication de base et du nombre de vues et de réponses (interactions) ayant été véhiculées par celle-ci. À cette fin, nous avons manuellement copié le contenu des publications sélectionnées dans le logiciel de codage QDA Miner pour faciliter l’analyse de contenu.

Ensuite, nous avons produit une grille de codage en fonction des données observées, nous permettant d’analyser le contenu sélectionné et d’en tirer des thématiques.

3.2. Les spécificités du terrain d’étude

Dans le cadre de notre étude, il a été nécessaire de nous pencher sur les particularités des forums de discussion en ligne afin d’en analyser le contenu de façon adéquate. Nous imprégner du vocabulaire et comprendre l’émotion par l’écrit ont été des étapes préalables à l’analyse de contenu.

3.2.1. Le vocabulaire employé sur les forums de discussion

De façon à interpréter correctement du contenu rédigé en ligne, il est nécessaire de définir le vocabulaire employé sur les forums de discussion. En effet, les forums de discussion détiennent des particularités générales, et certaines sont propres au site sur

⁶ Ici, par « messages », on fait référence aux publications de base et à leurs réponses.

lequel les forums opèrent. Le tableau 2 fait part des principaux concepts que l'on retrouve sur les forums de discussion en ligne.

Tableau 2. Terminologie des forums de discussion en ligne

| Concept | Définition |
|---------------------------|--|
| Message | Contribution à une discussion |
| Poster | Publier, mettre son message en ligne |
| Fil de discussion | Ensemble de messages par lesquels les différents utilisateurs conversent ou se répondent sur une thématique donnée |
| Topic | Sujet de discussion |
| Profil | Fiche complétée par l'individu donnant des informations diverses (âge, sexe, photographie, intérêts, etc.) |
| Smiley | Symbole destiné à préciser le ton d'un texte |
| Modérateur | Personne bénévole (ou non) veillant à respecter les normes et les règles établies par le forum |
| Avatar | Image utilisée pour se présenter |
| Pseudo, nom d'utilisateur | Identifiant permettant d'être reconnu sur le forum |
| Signature | Courte phrase apparaissant en bas de message du contenu libre (citation, lien, etc.) |
| Bio | Court paragraphe affiché sur le profil visant à parler de soi (intérêts) |
| Troll | Auteur de faux témoignages ayant, par exemple, pour but de créer une polémique sur le forum |

Source : Laplace, 2013.

3.2.2. L'émotion par l'écrit

En outre, il a été nécessaire de faire l'analyse de l'émotion sur les forums. Les disciplines comme la linguistique ou la psychologie ont produit de nombreux travaux portant sur cette dernière (Laplace, 2013). Des procédés sémio-discursifs ont été définis pour évoquer les émotions (tableau 3). Dans le cadre de notre étude, nous nous sommes servis de ceux-ci afin de donner sens au contenu des fils de discussion et des messages analysés.

Tableau 3. Procédés sémio-discursifs de l'émotion sur les forums de discussion en ligne

| Procédé | Définition | Exemple de segments ⁷ |
|--------------------|--|---|
| Procédés iconiques | Smileys constitués de signes de ponctuation :) ou sous forme numérique ☺ | « Hélas, c'est une fraude très très fréquente... et vous êtes tombé dans le piège 😞 » |

⁷ Les segments de texte sont issus des trois forums sélectionnés pour réaliser la présente étude.

| | | |
|---------------------------------------|---|---|
| Procédés graphiques ou typographiques | Utilisation de lettres majuscules, d'étirements graphiques, d'onomatopées, d'interjections, de la ponctuation de façon détournée en multipliant par exemple le même signe | « VERRRY IMPORTANT information on the photos romance scammer use [...] » |
| Énoncés d'émotions | Comprenant un terme d'émotion, un lieu psychologique et une source d'émotion | « After 3 weeks of no contact, and reassurance from the kind people on here, these feelings are gradually going, but a feeling of hurt as a result of the shock still lingers ». |
| Séquences de confiance | Témoignage qui accorde une place importante à l'émotion | « So basically, my message is one of hope, that things will get better, and to quote the old cliché, time is a great healer. And I also think its important in the healing process to share any feelings, so we can offer reassurance [...] » |

Source : Laplace, 2013.

3.3. Considérations éthiques particulières à cette étude

Bien que notre étude ne requière pas l'obtention d'un certificat éthique, puisqu'elle est considérée comme étant une recherche non intrusive basée sur Internet, nous devons tout de même considérer certains enjeux éthiques se rapportant à l'analyse de données textuelles rendues disponibles à travers les sites publics. De façon générale en recherche, toute information en ligne peut être analysée à condition qu'elle soit publiquement archivée, qu'aucun mot de passe ne soit nécessaire pour y accéder, qu'aucun règlement du site ne l'interdit et que le sujet ne soit pas très sensible⁸ (Burckman, 2004, cité par Laplace, 2013 ; Sugiura et al., 2016). Toutefois, l'absence de définition concernant ce qui constitue un « sujet très sensible » nous amène à avoir un regard critique quant au contenu que nous analysons. L'expérience frauduleuse pourrait être considérée comme très sensible pour certaines victimes alors que pour d'autres, non. En outre, l'extraction de données

⁸ Pour réaliser le présent travail, les directives du Comité éthique de l'Université de Montréal ont été suivies en ce sens.

impliquant des traces numériques et des informations identifiantes pourrait poser problème pour certains abonnés qui ne voudraient pas que celles-ci soient utilisées à des fins de recherche. Pour cette raison, nous avons pris la décision de ne pas révéler d'informations pouvant servir à identifier un abonné, qu'elles soient sensibles ou non (pseudonymes, adresses courriel, etc.).

3.4. Limites de l'étude

Plusieurs limites peuvent être soulevées à la suite de notre étude. Premièrement, nous devons tenir compte du fait que de nombreuses publications acquises sur les forums de discussion peuvent comporter des données incomplètes, ce qui peut limiter la profondeur de nos analyses (notamment en ce qui concerne les informations identifiantes des fraudeurs). Deuxièmement, nous tenons pour acquis que les personnes participant aux forums de discussion sont des victimes directes ou indirectes, puisque la majorité s'identifie comme telle, mais rien ne nous permet de confirmer cette présupposition. Il faut également tenir compte du fait qu'il y existe peut-être plusieurs typologies de victimes participant aux forums de discussion (par exemple, financière et non financière) et que celles-ci ne s'entraident pas nécessairement de la même façon. Par ailleurs, beaucoup d'individus fréquentent les forums de discussion sans y participer. La question de ce qu'ils font avec les informations qu'ils y trouvent ne peut être exploitée de façon satisfaisante. Notons également qu'il y existe un biais dans la sélection des publications et des sujets puisque la majorité des commentaires sont rédigés par une minorité d'utilisateurs. L'impossibilité d'observer ce que font les utilisateurs non participants aux échanges avec les informations constitue ainsi l'une des plus grandes limites de notre étude.

Chapitre 4 : Analyse et interprétation des résultats

Cette section présente les résultats issus de notre recherche. Notre recherche exploratoire sur les forums de discussion a dévoilé de nombreux enjeux se rattachant à la fraude amoureuse, qui pourraient donner lieu à une panoplie d'analyses optant pour des axes de recherche distincts. De façon à répondre à la question principale de l'étude concernant les mécanismes d'entraide en ligne entre les victimes de fraude amoureuse et à la question secondaire visant plus précisément la détection de traces numériques, nous

avons développé trois sections répondant concurremment aux deux axes de recherche. Chaque section présente des mécanismes d'entraide, dont la plupart intègrent des traces numériques sous différents angles.

La première section 4.1 aborde la façon dont les forums de discussion constituent un soutien et une voix pour les victimes. La section 4.2, pour sa part, présente la manière dont les victimes s'entraident mutuellement dans une lutte contre les cyberarnaqueurs. Les traces numériques seront d'ailleurs davantage abordées dans cette section. Finalement, la section 4.3 renvoie à la façon dont les victimes s'entraident afin d'informer et de sensibiliser les utilisateurs fréquentant les forums.

4.1. Les forums de discussion : un soutien et une voix pour les victimes

Cette première section traite de la façon dont les forums de discussion en ligne génèrent des mécanismes d'entraide entre les victimes de fraude amoureuse leur permettant de s'extérioriser par rapport à leur expérience. Cette section aborde la façon dont les internautes se réapproprient leur pouvoir et leur capacité d'agir grâce aux forums de discussion.

4.1.1. Le témoignage écrit : une forme de libération et de soutien moral

Sur les trois forums de discussion étudiés, un bon nombre de publications font l'objet de témoignage écrit concernant l'expérience victimaire. En effet, plusieurs victimes se tournent vers ces plateformes afin de partager leur histoire et font part des conséquences émotionnelles et financières générées par l'escroquerie. À la suite de la publication du témoignage, plusieurs internautes vont généralement intervenir pour offrir un soutien à la victime et saluer son courage. Dans ce mécanisme d'entraide, les abonnés sont moins portés à échanger entre eux, ils répondent plutôt à la publication originale. De façon générale, le témoignage écrit se manifeste différemment en fonction du statut de la victime, à savoir si la fraude est reconnue et acceptée ou non par l'auteur de la publication. Ainsi, le mécanisme d'entraide fondé sur le témoignage écrit vise deux objectifs différents. D'une part, certains témoignages sont livrés dans le but d'obtenir des conseils et du soutien sur la façon de procéder vis-à-vis une fraude. L'arnaque est à ce stade encore active, pas

nécessairement reconnue et non acceptée par la victime. Les participants vont alors intervenir en partageant leur avis à l'égard des informations qui ont été dévoilées dans le témoignage et proposer diverses actions à l'auteur(e) de la publication d'origine. Ici, la victime, qu'elle ait versé un montant d'argent ou non, commence à douter de la personne avec qui elle entretient une relation en ligne. Elle se tourne alors vers les forums de discussion afin d'envisager l'avis d'anciennes victimes ou d'internautes informés quant à sa situation. Le témoignage livré est, dans ces cas, davantage destiné à démasquer et à mettre fin à une fraude qu'autre chose. Il explique la situation tout en faisant part des émotions véhiculées par celle-ci. Ceci renvoie également à un mécanisme d'entraide davantage élaboré dans la troisième section, qui aborde les astuces visant à démasquer une arnaque. Voici un extrait d'une publication illustrant la façon dont le mécanisme d'entraide fondé sur le témoignage écrit a comme but d'élucider la nature d'une relation virtuelle entre un fraudeur et une victime :

Aujourd'hui, je m'adresse à vous parce que je ne sais pas quoi faire. Je suis Belge et j'ai été et le suis toujours, victime d'une fraude sentimentale. [...] J'espère que quelqu'un pourra m'aider réellement ici ou au moins me conseiller, c'est vraiment la seule chose dont j'ai besoin, de conseils. Alors, voilà mon histoire [...] Il y a une semaine, j'ai rencontré une personne sur le web qui m'a dit être à l'étranger et s'être fait voler. [...] Ma question donc est, que dois-je faire? Dois-je continuer pour cette fois-ci ?

Réponse :

Hélas, c'est une fraude très très fréquente... et vous êtes tombé dans le piège 😞, à l'étranger et s'être fait voler tous ses papiers... 😞 Surtout, ne refaite aucune transaction avec lui, ce n'est qu'un chèque volé, et lorsque vous allez remettre le chèque en banque, il reviendra impayé [...]

(Extrait du forum Signal-Arnaques).

Dans d'autres situations, le partage de témoignages écrits sur les forums de discussion a un tout autre objectif, soit celui de se « libérer » de l'expérience frauduleuse et victimaire. La victime cherche à s'affranchir d'un état de dépendance vis-à-vis l'escroquerie sentimentale pour s'émanciper. Ici, l'individu victimisé partageant son témoignage est au cœur du mécanisme – il utilise les forums de discussion comme outil pour s'enlever, en quelque sorte, un poids des épaules. Le contenu fait fréquemment part de séquences de confiance et d'énoncés d'émotions. Ces derniers s'accompagnent parfois

de procédés iconiques visant à illustrer le sentiment véhiculé par le message. Raconter son expérience devient ici un outil d'*empowerment* - le témoignage écrit est une méthode s'inscrivant dans une perspective de développement et l'auteur acquiert la maîtrise de ses moyens pour reprendre le contrôle de sa vie et s'épanouir. Témoigner de son expérience devient ainsi une manière de reconnaître la fraude et de l'accepter. La victime est prête à reprendre le contrôle sur sa vie. Pour entamer son processus de reconstruction, elle nécessite l'encouragement et le soutien moral de ses semblables et des internautes. Par ailleurs, il s'agit d'un outil à travers duquel la victime peut témoigner de façon anonyme, avec un pseudonyme fictif, limitant ainsi le jugement d'autrui qui pourrait être craint par certains des individus victimisés. Comme il a été mentionné dans la revue de littérature, plusieurs victimes se sentent humiliées et sont dépourvues de ressources vers lesquelles se tourner à la suite d'une fraude. Les forums de discussion en ligne leur permettent ainsi d'exprimer leurs points de vue et leurs sentiments, sans avoir à passer à travers des organisations et sans avoir à se sentir jugées par des personnes en situation d'autorité. Les témoignages écrits rappellent les groupes de soutien dans leurs bienfaits puisqu'ils permettent de mieux faire face à l'expérience frauduleuse et de mieux gérer les conséquences qui l'accompagnent en obtenant un soutien moral. Voici un extrait d'une publication illustrant le mécanisme d'entraide fondé sur le partage de témoignage écrit :

J'espère que tu seras soulagée d'avoir eu le courage de te confier même après si longtemps et je sais que malgré tes problèmes importants de santé que tu es soutenue par ton partenaire [...] (Extrait du forum Signal-Arnaques).

Ce mécanisme s'est plus particulièrement manifesté sur la plateforme Signal-Arnaques. En effet, sur les deux autres forums de discussion sélectionnés (anglophones), le partage de témoignage est beaucoup moins fréquent. Ceci peut être dû au fait que les normes sociales des plateformes ScamWarners et ScamSurvivors sont différentes de celles de Signal-Arnaques. Comme il a été mentionné dans la recension des écrits, Del Teso Craviotto (2006) suggère que les sites de rencontre s'apparentent à une communauté dans laquelle les utilisateurs partagent et dessinent un ensemble d'idées communes afin de permettre une communication cohérente fondée sur un langage, des règles de conversation et des mécanismes d'inférence communs. Cette idée pourrait également s'appliquer aux forums de discussion utilisés par les victimes de fraude amoureuse. Ainsi, les trois forums choisis

auraient des normes et des mécanismes d'inférence propres, ce qui pourrait en partie expliquer pourquoi les témoignages écrits sont davantage valorisés et fréquents sur Signal-Arnaques qu'ils ne le sont sur les forums anglophones. En effet, ces derniers semblent davantage destinés à partager des informations frauduleuses et à fournir de l'information plutôt que de servir de plateforme pour raconter le récit de sa propre expérience. En outre, d'autres hypothèses pourraient être celles selon lesquelles les utilisateurs francophones seraient culturellement davantage portés à se tourner vers les forums de discussion en ligne pour témoigner ou encore qu'ils disposent de moins de ressources pour les accompagner dans leur expérience frauduleuse, les dirigeant ainsi vers le monde en ligne pour trouver une forme de soutien.

4.1.2. L'identification à son semblable : un moyen pour briser l'isolement

Notre analyse a également fait ressortir la façon dont l'identification à son semblable constitue un mécanisme d'entraide important pour les victimes qui cherchent à briser l'isolement auquel elles sont fréquemment confrontées à la suite de l'expérience frauduleuse. En effet, participer à des échanges impliquant des individus ayant vécu des expériences similaires permet à la victime de démentir l'impression selon laquelle elle est seule à vivre une fraude amoureuse. L'analyse de contenu a notamment dévoilé que certaines victimes n'osent pas partager leur expérience avec leurs proches, par crainte d'être incomprises, prises pour des idiots, voire réprimandées par ceux-ci. Notons toutefois que dans certains cas les victimes ne désirent pas partager leur expérience puisqu'elle implique une situation d'infidélité. Cet exemple permet d'illustrer cette idée :

Je ne sais pas quoi faire car il détient quelques photos de moi pas très honorables et je n'aimerais pas qu'il les publie sur le web car je pense que cela est possible, j'ai peur de la suite. Dois-je le bloquer ou dois-je lui dévoiler que j'ai découvert l'arnaque ? Mon mari ne sait pas bien sûr et je ne veux pas qu'il découvre ma bêtise. Si je ne réponds pas, va-t-il s'énerver? Que faire? Merci pour vos retours et votre aide. (Extrait du forum Signal-Arnaque).

Les forums de discussion permettent aux individus semblables d'échanger sur leur situation et de partager une compréhension commune des enjeux qui se rattachent à une escroquerie sentimentale. Ce mécanisme d'entraide est essentiel pour passer au travers de l'expérience frauduleuse. Notons qu'une escroquerie sentimentale implique une

victimisation particulière, d'une part, puisque les autorités ne détiennent généralement pas les ressources ni les moyens d'arrêter un individu à l'étranger et, d'autre part, car il est quasiment impossible de récupérer les montants pécuniaires perdus. Ainsi, il peut être difficile pour une victime de tourner la page. Se rendre compte que d'autres individus vivent les mêmes conséquences permet ainsi aux victimes de briser leur isolement, de partager un vécu souvent incompris par des personnes non victimes et de graduellement accepter la fraude pour en tirer des pensées positives. L'extrait suivant permet d'illustrer cette idée. Ici, un internaute répond à une publication écrite par une victime, lui indiquant qu'elle n'est pas seule à s'être fait prendre par une arnaque amoureuse :

Mais il ne faut pas vous en vouloir. Vous n'êtes ni le premier, ni malheureusement le dernier à vous faire piéger ainsi. Et certains ont perdu de véritables fortunes à ce jeu-là. [...] (Extrait du forum Signal-Arnaques).

En outre, la majorité des publications génèrent quelques réponses, et les échanges impliquent généralement une minorité d'utilisateurs qui se répondent mutuellement. Toutefois, le nombre de vues sur chacune des publications est souvent très élevé, indiquant qu'un bon nombre de victimes « présumées » consultent les forums sans toutefois y participer. Le mécanisme d'entraide fondé sur l'identification à son semblable peut ainsi prendre forme à travers l'action non participante puisque les individus victimisés ont librement accès au contenu des messages et peuvent ainsi trouver le réconfort ou l'information nécessaire pour mieux gérer l'expérience frauduleuse dont ils sont victimes ou témoins. Le tableau 2 fait part du nombre moyen de réponses et de vues générées par les publications tirées des forums de discussion. À la lecture de celui-ci, on constate que ScamWarners génère énormément de publications visant à signaler un arnaqueur, mais qu'il s'agit du site où les internautes échangent le moins entre eux. À l'inverse, Signal-Arnaques démontre une faible abondance de publications originales, mais génère énormément de vues. Dans tous les cas, ceci indique qu'un nombre important d'internautes consultent les publications sans y participer, indiquant possiblement que des victimes les lisent pour en apprendre davantage sur les enjeux se rapportant à une arnaque sentimentale ou pour prendre connaissance de situations similaires à celle dans laquelle elles sont peut-être piégées.

Tableau 4. Nombre moyen de réponses et de vues sur les forums de discussion

| Forum | Nombre de publications extraites | Moyenne de réponses | Moyenne de vues par publication |
|------------------------|---|----------------------------|--|
| Signal-Arnaques | 37* | 8 | 4764 |
| ScamWarners | 25 150 | 3 | 1637 |
| ScamSurvivors | 6916 | 4,5 | N/É |

*Le site Signal-Arnaques comporte une section *forum* et un formulaire de *signalements*. Les informations concernant les traces numériques ont été extraites à partir des signalements et non des publications des forums. Ceci explique pourquoi le chiffre ici présenté est beaucoup plus bas que celui affiché dans le chapitre sur la méthodologie. Les analyses traitant du premier axe de recherche portant sur les mécanismes d'entraide sont, pour le site Signal-Arnaque, fondées sur les 37 publications dont nous parlons ici. Les deux autres forums ne font pas la distinction entre ces deux outils, raison pour laquelle les chiffres sont les mêmes.

4.1.3. L'accompagnement : un mécanisme pour se reconstruire

L'analyse des forums de discussion a également dévoilé un mécanisme d'entraide entre les victimes fondé sur l'accompagnement. Évidemment, la participation aux forums de discussion, tous sujets confondus, a souvent comme objectif d'accompagner les autres abonnés requérant une certaine forme d'aide. Toutefois, pour les victimes d'arnaque sentimentale, l'accompagnement agit comme un moyen de reconstruction de soi à la suite de l'expérience frauduleuse. En effet, il s'agit ici d'utiliser les leçons tirées de sa propre expérience pour accompagner et conseiller d'autres individus ayant été victimes de fraude. Ce mécanisme prend forme lorsque la victime accepte le résultat de son expérience et est prête à épauler son prochain. La victime agit alors comme mentor et conseiller sur le forum. Elle connaît bien les arnaques, les stratagèmes et les *modus operandi*; elle est en mesure de participer activement aux échanges entre les internautes. Elle surmonte les conséquences financières et émotionnelles en donnant un sens à son expérience frauduleuse. Accompagner des victimes réelles et potentielles lui permet de faire preuve de résilience et de se libérer d'un état de sujétion vis-à-vis les impacts de l'arnaque. Voici un extrait visant à illustrer cette idée. Il s'agit d'une réponse à un témoignage écrit d'une victime se disant prête à aller de l'avant :

Maintenant [...], c'est toi qui aide des victimes dans tes groupes et tu sais que tu peux compter sur les uns et les autres [...] Moi je lui redis Merci même si cet ami le fait en toute simplicité et sans attendre quoique ce soit en retour [...] (Extrait du forum Signal-Arnaques).

Dans ce message, on constate le rôle de conseiller que prend la victime une fois son processus de reconstruction entamé. Celle-ci s'est fait aider durant son expérience, et c'est dorénavant à elle d'accomplir cette tâche auprès d'autres victimes. Comme l'illustre le prochain extrait, ce mécanisme d'entraide implique que l'individu concerné puisse passer d'un statut de victime à celui de survivant. Ce rôle s'accompagne d'une responsabilité, soit celle de prévenir des escroqueries et d'accompagner les personnes qui en ont été victimes.

Closure. You want closure? To do this, you must change your own mind from that of a victim to that of a survivor. This helps you remove him from your life and also helps other victims of the same scammer, who has many more hooked at that moment. You must realize that you are not the only victim of him at that point in time or in the future and that posting his details can and does save others from falling to the same scammer. Your posts here can and do save real lives. (Extrait du forum ScamSurvivor).

Ce mécanisme d'entraide indique qu'il y existerait plusieurs stades de la victimisation présentant deux types de victimes formant la communauté des forums de discussion. D'un côté, il y aurait les « nouvelles » victimes, caractérisées par leur méconnaissance du phénomène de la fraude amoureuse et leur candeur vis-à-vis les arnaqueurs et les stratagèmes frauduleux. D'un autre, il y aurait les « anciennes » victimes, dorénavant qualifiées de victimes survivantes et caractérisées par leur résilience, leur connaissance des enjeux liés aux escroqueries sentimentales et par leur rôle d'accompagnement. Les internautes participeraient différemment aux échanges en fonction du cheminement réalisé dans leur processus de victimisation.

4.2. Les forums de discussion : une lutte contre les cyberarnaqueurs

Cette seconde section fait part de la façon dont les internautes et les victimes d'arnaque sentimentale utilisent les forums de discussion comme moyen pour lutter contre les fraudes et les cybercriminels. L'axe de recherche visant à analyser les traces numériques est particulièrement abordé dans cette section puisque les mécanismes d'entraide sont fondés sur celles-ci.

4.2.1. Le signalement et le partage de profils frauduleux : une abondance de traces numériques

L'un des principaux moyens d'entraide sur les forums de discussion en ligne consiste à signaler les profils malveillants issus des différents sites de rencontre ou de réseaux

sociaux. Ce mécanisme s'est manifesté en abondance sur les trois forums étudiés de façon similaire. Sur les forums de discussion anglophones ScamWarners et ScamSurvivors, les internautes créent des publications dont le titre constitue une information identifiante relative au profil frauduleux. Le contenu des messages varie, mais constitue généralement un copier-coller des échanges en ligne du fraudeur avec la victime et de traces numériques diversifiées (pseudonymes, numéro de téléphone, adresse courriel, photographies volées, etc.) pouvant permettre de retracer et de signaler un individu avec des intentions malveillantes. Notons que sur le site francophone Signal-Arnaques, un formulaire de signalement est disponible, faisant en sorte qu'une bonne partie des publications partagées dans le forum est destinée à traiter d'autres enjeux (témoignages, entre autres). Toutefois, l'outil de signalement donne accès à une abondance de traces numériques pouvant être utiles afin d'établir des liens entre des profils frauduleux, comme c'est le cas pour les forums anglophones. Cet outil rappelle notamment les IOC (*indicators of compromise*) que les professionnels du domaine de la cybersécurité s'échangent afin de fournir des renseignements à leurs semblables sur les attaques dont ils sont victimes afin d'éviter que d'autres organisations ne soient affectées par celles-ci. Les plateformes de signalement peuvent ainsi répondre au même genre d'objectifs que le IOC et peuvent à la fois être utiles pour les internautes généraux que pour les professionnels luttant contre la fraude amoureuse.

Le partage de faux profils est un mécanisme d'entraide visant à lutter contre les arnaques sentimentales en misant sur la prévention. En effet, partager un profil frauduleux permet aux internautes qui consultent les forums et à ceux qui s'informent sur ces profils à partir de moteurs de recherche (p. ex. : Google) d'être alertés quant aux individus malveillants, limitant ainsi l'opportunité criminelle d'un arnaqueur. Exposer les informations permettant d'identifier un faux profil permet aux victimes potentielles de démasquer la fraude avant qu'elles ne tombent dans le piège. Ce mécanisme permet aux victimes d'agir activement afin de lutter contre les fraudes amoureuses et de prévenir que de potentielles victimes se retrouvent dans la même situation.

D'un point de vue de la criminalistique, ce mécanisme d'entraide est particulièrement intéressant afin d'exploiter les traces numériques à des fins de renseignement criminel. En effet, l'extraction de données numériques disponibles sur les forums nous donne accès à

une panoplie d'indications concernant les auteurs présumés des infractions. Par exemple, la carte 1 présente la provenance (connue) des numéros de téléphone tirés de l'extraction de données du site Signal-Arnaques.

Carte 1. Provenance des numéros de téléphone signalés, Signal-Arnaques.



À la lumière de cette carte, on constate que les numéros de téléphone signalés proviennent de 26 pays différents. Presque l'entièreté des numéros provient de la France (1303). Ceci pourrait venir déconstruire l'idée populaire selon laquelle la majorité des arnaqueurs exécuteraient les arnaques depuis l'Afrique. En outre, ceci pourrait indiquer que les escrocs étrangers entretiennent des liens avec des complices en France ou encore qu'ils utilisent des outils technologiques pouvant cacher la réelle localisation associée au numéro de téléphone. Nous pouvons ici faire un lien avec la typologie de fraudeurs énoncée par Rege (2009) qui propose qu'une partie des fraudeurs sentimentaux agissent en petit groupe ou à travers un large réseau criminel. On retrouve également quelques cas en Côte d'Ivoire (32), au Bénin (28), aux États-Unis (23), au Royaume-Uni (15) et au Canada (14) (voir l'Annexe 3).

4.2.2. Le partage du contenu des conversations entre un fraudeur et une victime : reconstruction de modus operandi fondé sur les traces numériques

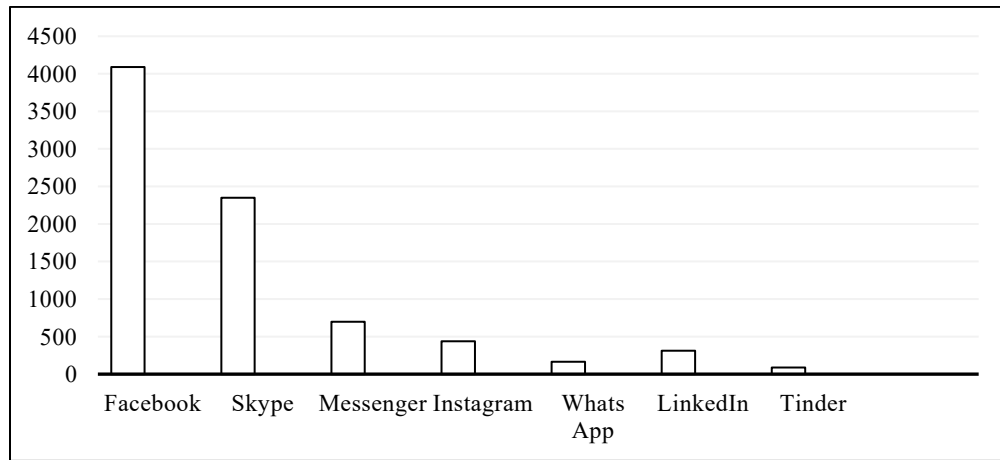
Dans le même ordre d'idées, plusieurs victimes partagent le contenu des conversations qu'elles ont entretenues avec les fraudeurs dans les forums de discussion. Notre analyse de contenu a démontré que les échanges sur les diverses plateformes de communication laissent de nombreuses traces numériques permettant de reconstruire les modus operandi des arnaqueurs sentimentaux. En effet, au-delà de pouvoir fournir des indications quant à l'anatomie de la fraude et à l'identification des auteurs présumés, les témoignages écrits et le partage de conversations fournissent des traces numériques pouvant contribuer à reconstruire les modus operandi des cyberarnaqueurs sentimentaux, notamment en ce qui concerne les outils technologiques dont ils se servent pour concrétiser leurs intentions malveillantes.

Par exemple, nous avons pu réaliser une analyse qui concerne les réseaux sociaux utilisés par les fraudeurs afin de rentrer en contact avec de potentielles victimes. Le graphique 1 fait part du nombre de publications de signalement comportant le nom d'un réseau social dans son contenu sur le forum Scam Warners. Le graphique 2, pour sa part, présente les fournisseurs de service courriel les plus utilisés par les faux profils ayant été signalés sur la plateforme Scam Survivors. Ces informations sont intéressantes puisqu'elles permettent d'identifier les plateformes les plus à risque d'héberger un profil frauduleux. Ainsi, les compagnies concernées peuvent mettre en place des mesures visant à mieux protéger leurs abonnés et à éviter la création de faux profils. En outre, en connaissant davantage les réseaux sociaux et les fournisseurs de service courriel employés par les fraudeurs, les victimes potentielles peuvent être mieux outillées afin de démasquer une intention malveillante.

La figure 1 nous permet de constater que Facebook est la plateforme la plus utilisée par les escrocs sentimentaux (4089), suivie de Skype (2350). Certains autres réseaux sont utilisés comme outil par les arnaqueurs, mais de façon moins importante. Notons toutefois ici que notre analyse fait part des signalements faits entre 2013 et 2021. Certaines plateformes ont gagné en popularité plus tard que d'autres. Il pourrait s'avérer intéressant de faire une analyse des réseaux sociaux mentionnés dans les publications pour chacune

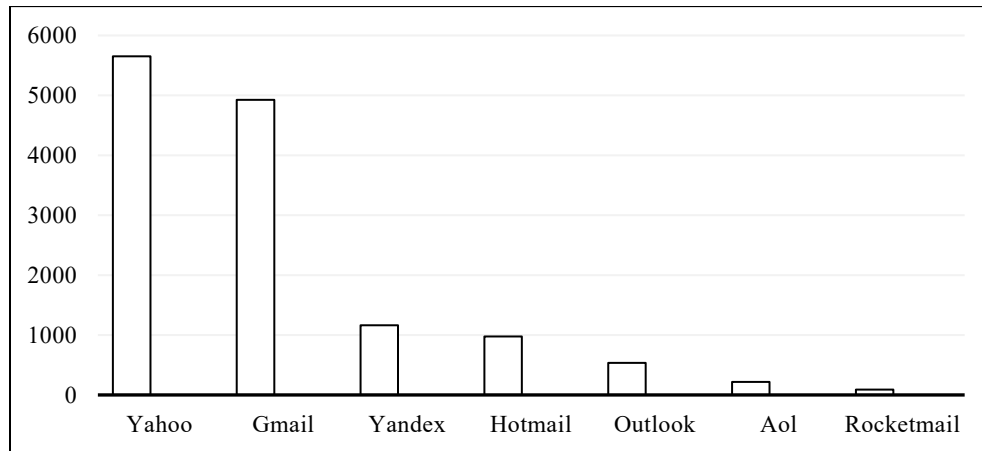
des années, de façon à déterminer quels moyens de communication gagnent en popularité auprès des arnaqueurs sentimentaux puisque, comme mentionné précédemment, les stratagèmes frauduleux évoluent conjointement avec le développement des réseaux sociaux.

Figure 1. Nombre de fois qu'un réseau social est mentionné dans une publication d'origine, ScamWarners, 2013 à 2021



La figure 2 nous permet de constater que les fournisseurs de service les plus utilisés par les arnaqueurs sentimentaux sont Yahoo (5651) et Gmail (4926). Notons également que la plupart des adresses courriel signalées détiennent un nom de domaine *.com*, pouvant ainsi complexifier la démarche d'investigation visant à déterminer la provenance d'une adresse. Toutefois, il demeure intéressant de se pencher sur les fournisseurs les plus utilisés de façon à mieux prévenir la création de faux profils auprès des compagnies concernées. En outre, il pourrait s'avérer pertinent de déterminer quels sont les facteurs de protection qui font en sorte que les autres fournisseurs de service courriel sont moins affectés par les fraudes amoureuses et la création de faux comptes.

Figure 2. Nombre de fois qu'un fournisseur de service courriel est mentionné dans une publication d'origine, ScamSurvivors, 2013 à 2021.



En bref, bien que nos analyses de données soient limitées dans le cadre de la présente recherche, notre extraction de données démontre que le partage et le signalement de profils frauduleux constituent un mécanisme d'entraide débordant de traces numériques pouvant être utilisées à des fins de renseignement visant la prévention, voire l'investigation dans certains cas. Puisqu'une importante partie de victimes ne porte jamais plainte, les forums de discussion et les plateformes de signalement constituent l'une des formes de registres comportant le plus d'informations pertinentes qui puissent contribuer à établir des patterns criminels en matière d'arnaque sentimentale. On retrouve notamment des traces numériques relatives aux numéros de téléphone (provenance, entre autres), aux adresses courriel (fournisseur de services et nom de domaine impliqués), aux réseaux sociaux utilisés par les fraudeurs, au contenu de leurs messages, aux photos qu'ils utilisent, réutilisent et partagent, et au calendrier de leur fraude (dates des échanges).

4.3. Des plateformes d'informations et de sensibilisation

En outre, les forums de discussion constituent de précieux outils en matière de partage d'informations et de sensibilisation vis-à-vis les escroqueries amoureuses. Notre analyse de contenu a notamment dévoilé qu'une importante partie d'internautes luttent contre les fraudes amoureuses en participant activement aux échanges prévus sur les plateformes. Ceux-ci partagent plusieurs astuces et informations générales visant à éduquer les autres utilisateurs quant aux risques liés aux rencontres en ligne et aux actions à entreprendre s'ils sont confrontés à une potentielle arnaque.

4.3.1. Les astuces pour démasquer une arnaque

L'un des mécanismes d'entraide fondés sur la sensibilisation consiste au partage d'astuces visant à démasquer une escroquerie sentimentale. Lorsqu'une publication d'origine fait état d'une situation dans laquelle un internaute doute des intentions de son interlocuteur virtuel, certains abonnés vont intervenir pour partager une opinion et fournir des astuces pour convaincre l'auteur de la publication qu'il est bel et bien confronté à une tentative de fraude. Ces interventions sont fréquemment faites par des victimes « survivantes » ou d'internautes au courant des tendances frauduleuses liées aux sites et applications de rencontre. Ce mécanisme d'entraide vise d'abord et avant tout à prévenir qu'une arnaque présumée se concrétise et que l'individu concerné se fasse duper.

En outre, certaines publications d'origine contiennent des informations visant à sensibiliser les utilisateurs aux risques liés aux arnaques sur Internet. Les abonnés d'un site peuvent ainsi consulter ces publications, parfois rédigées par les modérateurs et créateurs de la plateforme, parfois écrites par des utilisateurs désirant lutter contre les escroqueries. Les forums de discussion sont ainsi des outils préventifs, grâce auxquels la population générale peut s'éduquer et prendre connaissance de situations réelles et concrètes⁹. Puisque les modes opératoires des arnaqueurs sont fréquemment similaires, les internautes peuvent établir des liens entre la situation qui les concerne et celles partagées sur les forums, leur permettant de déterminer s'ils sont victimes d'une escroquerie ou non. L'extrait suivant illustre le mécanisme d'entraide fondé sur le partage d'astuces visant à démasquer une fraude. Ici, la publication a comme but d'informer les internautes quant aux modes opératoires des arnaqueurs et des étapes d'une arnaque sentimentale typique :

Usually, the main reasons for money requests are : medical bills for an illness of the scammers' child he can not deal with, while being abroad for business; unexpected costs due to a new contract signed by the scammer abroad or partnership in a recent business developed by the scammer abroad, able to bring huge revenues; accidents affecting the scammer /robbery letting the scammer without money and documents [...] (Extrait du forum ScamSurvivors)

⁹ Cette idée est fondée sur le nombre de vues générées par chacune des publications. Plusieurs internautes consultent les forums, sans toutefois y participer.

À la lecture de cet extrait, on constate que l'auteur du message tente d'informer les abonnés quant aux principales raisons évoquées par le fraudeur pour solliciter un montant d'argent à sa victime. Le message fournit des astuces permettant de déceler une situation frauduleuse.

Par ailleurs, les traces numériques sont pertinentes dans ce mécanisme puisqu'elles peuvent permettre aux internautes de démasquer une arnaque lorsque de nombreux indices indiquent qu'une fraude est en cours. Par exemple, une publication d'origine qui contient certains éléments (une adresse courriel avec un nom de domaine *.com*, une méthode de paiement telle que Western Union ou MoneyGram ou encore un profil avec une courte liste d'amis) fournit des indices aux abonnés participant aux échanges pour démasquer une intention malveillante et en faire part à l'auteur de la publication ayant sollicité de l'aide.

4.3.2. Les astuces pour couper le contact avec un cyberarnaqueur

Dans le même ordre d'idées, les victimes de fraude amoureuse s'entraident en partageant des astuces visant à couper le contact avec un interlocuteur aux intentions malveillantes. En effet, puisque les arnaques sentimentales sont souvent caractérisées par une victimisation répétée (en raison notamment du chantage qui l'accompagne régulièrement), il est important pour les abonnés d'être au courant des actions à entreprendre pour couper tout contact avec les fraudeurs de façon à détruire le pouvoir qu'il détient sur sa victime. De plus, ce mécanisme d'entraide vise également à rassurer la victime sollicitant de l'aide. Les internautes cherchent à lui faire comprendre qu'elle n'est pas seule à vivre ce genre d'expérience et que les fraudeurs mettent rarement leurs menaces à exécution. Couper les liens avec l'individu est la meilleure façon de mettre fin à l'arnaque en cours. De ce fait, plusieurs internautes accompagnent la victime pour qu'elle puisse clore cette expérience et mettre un terme à la relation qu'elle entretient avec un arnaqueur. Ils lui fournissent des conseils et lui apportent du soutien à travers les échanges sur le forum concerné. Les deux extraits suivants sont des réponses issues d'une publication d'origine faisant le récit d'une fraude amoureuse par une victime qui cherche conseils auprès d'internautes informés. Ceux-ci illustrent cette idée selon laquelle les participants aux forums accompagnent la victime pour qu'elle fasse cesser l'arnaque :

Surtout, ne refaites aucune transaction avec lui, ce n'est qu'un chéquier volé, et lorsque vous allez remettre le chèque en banque, il reviendra impayé et vous lui aurez envoyé de l'argent pensant qu'il était de bonne foi [...]

Vous êtes trop dur avec vous-même. Je ne dirais pas [que vous êtes] "trop bon, trop con". Mais plutôt trop bon, trop vulnérable. Si on peut se demander pourquoi toutes les arnaques fonctionnent encore, c'est simple. On ne naît pas avec la malveillance inscrite dans nos gènes. Autrement dit, quand on est jeune, avec un caractère tel que le vôtre, c'est-à-dire gentil, on ne sait pas encore jusqu'où peut aller la perversité. On a simplement bon cœur [...](Extrait du forum Signal-Arnaques).

Par ailleurs, un bon nombre d'internautes participant aux forums de discussion sont des victimes indirectes d'une arnaque. Par exemple, il s'agit souvent de proches d'une victime qui désire amener cette dernière à réaliser que la relation qu'elle entretient virtuellement est une escroquerie. Cet extrait permet d'illustrer cette situation :

Bonjour, nous venons de découvrir que ma mère, 72 ans, est (probablement) victime d'une fraude et nous sommes désespérés. Nous sommes aussi inquiets pour sa sécurité. Ma mère vit seule et (relativement) isolée, socialement, en dehors de la famille. Elle a décidé récemment de chercher à rencontrer quelqu'un (ce n'est que mieux), mais semble être tombée dans un piège à l'arnaque sentimentale [...] Elle a eu une communication téléphonique avec une personne (elle dit s'être rendu compte que cette personne ne parlait pas de la même manière qu'elle écrivait, mais sans plus) et a (probablement) envoyé de l'argent [...] Elle reste sur la défensive, malgré nos tentatives d'en savoir un peu plus, ou d'essayer de la mettre en garde. Pour le reste, elle est dans le déni. (Extrait du forum Signal-Arnaques).

Les astuces pour démasquer une fraude et y mettre fin sont ainsi des outils particulièrement recherchés par ces abonnés afin de lutter contre une arnaque sentimentale qui les concernent intimement ou non. Plusieurs internautes vont partager ces conseils en renvoyant à leur propre expérience.

4.3.3. Les institutions et les organismes à contacter

En outre, toujours dans une optique d'information et de sensibilisation, les internautes et les victimes échangeant sur les forums de discussion partagent également des informations quant aux actions à entreprendre pour rapporter une arnaque aux autorités. Notons toutefois que notre analyse de contenu a dévoilé qu'un bon nombre de victimes éprouvent une certaine réticence à contacter les organisations policières : « Porter plainte n'arrangera en rien ma situation » (Extrait du forum Signal-Arnaques). Étant donné les très

faibles chances d’obtenir une réclamation des frais pécuniaires perdus et du sentiment de honte et d’humiliation qui accompagnent fréquemment la victimisation, peu de victimes signalent l’escroquerie auprès des institutions. Toutefois, plusieurs s’intéressent aux organisations existantes pouvant leur fournir du soutien et de l’aide afin de se reconstruire à la suite de leur expérience frauduleuse. De ce fait, les utilisateurs des forums de discussion vont échanger afin d’informer les individus qui fréquentent les plateformes des diverses options s’offrant aux victimes pour être accompagnées par un organisme reconnu au travers de leur processus victimaire.

La méfiance vis-à-vis les institutions est un enjeu intéressant pouvant en partie expliquer la sous-déclaration des arnaques amoureuses auprès des autorités. Les forums de discussion sont ainsi un terrain d’étude alternatif aux données policières afin de considérer l’ampleur des escroqueries sentimentales de manière plus exhaustive. En bref, ils sont des plateformes d’information et de sensibilisation pour les utilisateurs, mais également des outils informatifs pour les chercheurs afin d’avoir accès aux tendances et aux enjeux récents liés aux fraudes amoureuses.

Le tableau 5 résume les divers mécanismes d’entraide issus de notre recherche et présente leur(s) objectif(s) et la pertinence des traces numériques pour chacune des méthodes présentées. Il est également classé en fonction des mécanismes les plus fréquemment dénotés dans les publications analysées.

Tableau 5. Les mécanismes d’entraide entre les victimes de fraude amoureuse

| Mécanismes d’entraide en ligne des victimes de fraude amoureuse | | | |
|--|--|--|---|
| Rang | Méthode | Objectif(s) | Pertinence des traces numériques |
| 1 (Dénoté en abondance sur les | Le signalement et le partage de profils frauduleux | Prévenir des cas de fraude Exposer les cybercriminels Établir des liens entre les cyber-arnaqueurs | Le partage de photographies volées, de pseudonymes, d’adresses courriel, de numéros de téléphone, etc. permet d’établir des liens entre des cas de fraude et de limiter l’opportunité criminelle des fraudeurs. |

| | | | |
|--|--|---|--|
| trois sites concernés ¹⁰) | | | |
| 2 (Dénotés sur les trois forums concernés et plus particulièrement sur Signal-Arnaques) | L'accompagnement et la participation active sur les forums | Prévenir des cas de fraude Donner un sens à son expérience (se reconstruire) | Partager les traces numériques de façon active sur les forums permet d'avoir un registre à jour des informations identifiantes associées à des escrocs, permettant ainsi de mieux prévenir une victimisation multiple. |
| 3 Dénotés sur les trois forums concernés | Partage d'astuces pour démasquer une escroquerie | Prévenir des cas de fraude Exposer les cybercriminels | Reconnaître les <i>patterns</i> dans les traces numériques considérées douteuses permet d'identifier une intention malveillante. |
| 4 Dénotés sur les trois forums concernés | Partage d'astuces pour interrompre le processus frauduleux | Prévenir la concrétisation d'une fraude Prévenir la victimisation répétée | N/A |

¹⁰ Rappelons que le site Signal-Arnaques comporte une plateforme expressément liée à ce mécanisme d'entraide (qui n'est pas un forum en soi).

| | | | |
|--|---|--|--|
| <p>5</p> <p>Dénoté sur les trois forums, mais principalement sur Signal-Arnaques</p> | <p>Le témoignage écrit</p> | <p>Trouver un soutien moral Prévenir des cas de fraude Démâquer une tentative de fraude Se libérer du poids de la fraude Reconstruire un mode opératoire</p> | <p>Présence de nombreuses traces numériques (pseudonymes de divers réseaux sociaux, adresses courriel, photos, moyens de transfert d'argent, numéros de téléphone, etc.) permettant de reconstruire l'anatomie de la fraude et les modus operandi employés par les cybercriminels.</p> |
| <p>6</p> <p>Dénotés sur les trois forums</p> | <p>Partage d'informations relatives aux institutions et organismes à contacter en cas de fraude amoureuse</p> | <p>Informer les victimes et les internautes des ressources à leur disposition relativement aux fraudes amoureuses</p> | <p>La conservation des traces numériques peut être utile à des fins d'investigation pour identifier un individu malveillant.</p> |
| <p>7</p> <p>Dénoté sur les trois forums, mais principalement sur Signal-Arnaques</p> | <p>L'identification à son semblable</p> | <p>Briser l'isolement</p> | <p>N/A</p> |

N/A : Non applicable.

Chapitre 5 : Discussion

L'objectif principal de la présente étude est de comprendre, dans un premier temps, comment les victimes d'arnaque sentimentale s'entraident en ligne à la suite de leur expérience frauduleuse. Dans un second temps, elle s'intéresse à la pertinence des traces numériques disponibles à travers ces mécanismes d'entraide. Les résultats présentés dans le chapitre 4 mènent à certaines réflexions nécessaires afin de considérer pleinement les axes de recherche de notre étude.

5.1. Les forums de discussion : un outil permettant aux victimes de retrouver les bienfaits du monde en ligne

Même après avoir été victime d'un crime commis sur Internet, nos résultats démontrent qu'une importante partie d'internautes continuent à valoriser les échanges dans le cybermonde. En effet, la façon dont les victimes s'entraident sur les forums de discussion illustre un espace sécuritaire dans lequel les victimes peuvent s'exprimer, s'accomplir et obtenir un soutien. Les divers mécanismes d'entraide évoquent comment les victimes se réapproprient leur pouvoir dans le monde en ligne. À l'évidence, ils illustrent cette idée selon laquelle l'entraide en ligne agit à titre d'outil afin de retrouver les bienfaits d'Internet après avoir subi ses préjudices. Tantôt, les victimes font l'objet d'une arnaque irréparable commise sur Internet; tantôt, elles utilisent ce même outil afin de lutter contre ceux leur ayant causé du tort et d'épauler leurs semblables.

Notons que les mécanismes d'entraide présentés s'amalgament les uns avec les autres. Certaines publications visent davantage à partager sa propre expérience; d'autres visent à exposer les cybercriminels; puis d'autres ont comme objectif de sensibiliser et d'informer les internautes. Toutefois, en raison des échanges entre les abonnés, ces mécanismes se combinent et ont tous un même objectif commun, soit celui de prévenir que de nouvelles victimes tombent ou retombent dans un piège frauduleux. Rappelons également qu'un bon nombre d'internautes consultent les publications et les messages sans participer aux échanges, indiquant que les forums de discussion en ligne peuvent être utiles à un nombre vertigineux de victimes, quel que soit leur statut (victimes de fraude financière, non financière, indirectes (p. ex. : un proche, etc.)).

Ceci soulève des questionnements quant à la façon dont les victimes de cybercrimes commis par l'entremise d'Internet utilisent et agissent dans le cyberspace à la suite de leur expérience. Sont-elles plus craintives? Plus prudentes? Comment voient-elles le cybermonde alors qu'il représente l'outil principal menant aux torts qu'elles ont subis? Quelles relations entretiennent-elles avec les internautes dorénavant? Ces questions pourraient faire l'objet d'études criminologiques visant à enrichir les connaissances sur la façon dont les victimes se reconstruisent et se réconcilient avec le monde en ligne à la suite de leur expérience frauduleuse. Notre étude nous porte à croire que les individus ayant subi

une arnaque sentimentale continuent d'utiliser des plateformes d'échange et arrivent à en tirer du positif. Toutefois, cette idée mériterait d'être approfondie, par exemple, à l'aide d'une méthodologie privilégiant des entretiens semi-dirigés.

5.2. Le signalement en ligne : un registre qui gagne à être étendu internationalement

En ce qui concerne les traces numériques laissées par les fraudeurs dans leur mode opératoire, nos résultats démontrent que les internautes ont accès à plusieurs informations pertinentes pouvant contribuer au processus d'investigation et de renseignement visant à lutter et prévenir les arnaques sentimentales. Prendre connaissance de la façon dont les cybercriminels laissent des traces de leur crime et de la manière dont les victimes conservent et partagent celles-ci peut contribuer à guider le travail des enquêteurs et des analystes en renseignement qui désirent mettre la main sur des informations relatives aux arnaqueurs amoureux. Combinées avec les données policières, les traces numériques partagées sur les forums de discussion peuvent notamment servir à identifier des patterns criminels et à identifier les entreprises les plus affectées par les faux profils. La criminologie et la criminalistique peuvent ainsi réunir leurs savoirs afin de développer des outils techniques et des stratégies préventives pour minimiser les opportunités criminelles et prendre les précautions nécessaires auprès des individus vulnérables et à risque.

La pertinence des plateformes de signalement en ligne dorénavant démontrée, il est nécessaire d'aborder la convenance d'un site de signalement international. En effet, nos résultats ont démontré que les différents sites étudiés détiennent chacun des normes et des données qui leur sont spécifiques. Deux forums sont destinés aux internautes anglophones, puis un aux abonnés s'exprimant en français. Dès lors, créer une plateforme de signalement encadrée par une institution internationale permettrait d'avoir accès au contenu et aux données de plusieurs communautés distinctes et de les comparer. Ce registre pourrait intégrer des sections pour chacune des traces liées à l'auteur présumé de l'arnaque, comme son ou ses pseudos, son adresse courriel, son numéro de téléphone et les réseaux sociaux utilisés. En outre, une section pourrait être créée, sous forme de choix de réponses ou de questionnaire, pour aborder le mode opératoire du fraudeur. Par exemple, on pourrait y retrouver une coche permettant de sélectionner une méthode typique (p. ex. : homme

militaire, urgence médicale impliquant un coût, détention à l'étranger, etc.), puis une case visant à élaborer la situation frauduleuse de façon plus détaillée. Ainsi, les données seraient plus facilement désagrégées, ce qui faciliterait les analyses pouvant être fondées sur ces dernières. La création d'une telle plateforme de signalement contribuerait à lutter contre les cyberarnaqueurs et fournirait des données pertinentes pour tout analyste voulant étudier un enjeu relatif à la fraude amoureuse. Notons que le Centre anti-fraude du Canada et le Centre national de coordination contre la cybercriminalité (GNC3) travaillent actuellement sur la mise en œuvre d'un nouveau système de signalement des incidents de cybercriminalité et de fraude pour les entreprises et les particuliers canadiens (CAFC, 2021). Toutefois, puisque les cybercriminels ciblent plusieurs pays à la fois (généralement de la même langue), il serait pertinent de créer ce genre de système à l'international.

5.3. Considérations à prendre dans l'interprétation des forums de discussion

Bien que notre analyse ait pu faire ressortir certains modèles généraux de mécanisme d'entraide, les forums de discussion étudiés dans le cadre de la présente étude ont démontré certains écarts. Par exemple, nous avons mentionné précédemment que le forum du site Signal-Arnaques comportait beaucoup plus de témoignages écrits portant sur l'expérience victimaire que les deux forums anglophones. En outre, on ne retrouve pas toutes les mêmes traces numériques d'un forum à un autre. Dans le cadre de notre recherche, nous avons relevé des mécanismes d'entraide se retrouvant dans les trois sites étudiés. Toutefois, il existe probablement des mécanismes propres à chacun des sites. En effet, étant donné que chacun des forums a des normes, des règles et une communauté spécifiques, nous devons mener une réflexion quant à la possibilité qu'une analyse approfondie fondée sur chacun des sites de façon indépendante puisse donner lieu à des mécanismes d'entraide propres au site concerné. En d'autres mots, certains mécanismes pourraient être présents sur une plateforme et pas sur une autre. Toutefois, même si ces mécanismes ne sont pas communs à la majorité des sites abordant la fraude amoureuse, ils demeurent possiblement très influents pour les victimes qui consultent le forum issu d'un site en question. Il ne faut donc pas négliger leur impact sur les internautes. La possibilité de retrouver des

mécanismes d'entraide généraux au monde en ligne et d'autres spécifiques à des plateformes particulières gagne à être davantage approfondie.

Ensuite, notons que plusieurs facteurs peuvent influencer l'interprétation du contenu disponible sur les forums de discussion. D'une part, du côté des traces numériques, une importante partie de données sont incomplètes ou manquantes. Par exemple, l'analyse de la provenance des numéros de téléphone signalés ne peut être fondée qu'en fonction des données d'un pays concerné connu. Notre impossibilité à traiter ces informations vient donc limiter l'exhaustivité des résultats présentés. Il faut tenir compte du fait qu'un pays pourrait être beaucoup plus concerné par les fraudes amoureuses que nos résultats ne le suggèrent et que le classement présenté pourrait être amené à changer si ces données incomplètes devenaient plus riches et informatives. D'autre part, l'absence d'accès à la gestuelle et l'impossibilité de relancer les individus quant au contenu partagé limitent l'interprétation des forums de discussion. Une méthodologie plus intrusive intégrant une participation active du chercheur sur les forums de discussion et permettant d'échanger avec les internautes aurait permis d'obtenir davantage le point de vue des victimes sur la façon dont elles s'entraident en ligne.

Chapitre 6 : Dimension intégrative

Le crime se concrétise lorsqu'un ensemble de facteurs déterminants, incrustés dans un individu ou dans les structures sociales qui l'entourent, se conjuguent à des circonstances environnementales dans lesquelles une transgression pénale est saisissable, rentable et peu risquée (Clarke, 1997). Le crime est ainsi une action transgressive, déterminée par des entités sociales, psychologiques, physiques et technologiques. Pour prévenir la criminalité, il faut porter une attention particulière au déroulement des délits, aux facteurs de risque et aux facteurs de protection associés à des cibles ou à des victimes potentielles, au contrôle d'accès d'un environnement et à sa surveillance. Dès lors, pour étudier le crime dans son ensemble, il paraît évident d'avoir à considérer la matérialité des choses composant sa dimension sociale (Vinck, 2009). La co-disciplinarité entre la criminologie et les sciences forensiques apparaît ainsi comme un axiome dans lequel s'installe une certaine tautologie. D'une part, les connaissances sur la criminalité fournissent des renseignements quant à la détection et à l'interprétation de traces et d'autre

part, à l'inverse, la trace et l'identité sont des données élémentaires générant des connaissances sur la criminalité.

Dans l'étude d'un phénomène criminel comme celui de la fraude amoureuse, la nécessité de combiner ces deux champs d'expertise distincts, mais complémentaires, est d'autant plus évidente. Premièrement, nos résultats ont démontré que les traces numériques constituent des données concrètes permettant de reconstruire un comportement criminel. Elles nous informent notamment sur la façon dont les arnaqueurs s'y prennent afin d'amadouer leurs victimes et de concrétiser leurs intentions malveillantes. Les traces numériques relatives aux informations identifiantes nous permettent d'en apprendre davantage sur les modes opératoires des fraudeurs et sur leur trajectoire criminelle. Notons que même dans les situations où l'identité d'une trace est inconnue, sa simple présence constitue le signe d'une activité d'un ou de plusieurs individus pouvant être examinés plus minutieusement avec le temps (Rossy et al., 2021). Par conséquent, les savoirs criminologiques sont essentiels afin de guider le travail d'investigation du forensicien. En effet, connaître la façon dont les criminels se comportent et laissent des traces dans leur mode opératoire peut contribuer à cet acteur du système de justice, dans la mesure où ces connaissances peuvent lui indiquer où rechercher des traces pertinentes à des fins d'enquête. Ce postulat est d'autant plus vrai dans le cybermonde (Rossy et Décary-Héту, 2018).

Ensuite, la nécessité d'établir une co-disciplinarité entre la criminologie et les sciences forensiques est indubitable si l'on considère que la détection de liens et de patterns entre des acteurs et des activités est fondée sur la comparaison de traces et d'informations identifiantes (Rossy et al., 2021). La lutte et la prévention du crime s'attardent notamment à la relation existante entre des entités composant un problème précis. Établir des liens entre ces entités permet, par exemple, d'induire que tels événements sont liés à tels individus ou encore de déterminer comment certains groupes s'organisent et partagent des informations afin de mettre à exécution leurs intentions malveillantes et criminelles (Rossy et al., 2020). En outre, la détection de liens permet d'établir des facteurs de risque liés à certaines victimes ou cibles. Dans cette optique, et pour traiter d'un phénomène criminel comme la fraude amoureuse, les traces numériques et les informations identifiantes

peuvent être utiles afin de reconstruire un réseau criminel ou d'établir des liens entre différentes arnaques.

Finalement, dans l'état actuel des législations concernant le cybermonde, il est nécessaire de mettre en relation la criminologie et la sciences forensiques de façon à contribuer à la prééminence du droit sur Internet. La cybercriminalité et la cybersécurité sont aujourd'hui des enjeux majeurs, et le caractère transnational qui les désigne pose problème à de nombreux égards (Conseil de l'Europe, 2014). Notons, entre autres, qu'un bon nombre d'auteurs d'actes criminels sont exemptés de répression pénale en raison de l'ambiguïté juridique qui encadre le cybermonde. Les activités commises à l'aide de moyens numériques ne sont pas virtuelles, au sens où elles n'échappent pas à la réalité (Conseil de l'Europe, 2014). Dans leurs conséquences, les cybercrimes peuvent s'avérer tout aussi dommageables que les crimes contre la personne commis physiquement. Toutefois, le droit pénal exprime un retard apparent vis-à-vis l'évolution des délits commis dans le cyberespace. Dans le cas d'une rencontre en ligne, même pour l'internaute aguerris, des questions fondamentales surgissent quant aux intentions et à l'identité de l'émetteur ainsi qu'à l'authenticité du contenu qu'il partage. Sur Internet, tous peuvent émettre, recevoir, copier et manipuler (Cohen-Tanugi, 2001). À qui avons-nous à faire ? Les intentions de mon interlocuteur sont-elles intègres ? Les informations auxquelles nous avons accès sont-elles complètes ? D'où mon interlocuteur communique-t-il ? Qui est responsable des crimes commis sur Internet ? Comment sanctionner ? Comment dédommager les victimes ? Ces questions, qui constituent des exemples parmi tant d'autres, rejoignent toutes de près ou de loin la criminologie et les sciences forensiques. L'opacité numérique est un enjeu des plus actuels et la co-disciplinarité entre ces deux champs d'expertise mérite d'être mise de l'avant afin qu'un encadrement plus clair des actes criminels commis dans le monde numérique puisse être établi.

Conclusion

L'avènement des technologies de communication et de l'intérêt grandissant des individus en ce qui concerne les rencontres amoureuses en ligne aura considérablement fait augmenter le nombre d'escroqueries sentimentales au cours des dernières années. L'arnaque amoureuse constitue l'une des fraudes en ligne causant le plus de dommages pécuniaires pour les victimes au Canada. Malgré tout, ce phénomène demeure méconnu et sous-déclaré, et peu d'études intègrent l'une des entités principales qui la composent, à savoir le cyberespace. En effet, certaines études (voir entre autres Buchanan et Whitty, 2014 ; Modic et Anderson, 2015 ; Whitty, 2017) abordent les caractéristiques des victimes et la façon dont elles vivent leur expérience frauduleuse. D'autres (voir entre autres Rege, 2009 ; Whitty, 2013 ; Edwards et al., 2018) traitent plutôt du script criminel des fraudeurs, de leurs particularités et de leur mode opératoire. Toutefois, aucune ne semble avoir été menée afin d'étudier la façon dont les victimes utilisent le cyberespace pour s'entraider et se reconstruire à la suite de leur expérience. En outre, les traces numériques ne sont que très rarement abordées (voir entre autres, Edwards et al., 2018). Ainsi, la présente étude avait comme objectif d'analyser, d'une part, les façons dont les victimes d'arnaque amoureuse s'entraident en ligne à la suite de leur expérience frauduleuse et, d'autre part, de détecter les traces numériques laissées par les fraudeurs à travers ces mécanismes d'entraide. À partir des études jusqu'ici menées sur l'entraide en ligne (voir entre autres Puustinen et al., 2015 ; Berthelot-Guiet et Charbonneaux, 2020 ; Lee, 2020), notre cadre conceptuel s'appuie sur l'idée selon laquelle certains individus vivant des expériences semblables partagent des informations afin de s'entraider sur certains sites conçus à cet effet. De ce fait, nous avons réalisé une recherche exploratoire fondée sur trois forums de discussion destinés aux victimes de fraude amoureuse, soit ceux de Signal-Arnaques, ScamWarners et ScamSurvivors.

Le premier mécanisme d'entraide soulevé lors de notre analyse concerne la façon dont les forums de discussion en ligne constituent une forme de soutien et de voix pour les victimes. D'une part, ces dernières publient des messages faisant l'objet de témoignages écrits afin de trouver conseil auprès des internautes ou encore pour raconter leur récit de façon à s'enlever un poids des épaules. D'autre part, plusieurs victimes utilisent les forums

de discussion afin de briser l'isolement auquel elles sont confrontées. L'anonymat à travers duquel les participants peuvent publier et échanger sur ces plateformes est d'ailleurs bénéfique pour ceux et celles désirant avoir recours à une certaine forme d'aide sans avoir à s'identifier formellement. L'accompagnement et la participation active sur les forums constituent également un mécanisme d'entraide relevé permettant aux victimes de se reconstruire à la suite de leur expérience et de prévenir qu'une autre personne soit victime d'une telle arnaque.

Ensuite, le signalement et le partage de profils frauduleux représentent des mécanismes d'entraide les plus utilisés sur les forums de discussion destinés à lutter contre la fraude amoureuse. Il permet notamment de prévenir des cas de fraude et d'exposer les cybercriminels. Ce mécanisme déborde de traces numériques pouvant s'avérer pertinentes (photographies, adresses courriel, numéros de téléphone, etc.) pour établir des liens entre des cas de fraude et limiter l'opportunité criminelle des arnaqueurs. Nous avons d'ailleurs pu, à travers ce mécanisme, extraire des informations comme la provenance des numéros de téléphone, les réseaux sociaux et les fournisseurs de service courriel les plus utilisés par les fraudeurs. Ces traces sont particulièrement utiles à des fins de renseignement visant à définir les facteurs de risque et les facteurs de protection associés aux arnaques sentimentales.

En outre, les forums de discussion en ligne servent d'outil de sensibilisation et d'information auprès des internautes. Notre analyse a notamment démontré qu'un nombre important de publications comportaient des astuces visant à démasquer une escroquerie ou à interrompre le processus frauduleux ainsi qu'à fournir des informations relatives aux institutions et organismes à contacter dans le cas où une fraude venait à se concrétiser. Ces mécanismes visent plusieurs objectifs, tels qu'exposer les cybercriminels, prévenir une victimisation répétée ou de nouvelles fraudes ainsi qu'à tenir au courant les internautes des ressources à leur disposition. Les traces numériques ont également un rôle à jouer dans ces mécanismes puisqu'elles permettent notamment de reconnaître les patterns dans les informations considérées douteuses afin d'identifier une intention malveillante (astuces visant à démasquer une escroquerie). La conservation de traces est également utile à des fins d'investigation pour identifier un cybercriminel (mécanisme visant les institutions à contacter).

Cette étude met en exergue la façon dont les victimes d'arnaque sentimentale se reconstruisent et se réconcilient avec le cybermonde grâce à l'aide qu'elles trouvent et fournissent sur les forums de discussion en ligne. Par ailleurs, la mise en place d'une plateforme de signalement internationale permettrait entre autres de mieux lutter contre ces arnaques et d'aborder leur caractère transfrontalier en regroupant les informations jusqu'ici réparties en de nombreux forums de discussion issus de pays et de langues différentes.

Finalement, cette étude ouvre la porte à une panoplie d'angles de recherche pouvant aborder l'entraide en ligne des victimes d'acte criminel et les traces numériques fournies par ces dernières pouvant contribuer à produire du renseignement. Rappelons qu'une importante part de victimes ne dénoncent pas les intentions malveillantes d'un fraudeur auquel elles auraient pu être confrontées (surtout si elles ne tombent pas dans le piège), mais partagent ses informations identifiantes sur les forums de discussion et les plateformes de signalement. Ainsi, ces banques de données comportent une masse de traces pertinentes, dont certaines ne seront jamais portées à l'attention des autorités. La nécessité d'établir une co-disciplinarité entre la criminologie et la criminalistique s'avère de plus en plus évidente, particulièrement pour les crimes facilités par les moyens technologiques et les réseaux sociaux. La fraude amoureuse est un phénomène qui mérite une attention particulière de par son ampleur et les nombreuses dynamiques sociologiques et technologiques qui la composent. Il pourrait s'avérer pertinent, par exemple, de reconstruire les plus récents modes opératoires des fraudeurs en fonction des publications les plus à jour publiées sur les forums de discussion. Ceci permettrait de déterminer si ces modes opératoires ont évolué avec le développement des plus récents moyens de communication en les comparant avec les résultats d'études antérieures (voir entre autres, Whitty, 2013). En somme, puisque la présente étude n'a fait l'objet que de trois forums de discussion publics, il existe une perspective de recherche dans sa réplique à d'autres types d'outils d'échanges (p. ex. : groupes privés) de façon à déterminer si les mécanismes d'entraide ici dénotés s'appliquent ailleurs.

Références bibliographiques

- 10 Online Dating Statistics (for Canada) You Should Know. (s. d.-a). Eharmony. Consulté 7 août 2021, à l'adresse <https://www.eharmony.ca/online-dating-statistics/>
- Anderson, M., Vogels, E.A. et Turner, E. (2020). *The Virtues and Downsides of Online Dating*. Pew Research Center. <https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/>
- Anesa, P. (2020). Lovextortion : Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, 35, 100398. <https://doi.org/10.1016/j.dcm.2020.100398>
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759-763. <https://doi.org/10.1089/cyber.2010.0307>
- Archer, A. K. (2017). « I Made a Choice » : Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles [Mémoire de maîtrise, Regis University]. EPublications. <https://epublications.regis.edu/cgi/viewcontent.cgi?article=1830&context=theses>
- Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks : Research challenges and directions. *Digital Investigation*, 28, 126-138. <https://doi.org/10.1016/j.diin.2019.02.001>
- Ashurst, L., & McAlinden, A.-M. (2015). Young people, peer-to-peer grooming and sexual offending : Understanding and responding to harmful sexual behaviour within a social media society. *Probation Journal*, 62(4), 374-388. <https://doi.org/10.1177/0264550515619572>
- Bastiaensens, S., Van Cleemput, K., Vandebosch, H., Poels, K., DeSmet, A., & De Bourdeaudhuij, I. (2019). "Were You Cyberbullied? Let Me Help You." Studying Adolescents' Online Peer Support of Cyberbullying Victims Using Thematic Analysis of Online Support Group Fora. Dans H. Vandebosch & L. Green (Éds.), *Narratives in Research and Interventions on Cyberbullying among Young People* (p. 95-112). Springer International Publishing. https://doi.org/10.1007/978-3-030-04960-7_7
- Berthelot-Guiet, K., & Charbonneaux, J. (2020). Vers une entraide numérique intergénérationnelle ? Le cas du Glioblastome sur les forums de discussion en ligne. *Revue*

française des sciences de l'information et de la communication, 19, Article 19.
<https://doi.org/10.4000/rfsic.8642>

Boyd, D.M., et N.B. Ellison. (2007). Social network sites : Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (1): 210 à 230.
<https://doi.org/10.1111/j.1083-6101.2007.00393.x>

Brooks, M. (2011). How Has Internet Dating Changed Society? *Internet Dating Executive Alliance*.
<https://www.onlinepersonalswatch.com/files/idea-white-paper-final-review-copy-only-updated-1-19-2.pdf>

Buchanan, T., & Whitty, M. (2014). The online dating romance scam : Causes and consequences of victimhood. *Psychology*, 20.
<https://doi.org/10.1080/1068316X.2013.772180>

Buquet, A. (2011). *Manuel de criminalistique moderne et de police scientifique* (5ème édition). Criminalité internationale.

Cali, B. E., Coleman, J. M., & Campbell, C. (2013). Stranger Danger? Women's Self-Protection Intent and the Continuing Stigma of Online Dating. *Cyberpsychology, Behavior, and Social Networking*, 16(12), 853-857. <https://doi.org/10.1089/cyber.2012.0512>

Cameron, D. et Kulick, D. (2006). *The Language and Sexuality Reader*. Routledge & CRC Press.
<https://www.routledge.com/The-Language-and-Sexuality-Reader/Cameron-KULICK/p/book/9780415363075>

Cialdini, R.B. (2007) : *Influence : The Psychology of Persuasion (Revision Edition)*. Harper Business, Dunmore.

Clarke, R. V. (Éd.). (1997). *Situational crime prevention : Successful case studies* (2. ed). Criminal Justice Press.

Coat, M. (2020). *Victimes de cyberfraude : Impacts et enjeux auprès des institutions financières et des services de police locale*. [Mémoire, Université de Montréal].

Cohen-Tanugi, L. (2001). Le clair-obscur d'Internet. *Pouvoirs*, n° 97(2), 85-90.

Commissaire aux droits de l'homme. (2014). *La prééminence du droit sur l'internet et dans le monde numérique en général*. Conseil de l'Europe. <https://rm.coe.int/la-preeminence-du-droit-sur-l-internet-et-dans-le-monde-numerique-en-g/16808b3e6f>

Commission des Services financiers et des Services aux consommateurs. (2018, février 18). *Bulletin du CAFC: Palmarès des 10 fraudes les plus courantes* | (FCNB). <https://fcnb.ca/fr/nouvelles-et-activites/bulletin-du-cafc-palmares-des-10-fraudes-les-plus-courantes>

Couch, D., Liamputtong, P., & Pitts, M. (2012). What are the real and perceived risks and dangers of online dating? Perspectives from online daters: Health risks in the media. *Health, Risk & Society*, 14, 697-714. <https://doi.org/10.1080/13698575.2012.720964>

Cross, C. (2020). Romance fraud. Dans T. J. Holt & A. Bossler (Éds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (p. 1-22). Palgrave Macmillan. https://link.springer.com/referenceworkentry/10.1007/978-3-319-90307-1_41-1

Decree President Council Ministers. (2013). *Directive Laying Down Guidelines for Cyber Protection and the National Cyber Security*.

Del-Teso-Craviotto, M. (2006). Language and sexuality in Spanish and English dating chats1. *Journal of Sociolinguistics*, 10(4), 460-480. <https://doi.org/10.1111/j.1467-9841.2006.00288.x>

Ducret, Baillif, B. (2018). *Arnacoeurs, les escrocs de l'amour en ligne*. <https://pages.rts.ch/emissions/temps-present/international/9850144-arnacoeurs-les-escrocs-de-l-amour-en-ligne.html>

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, 67(1), 97-116. <https://doi.org/10.1007/s10611-016-9649-z>

Edwards, M., Suarez de Tangil Rotaèche, G. N., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2018). The Geography of Online Dating Fraud. In *Workshop on Technology and Consumer Protection (ConPro)* <https://doi.org/https://www.ieee-security.org/TC/SPW2018/ConPro/>

Enoch, J.S. (2008, juillet 28). *Love's Labor Looted: Internet Dating Scams Can Get Expensive*. Consumer Affairs. <https://www.consumeraffairs.com/news04/2008/07/eharmony.html>

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. Dans T. Tryfonas & I. Askoxylakis (Éds.), *Human Aspects of Information Security, Privacy, and Trust* (p. 36-47). Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4

Fiore, A., Taylor, L., Mendelsohn, G., & Hearst, M. (2008). *Assessing Attractiveness in Online Dating Profiles*. 797-806. <https://doi.org/10.1145/1357054.1357181>

Galinéon-Méléneq, B. et Zlitni, S. (2013). *Traces numériques : de la production à l'interprétation*. CNRS Éditions.

Ghimiray, D. (2021, juin 4). *Qu'est-ce qu'un serveur proxy et comment fonctionne-t-il ?* AVG. <https://www.avg.com/fr/signal/proxy-server-definition>

Gouvernement du Canada, G. royale du C. (2019, février 12). *Les victimes de l'arnaque amoureuse se font détrousser de plus de 22,5 M\$ en 2018 | Gendarmerie royale du Canada*. <https://www.rcmp-grc.gc.ca/fr/nouvelles/2019/victimes-larnaque-amoureuse-font-detrousser-225-2018>

Gouvernement du Canada, G. royale du C. (2020, janvier 31). *Signaler les cas de fraude et de cybercriminalité*. <https://www.antifraudcentre-centreantifraude.ca/report-signalez-fra.htm>

Gouvernement du Canada, G. royale du C. (2021, mars 1). *Mois de la prévention de la fraude*. <https://www.antifraudcentre-centreantifraude.ca/features-vedette/2021/03/fraud-prevention-fraude-fra.htm?fe>

Government of Canada, S. C. (2021, mars 24). *Canadians' assessments of social media in their lives*. <https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm>

Greiner, C. (2018). *Evaluation des contenus de forums d'entraide en ligne d'utilisateurs de cannabis* [University of Geneva]. <https://doi.org/10.13097/archive-ouverte/unige:107228>

Karyda, M., & Mitrou, L. (2007). Internet Forensics : Legal and Technical Issues. *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*, 3-12. <https://doi.org/10.1109/WDFIA.2007.4299368>

Laplace, I. (2013). *La recherche qualitative en santé à partir de forums internet* [Mémoire stage praticien, Université de Lyon]. http://anciensite.clge.fr/IMG/pdf/memoire_Isabelle_LAPLACE.pdf

Leclerc, B. (2018). Boosting crime scene investigations capabilities through crime script analysis. Dans Rossy, Q., Décary-Héту, D., Delémont, O., and Mulone, M. (eds) *The Routledge International Handbook of Forensic Intelligence and Criminology*. Routledge, pp. 102–111.

Lee, J. (s. d.). *Understanding Norwegian youth online help seeking through bigdata analysis* [Mémoire de maîtrise, Université d'Oslo]. https://www.duo.uio.no/bitstream/handle/10852/85069/jisu_lee_master_thesis.pdf?sequence=1&isAllowed=y

Legros Boisseau. (2020). *Signal Arnaques*. [Entrevue réalisée dans le cadre du mémoire]. Université de Montréal.

Lemieux, V. (2013). *Criminal Networks*. (n° JS62-107/2003). Gendarmerie Royale du Canada. <https://publications.gc.ca/collections/Collection/JS62-107-2003E.pdf>

Machimbarrena, J. M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018). Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use. *International Journal of Environmental Research and Public Health*, 15(11), 2471. <https://doi.org/10.3390/ijerph15112471>

Margot, P. (2014). Traçologie: la trace, vecteur fondamental de la police scientifique. *Revue internationale de criminologie et de police scientifique*, 1(4).

Metz, S., & Péliissier, C. (2010). Un modèle de caractérisation de l'aide : Le cas dans l'enseignement à distance. *Réformes et changements pédagogiques dans l'enseignement supérieur*.

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General Cyberspace : Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal*, 5(3), 1843-1856. <https://doi.org/10.1109/JIOT.2018.2815535>

Pastinelli, M. (2011). *L'observation participante dans les démarches d'ethnographie en ligne*. [communication orale]. Université Laval. <https://fr.slideshare.net/grmsmediasante/lobservation-participante-dans-les-dmarches-dethnographie-en-ligne>

Paveau, M.-A. (2019). Introduction. Écrire, parler, communiquer en ligne : Nos vies sociolangagières connectées. *Langage et société*, N° 167(2), 9-28.

Phan, A., Seigfried-Spellar, K.C., & Choo, K. (2021). Threaten me softly: A review of potential dating app risks. *Computer in Human Behavior Reports*, 3. <https://doi.org/10.1016/j.chbr.2021.100055>

Pooley, K., & Boxall, H. (s. d.). *Mobile dating applications and sexual and violent offending*. 16.

Powell A., Haynes C. (2020) *Social Media Data in Digital Forensics Investigations*. Dans Zhang X., Choo KK. (eds) *Digital Forensic Education. Studies in Big Data*. vol 61. Springer, Cham. https://doi.org/10.1007/978-3-030-23547-5_14

Powell, A., Scott, A. J., & Henry, N. (2020). Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology*, 17(2), 199–223. <https://doi.org/10.1177/1477370818788006>

Puustinen, M., Bernicot, J., Volckaert-Legrier, O., & Baker, M. (2015). Naturally occurring help-seeking exchanges on a homework help forum. *Computers & Education*, 81, 89-101. <https://doi.org/10.1016/j.compedu.2014.09.010>

Qeis, M. (2016). *The Game of Deception : How Visual Seduction Operates within The Field of Online Dating Sites*. The International Conference on Media.

Rege, A. (2009). What’s Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology (IJCC)*, 3, 974-2891.

Ribaux, O., & Souvignet, T. (2020). “Hello are you available?” Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, 33, 300978. <https://doi.org/10.1016/j.fsidi.2020.300978>

Rossy, Q. (2016). La visualisation relationnelle au service de l’enquête criminelle. Dans Boivin, R. et Morselli, C. (dir) *Les réseaux criminels*. Les Presses de l’Université de Montréal.

Rossy, Q., & Ribaux, O. (2020). Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms. *European Journal on Criminal Policy and Research*, 26, 1-22. <https://doi.org/10.1007/s10610-020-09438-3>

Scannell, M. J. (2019). Online Dating and the Risk of Sexual Assault to College Students. *Building Healthy Academic Communities Journal*, 3(1), 34-43. <https://doi.org/10.18061/bhac.v3i1.6688>

Shaari, A. H., Kamaluddin, M. R., Paizi@Fauzi, W. F., & Mohd, M. (2019). Online-Dating Romance Scam in Malaysia : An Analysis of Online Conversations between Scammers and Victims. *GEMA Online® Journal of Language Studies*, 19(1), Article 1. <https://doi.org/10.17576/gema-2019-1901-06>

Smith-Merry, J., Goggin, G., Campbell, A., McKenzie, K., Ridout, B., & Baylous, C. (2019). Social Connection and Online Engagement : Insights From Interviews With Users of a Mental Health Online Forum. *JMIR Mental Health*, 6(3), e11084. <https://doi.org/10.2196/11084>

Snaychuk, L. A., & O'Neill, M. L. (2020). Technology-Facilitated Sexual Violence : Prevalence, Risk, and Resiliency in Undergraduate Students. *Journal of Aggression, Maltreatment & Trauma*, 29(8), 984-999. <https://doi.org/10.1080/10926771.2019.1710636>

Sogliuzzo, G. (2013, 8 mars). *Identité/Présence numérique : quelles traces laissons-nous sur le web?*. <http://beaumont-redon.fr/wp/cultureinfomedias/wp-content/blogs.dir/31/files/2013/11/Atelier-infodoc-seconde-identite-num%C3%A9rique.pdf>

Sugiura, L., Wiles, R., & Pope, C. (2017). Ethical challenges in online research : Public/private perceptions. *Research Ethics*, 13(3-4), 184-199. <https://doi.org/10.1177/1747016116650720>

Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. *Network Security*, 2014(11), 9-16. [https://doi.org/10.1016/S1353-4858\(14\)70112-6](https://doi.org/10.1016/S1353-4858(14)70112-6)

Vinck, D. (2009). De l'objet intermédiaire à l'objet-frontière. *Revue d'anthropologie des connaissances*, Vol. 3, n° 1(1), 51-72.

Whitty, M. (2013). The Scammers Persuasive Techniques Model : Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, 53, 665-684. <https://doi.org/10.1093/bjc/azt009>

Whitty, M. T. (2017). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105-109. <https://doi.org/10.1089/cyber.2016.0729>

Yen, T.-F., & Jakobsson, M. (2016). Case Study : Romance Scams. Dans M. Jakobsson (Éd.), *Understanding Social Engineering Based Scams* (p. 103-113). Springer. https://doi.org/10.1007/978-1-4939-6457-4_10

Yoo, J. (2005). *Fighting the New Terrorism*. http://www.aei.org/publications/pubID.22735.filter.all/pub_detail.asp.

Zhong, L. R., Keibell, M. R., & Webster, J. L. (2020). An exploratory study of Technology-Facilitated Sexual Violence in online romantic interactions : Can the Internet's toxic disinhibition exacerbate sexual aggression? *Computers in Human Behavior*, 108, 106314. <https://doi.org/10.1016/j.chb.2020.106314>

Annexes

Annexe 1. Format des trois forums sélectionnés sous forme de captures d'écran

| ScamWarners | | | |
|--|-------------------------------|---|--|
| TOPICS | STATISTICS | LAST POST | |
| Blackmail Scams - Sextortion Scams by Bryon Williams Sat Jan 20, 2018 12:14 pm | 1418 Replies 1188624 Views | by Terminator5 Sat Jul 05, 2021 5:25 am | |
| Scammers Impersonating Military Personnel by Dotti Thu Feb 12, 2015 8:22 am | 2 Replies 107934 Views | by AlanJones Sat Apr 07, 2015 2:21 am | |
| Teen Sextortion - Teen Blackmail Extortion by Bryon Williams Thu Aug 10, 2017 4:00 pm | 0 Replies 21897 Views | by Bryon Williams Thu Aug 10, 2017 4:00 pm | |
| Information for Romance Scam Victims by Dotti Sun May 02, 2011 7:50 am | 1 Replies 100502 Views | by Dotti Fri Mar 07, 2014 2:30 pm | |
| Romance Scam victim interview requests by Dotti Fri Jun 01, 2012 10:30 am | 0 Replies 47081 Views | by Dotti Fri Jun 01, 2012 10:30 am | |
| Are you in contact with a love scammer? by Dotti Fri Sep 04, 2009 7:55 am | 3 Replies 221006 Views | by Dotti Fri Sep 04, 2009 7:55 am | |
| An introduction to love or dating scams by Julia Sat Jul 14, 2007 2:20 pm | 0 Replies 95879 Views | by Julia Sat Jul 14, 2007 2:20 pm | |
| Mark, markmiller60001@gmail.com by meluu53 Tue Aug 17, 2021 9:07 am | 0 Replies 11 Views | by meluu53 Tue Aug 17, 2021 9:07 am | |
| johnstongreg285@gmail.com by meluu53 Tue Aug 17, 2021 9:05 am | 0 Replies 10 Views | by meluu53 Tue Aug 17, 2021 9:05 am | |

| ScamSurvivors | | | | |
|---------------|--|---------|---------|---|
| ANNOUNCEMENTS | | REPLIES | VIEWS | LAST POST |
| | Thread of Shame by firefly Mon Sep 10, 2018 8:37 pm | 14 | 336419 | by firefly Wed Apr 21, 2021 4:56 pm |
| | What to do if you are a victim of a scam by firefly Tue Sep 23, 2014 3:31 pm | 2 | 332390 | by SlapHappy Tue Dec 09, 2014 10:44 pm |
| | How the scams work by firefly Tue Jul 22, 2014 6:42 am | 13 | 538510 | by firefly Sat Jan 13, 2018 8:16 pm |
| | recovery and reassurance by jamesbrown14 Tue Nov 06, 2012 2:04 pm | 555 | 4531081 | by firefly Fri Aug 06, 2021 6:47 pm |
| | Forum rules and frequently asked questions. by Wayne Mon Apr 30, 2012 2:13 am | 6 | 361602 | by SlapHappy Sat Nov 17, 2018 12:19 pm |

| TOPICS | | REPLIES | VIEWS | LAST POST |
|--------|---|---------|--------|--|
| | Romance scammer submissions. by Wayne Sun Aug 25, 2019 2:18 pm | 0 | 21936 | by Wayne Sun Aug 25, 2019 2:18 pm |
| | Most common people scammers steal photos of. by Wayne Sat Jun 09, 2012 1:00 am | 17 | 108430 | by Big Al Mon Feb 19, 2018 4:36 pm |
| | How to spot if your valentine is a scammer. by Wayne Fri Feb 14, 2014 2:15 am | 1 | 46797 | by SlapHappy Wed Oct 14, 2015 5:28 pm |
| | The post-scam stage - waking up to reality by firefly Sat Aug 01, 2015 12:09 am | 1 | 115254 | by firefly Sat Sep 05, 2015 2:00 am |
| | VERY IMPORTANT information on the photos romance scammer use by Wayne Mon Apr 30, 2012 5:30 pm | 0 | 53450 | by Wayne Mon Apr 30, 2012 5:30 pm |
| | Scammers abusing stolen photos of Elvira K. by Big Al Wed Aug 11, 2021 10:57 pm | 1 | 45 | by Big Al Tue Aug 17, 2021 2:37 pm |
| | bukettulpan@gmail.com by Big Al Tue Aug 17, 2021 2:22 pm | 3 | 5 | by Big Al Tue Aug 17, 2021 2:31 pm |

Signal-Arnaques

| Arnaques sentimentales | | | |
|---|----------|---|--|
| Nouveau sujet <input type="text" value="Dans ce forum..."/> | | Marquer tous les sujets comme lus • 37 sujets 1 2 > | |
| SUJETS | RÉPONSES | VUES | DERNIER MESSAGE |
| Arnaques sentimentales par Laura2020 » mer. 31 mars 2021 00:05 | 3 | 2555 | par Mad94 sam. 29 mai 2021 12:25 |
| Victime d'arnaque par Laura2020 » mar. 30 mars 2021 02:18 | 1 | 2328 | par rorococ045 mar. 30 mars 2021 19:45 |
| Proche sous l'emprise d'une arnaque - Que faire? par grosapatouf » mer. 14 oct. 2020 22:41 | 7 | 3715 | par rorococ045 mar. 30 mars 2021 19:42 |
| Arnaque Sentimentale - Plainte et suite par Luc250 » dim. 14 févr. 2021 19:25 | 2 | 1323 | par Luc250 lun. 15 févr. 2021 19:16 |
| Arnaque sentimentale par Caprisun » ven. 6 nov. 2020 17:50 | 1 2 3 | 27 | par dans-mon-droit ven. 29 janv. 2021 15:57 |
| Arnaque aux sentiments + héritage par Guidon » lun. 8 juin 2020 04:27 | 7 | 3240 | par billetdecent lun. 2 nov. 2020 15:42 |
| arnaques aux sentiments et soi-disant héritage par galeo » dim. 18 oct. 2020 07:31 | 3 | 510 | par Mad94 dim. 18 oct. 2020 12:35 |
| Faux profils sur Instagram par Deathstroke » jeu. 15 oct. 2020 19:28 | 0 | 553 | par Deathstroke jeu. 15 oct. 2020 19:28 |
| comment savoir si j'ai été victime d'une arnaque sentimentale par Aloha17* » mer. 12 août 2020 17:48 | 9 | 1183 | par jcv43 mer. 26 août 2020 08:04 |
| ARNAQUE WEBCAM par Dylan Lopez » mer. 5 août 2020 05:38 | 8 | 2408 | par Atina dim. 23 août 2020 18:45 |
| Arnaque Applications Rencontres par zakikei » dim. 10 mai 2020 19:55 | 6 | 1488 | par zakikei dim. 17 mai 2020 02:31 |

Annexe 2. Grille de codage développée à partir des forums de discussion (analyse de contenu)

| Codes | Catégories |
|---|---|
| Blessure (émotionnelle) antérieure | Éléments de vulnérabilité |
| Famille dysfonctionnelle | |
| Traumatisme antérieur (viol) | |
| Recherche d'une relation passionnelle | |
| Fragilité | |
| Naïveté | |
| Sentiment de honte | Reconnaître être victime (post-arnaque) |
| Tristesse | |
| Isolement social | |
| Perte pécuniaire | |
| Rêve brisé | |
| Intérêt prononcé de l'interlocuteur envers la victime | Idéalisation de la relation (tomber amoureux) |
| Se sentir amoureux | |
| Interlocuteur « à l'écoute » de la victime | |
| Qualités attirantes de l'interlocuteur | |
| Aveuglé par l'amour | |
| Projection d'un avenir commun | |
| Adresse courriel | Traces numériques partagées par les victimes |
| Pseudonyme | |
| Numéro de téléphone | |
| Fournisseur de service de téléphonie | |
| Fournisseur de service mail | |

| | |
|---|------------------------------------|
| Date(s) | |
| Photographie(s) | |
| Réseau social utilisé | Mode opératoire et script criminel |
| Méthode de prise de contact | |
| Envoi de <i>sextos</i> /photos | |
| Évènement urgent et exceptionnel | |
| Méthode de transfert d'argent | |
| Changement de comportement de l'interlocuteur | Transition vers l'anarque |
| Ambiguïté dans le discours du fraudeur | |
| Soutirer de l'empathie/sympathie | |
| Menace(s) | |
| Insistance/Persistance du fraudeur | |
| Tentative du fraudeur pour reprendre contact avec la victime | |
| Raconter son récit | Partager son expérience |
| Leçon tirée | |
| Se libérer | |
| Se réapproprier son pouvoir | |
| Survivant (devenir mentor) | |
| Désir d'aider son prochain | |
| Appel à l'aide | Recherche soutien/conseils |
| Nécessité d'être aidé | |
| Questionnement | |
| Doute vis-à-vis l'interlocuteur | |
| Inquiétude vis-à-vis un proche | |
| Réparation de l'arnaque | Quoi faire et qui contacter |
| Réticence à contacter les autorités | |
| Organismes à contacter | |
| Institutions à contacter : <ul style="list-style-type: none"> • Police ; • Banque ; • Etc. | |
| Groupe de soutien | |
| Sensibilisation | Prévention |
| Attention aux fausses victimes (fraudeurs) | |
| Nécessité d'exposer les fraudeurs | |
| Quoi faire pour freiner l'arnaque | Accompagner les victimes |
| Quoi faire la prochaine fois | |
| Relancer la victime | |
| Empathie | |
| Rassurer la victime | |
| Être là pour la victime | |
| Réponses rapides | |
| Encouragement | |

| | |
|--|---------------------------------|
| Soutien moral | |
| Remerciement | Reconnaissance d'être aidé |
| Relancer le forum | |
| Confronter le fraudeur | Démasquer la fraude |
| Se référer à d'autres victimes | |
| Montrer les preuves à la victime | |
| Couper tous contacts | Arrêter le processus frauduleux |
| Prévenir les autorités | |
| Ne pas céder aux menaces | |
| Ne pas douter des intentions malveillantes | |
| Ne pas chasser le fraudeur | |

Annexe 3. Provenance des numéros de téléphones signalés, Signal-Arnaques

| Pays | Nombre de numéros de téléphones signalés |
|---------------|--|
| France | 1303 |
| Côte d'Ivoire | 32 |
| Bénin | 28 |
| États-Unis | 23 |
| Royaume-Uni | 15 |
| Canada | 14 |
| Belgique | 12 |
| Russie | 4 |
| Suisse | 3 |
| Ukraine | 3 |
| Thaïlande | 2 |
| Autres | 10 |