REVUE AFRICAINE DE CRIMINOLOGIE

ROLE CAUSAL DES VICTIMES DANS L'ESCROQUERIE SUR INTERNET EN COTE D'IVOIRE

CAUSAL ROLE OF VICTIMS IN INTERNET FRAUD IN IVORY COAST

VEH GOUE ARNAUD LANDRY
Cel. (+225) 0748143718/0102901515
Email : gouelandry@gmail.com

RESUME

L'étude propose une analyse du processus de la victimisation à l'escroquerie via Internet en Côte d'Ivoire. Elle apporte un éclairage sur le processus, les logiques et les conséquences de la victimisation. Les théories du mode de vie et de l'exposition, des perspectives, des besoins et de l'appropriation sociale des technologies ont facilité la compréhension des attitudes et agissements victimaires observés dans le cyberespace. Deux cent quatre-vingts (280) individus concernés par ces actes vulnérables ont composé l'échantillon et pris part à l'enquête. Les analyses descriptives et quantitatives menées, dressent le processus de victimisation, le portrait et le rôle causal des victimes d'une part et déterminent les logiques en interaction liées à la victimisation d'autre part. De nombreuses conséquences en découlent. La prévention de la victimisation à l'ère du numérique s'impose.

Mots-clés : victimisation, victimes, cyberescroquerie, cyberescrocs.

ABSTRACT

This study offers an analysis of the victimization process in internet fraud in Côte d'Ivoire. It provides insight into the process, the logic, and the consequences of victimization. Lifestyle and exposure theories, as well as perspectives on needs and the social appropriation of technologies, has made easier the understanding of victim attitudes and behaviors noticed in cyberspace. Two hundred and eighty (280) people who are concerned with these vulnerable acts have been used as sample and have helped in conducting the survey. On the one hand, the descriptive and quantitative analyses conducted outline the victimization process, the profile, and the causal role of victims. On the other hand, they determine the interacting logics related to victimization. Lots of consequences arise from this. Prevention of victimization in the digital age is an imperative need.

Keywords : victimization, victims, cyber fraud, cybercriminals.

I-Introduction

L'escroquerie sur internet représente l'une des formes spécifiques de la cybercriminalité les plus répandus à l'échelle mondiale. La Côte d'Ivoire n'est pas en reste. Elle voit se développer dans son cyberespace cette forme d'atteintes aux biens. Elle est devenue, au fil des années, un vecteur de réussite sociale (BOGUI, 2010). L'analyse des rapports d'activité des trois dernières années de l'Agence Nationale des Systèmes de Sécurité et de l'Informatique (ANSSI) montre une hausse continue des plaintes. En effet, celles-ci sont passées de 607 en 2022 à 802 en 2023, puis à 2328 en 2024, soit une augmentation de 283% entre 2022 et 2024 (ANSSI-CI, 2024). Selon l'ANSSI (2024), l'augmentation des plaintes se justifierait par le basculement de la criminalité traditionnelle dans l'espace numérique par un usage accru de l'Internet comme outil de commission, par l'accroissement du nombre d'utilisateurs des technologies numériques, ainsi que la diversification des services en lignes et de la qualité de l'assistance apportée aux victimes. Et le préjudice financier est estimé à plus de 5 milliards de FCFA entre 2022 et 2024 (ANSSI-CI, 2024). Ces chiffres signifient clairement que la cyberescroquerie est toujours d'actualité et que toutes les actions doivent être prises afin de freiner cette délinquance numérique. La chaine Radio Canada a diffusé récemment un reportage intitulé « Brouteur, un fraudeur qui piège ses victimes sur Internet » dans lequel, semble-t-il, les Québécois, sont les « cibles faciles » de choix des brouteurs ivoiriens, un réseau criminel qui a fait de l'arnaque amoureuse sa spécialité avec des méthodes sophistiquées. Cela sous-entend que des personnes physiques et/ou morales sont exposées et/ou victimes (ANSSI, 2024). La cyberescroquerie s'apparente davantage à une construction sociale complexe permettant d'entretenir un climat de méfiance permanente, plutôt qu'à un phénomène clairement repéré et analysé (GUARNIERI & PRZYSWA, 2012). Toutefois, les recherches disponibles confirment que les délits subis dans le cyberespace ne sont que rarement dénoncés, que les sondages de victimisation et les statistiques officielles de la criminalité ne les prennent vraiment en considération qu'à partir des années 2010, et que la classification de ces différents types de délits varie d'un pays à l'autre (CANEPPELE & AEBI, 2019). Le phénomène cybercriminel ne se résume plus donc à des actes isolés, anecdotiques, ou spectaculaire. Il est considéré désormais comme un risque sécuritaire majeur (GUARNIERI & PRZYSWA, 2012). L'Internet, en particulier, présente un certain nombre de risques en termes de contacts et de contenus potentiellement néfastes. Ces risques se déclinent à l'utilisation abusive de données personnelles, la réception des contenus

non désirés, aux informations fausses et aux contenus préjudiciables générés par les utilisateurs (REPC, 2019). Le temps d'exposition au risque multiplie les opportunités de tomber sur des occasions autant de commettre un délit que d'en être victime, ce qui explique la corrélation observée à maintes reprises entre délinquance et victimisation (PAUWELS ET SVENSSON, 2011). L'anonymat proportionné par Internet a permis aux cyberdélinquants – jusqu'à ce moment invisible – de se manifester, et les réseaux sociaux leur ont permis de développer la cohésion nécessaire pour s'organiser. Subséquemment, sur Internet cohabitent les manifestations les plus élevées de l'esprit humain comme les plus abjectes (LINDE & AEBI, 2020). L'utilisation problématique d'Internet peut mener à plusieurs conséquences négatives, notamment des problèmes sociaux et familiaux, des problèmes de santé mentale et même des tentatives de suicide (DUFOUR, GAGNON, NADEAU, LEGARE, 2019). Il est important d'être conscient de la relation entre les risques et les préjudices auxquels sont exposés tous les utilisateurs. Tous les risques ne causent pas des préjudices, et certains risques causent des préjudices plus souvent que d'autres. Et les risques cohabitent avec les opportunités (REPC, 2019) dans le cyberespace. Il est clair que certains des risques sont clairement liés à des infractions pénales (par exemple, l'extorsion sexuelle), tandis que d'autres concernent des comportements non criminalisés (par exemple, les préjudices résultant d'un contenu inapproprié pour un certain âge) (REPC, 2019). La cyberescroquerie est certes le fait de personnes qui portent atteinte à des règlementations. Mais, elle est aussi et surtout rendue possible parce que des usagers laissent des traces à ces cyberescrocs pour commettre leurs exactions ; ces traces peuvent être laissées consciemment ou inconsciemment (VEH, 2019). Et, la modification des habitudes de consommation est déterminante dans la commission de la cybercriminalité. Si la consommation permet à celle-ci d'évoluer, il faut mentionner que cette criminalité particulière progresse en passant par diverses formes. C'est en partant des diverses utilisations du cyberespace elles-mêmes que l'on voit apparaître une évolution de la cybercriminalité. Cette évolution s'adapte au modus operandi, (TANO, 2015). Les habitudes se sont transformées avec l'usage des réseaux électroniques. Sont ainsi concernés aussi bien les achats et le commerce. La dématérialisation de l'ensemble des systèmes de paiement, le recours à la monétique, à l'usage des réseaux électroniques et sociaux peuvent déboucher sur la commission d'actes relevant de la cybercriminalité (TANO, 2015). C'est-à-dire que le développement de nouvelles pratiques de consommation numérique telles que les services de transfert d'argent, de paiements de biens matériels et immatériels, qui offrent la possibilité à de nombreux consommateurs

éloignés des circuits de consommation d'y être insérés (GONZALES & DECHANET, 2015) et d'être les cibles des cyberescrocs. Ces pratiques de consommation permettent aux cyberdélinquants de configurer et modeler leurs manœuvres frauduleuses sur les réseaux ; en sachant que les usages des dispositifs numériques sont devenus des activités de plus en plus ordinaires dans le quotidien des individus et des impératifs pratiques (GRANJON & DENOUËL, 2011). Les usages sur les réseaux sociaux sont surtout liés à l'absence de contrôle de la part des utilisateurs. Il faut mesurer ici l'importance de ces nouveaux moyens de communication. L'usage démesuré de ces réseaux sociaux de la part des internautes conduit au stockage d'informations qui transitent par leurs bases de données et sont d'importantes mines d'informations, personnelles ou professionnelles, qui se retrouvent sur la toile publique. C'est en cela que des personnes mal intentionnées pourraient y avoir recours à des moments insoupçonnés (TANO, 2015). La cybercriminalité se diversifie ainsi dangereusement ; et les cyberescrocs et les cyber fraudeurs déploient un large éventail d'arnaques sur les réseaux (SCHLANGER et al., 2015) en exploitant les attitudes et/ou les comportements des utilisateurs et les caractéristiques du cyberespace, prolongement de la réalité sociale dans le virtuel. Les usagers, en tant qu'acteurs dotés « d'un minimum de savoir-faire nécessaire » pour rendre les technologies numériques opérationnelles, sont à la base de la notion d'appropriation. Bien qu'il soit incontestable que les cybercriminels ont un minimum de maîtrise technique et cognitive face aux technologies numériques (N'DIAYE,2008), il faut comprendre le processus par lequel « an individual or a community fit the ITCs to their needs » (un individu ou une communauté adapte les Technologies Informatiques et la Communication à ses besoins) en leur assignant des fonctions et des finalités propres à leurs besoins (ERWIN ET TAYLOR, 2005). Ces fonctions et ces finalités peuvent être détournées d'une part par les cyberescrocs pour constituer des menaces sur les cybercitoyens et les consommateurs, ainsi que pour le développement de la société de l'information et de l'économie (CISSE, 2011) et d'autre part par les utilisateurs pour conduire à des vulnérabilités (BAUMARD, 2014). Face à ces constats, nous pouvons nous interroger sur le profil des victimes de la cyberescroquerie ? Qu'est ce qui pourrait expliquer la victimisation des usagers ? Quelles seraient les implications de ces agirs ?

Pour répondre à ces questions, des théories ont été retenues pour la compréhension de la victimisation à la cyberescroquerie. En effet, les théories du mode de vie et de l'exposition, des perspectives, des besoins et de l'appropriation sociale des technologies paraissent plus indiquées pour comprendre les attitudes et agissements victimaires lors de la survenance de

cette délinquance. La théorie du mode de vie et de l'exposition est importante parce qu'elle a été l'une des premières théories systématiques de la victimisation criminelle. La principale prémisse de la théorie est que les différences dans les risques de victimisation sont associées à des différences dans les modes de vie. HANDLING, GOTTFREDSON ET GAROFALO (1978) définissent le mode de vie comme « les activités quotidiennes routinières, à la fois les activités professionnelles et les activités de loisirs ». Ainsi, selon le modèle de mode de vie/exposition, le comportement d'un individu est important pour prédire son risque de victimisation ou d'être victime. Certains utilisateurs sont exposés au risque de victimisation en raison de leur style de vie, des usages et/ou de leurs habitudes dans le virtuel. Le fait de passer beaucoup de temps de navigation en ligne sur des plateformes, des réseaux sociaux, des sites de rencontres, des forums et de rechercher activement des opportunités financières, des bourses, la cryptomonnaie et de jeux en ligne peuvent être des risques de victimisation. Il arrive que selon les techniques et pratiques utilisées par la plupart des cybercriminels : les arnaques à l'héritage, le chantage, l'arnaque aux sentiments, l'utilisation de faux documents (cartes bancaires, chèques etc.) (ANON, 2014) découlent des usages et services numériques. HANDLING, GOTTFREDSON ET GAROFALO (1978) ont examiné aussi les caractéristiques associées aux risques d'être victime d'un crime contre la personne. Ces auteurs ont constaté que plusieurs caractéristiques démographiques étaient associées à une forte probabilité d'être victime d'un crime contre la personne, notamment l'âge, l'état matrimonial, la situation d'emploi et le sexe. Qu'il s'agisse de fraude, d'escroquerie, d'extorsion, de vandalisme ou de harcèlement par exemple, les comportements malveillants ou criminels exploitent les caractéristiques d'Internet et portant préjudice aux internautes, aux organisations et à la société (GHERNAOUTI-HELIE ET A. DUFOUR, 2012) ; et les victimes sont à la fois des hommes et des femmes de plus d'une vingtaine d'année, exerçant à la fois dans l'administration publique que les entreprises privées et le secteur informel (VEH, 2017).

La théorie des perspectives, par ailleurs, mette en relief les comportements irrationnels face à la promesse de gains rapide. Elle s'articule autour de l'idée que les individus ne prennent pas des décisions en fonction de valeurs absolues, mais plutôt en fonction de gains et de pertes potentiels par rapport à un point de référence. Ce point peut être subjectif et dépend du contexte, de l'expérience passée et des aspirations de l'individu (KAHNEMAN & TVERSKY, 1979). En mettant en lumière les biais cognitifs qui influencent les choix, elle nous a permis de mieux comprendre pourquoi les victimes ne prennent pas toujours des décisions rationnelles. Les

démarches à effectuer pour percevoir les legs, les héritages, la loterie, les dédommagements dans les formes de cyberescroquerie relevant de l'acquisition de biens semblent être moindre en comparaison des sommes (gains) à recevoir par les victimes. La réception de ces gains est soumise au paiement de certains frais très souvent modiques au regard de la somme à recevoir ou à gagner par les moyens de paiement électronique (VEH, 2019). Quant à la théorie des besoins de MASLOW (1954), elle met en exergue l'importance des motivations qui régissent les comportements et éclaire sur les buts fondamentaux qui dirigent ceux-ci. Cette théorie classe les besoins humains en cinq niveaux, à savoir les besoins physiologiques, de sécurité, d'appartenance, d'estime et d'accomplissement. Cette structuration permet de mieux comprendre comment ces besoins influencent la motivation pour les atteindre. Cependant, la satisfaction de ces besoins diffère d'un individu à un autre et l'on ne peut prétendre satisfaire un besoin que lorsque le précédent l'est. Dès lors, les besoins d'appartenance se manifestent par le désir de créer des liens sociaux, que ce soit à travers l'amour, l'affection ou les relations interpersonnelles. L'importance des interactions humaines ne peut être sous-estimée. La satisfaction de ces besoins favorise des relations saines et un sentiment d'acceptation au sein de la société. Les relations virtuelles sont perçues comme plus accessibles, réalisables et acceptables. Ainsi, va-t-il naître entre les victimes et les cyberescrocs des relations « amoureuses », une confiance mutuelle et une entente sans pareille de sorte à rendre leur interaction étroite et à dissiper tout doute. Une certaine complicité apparait entre les victimes et les cyberescrocs et une responsabilité tacite les lie (VEH, 2019). Enfin, la théorie de l'appropriation sociale des technologies s'intéresse aux pratiques de la vie quotidienne des usagers d'internet. À l'analyse, les usagers ont une forte dépendance pour le travail, les relations et les opportunités en raison des pratiques (MICHEL DE CERTEAU, 1990) et des attributions de sens (à l'objet, à ses usages), d'acquisition d'une compétence et d'une culture technique, d'insertion dans la vie quotidienne et articulation à d'autres pratiques culturelles (LATZKO-TOTH, G., ET PROULX S., 2015). Ils font siens, s'attribuent la propriété et s'en rendre maîtres de l'outil (PLANTARD & AL., 2020). Les usagers l'intègrent à leur vie quotidienne tout en l'adaptant à leur personnalité, à leurs besoins et à leurs perceptions. Leurs usages vont les conduire à produire de nombreuses données les exposant dans le cyberespace et les rendant vulnérables à de potentiels crimes numériques.

Ces repères théoriques nous conduisent à formuler l'hypothèse suivante : « *la victimisation à la cyberescroquerie à Abidjan s'explique par une surexposition sur Internet,*

mais également par une attirance pour le gain facile, renforcée par une quête affective dans un contexte d'appropriation progressive du numérique. » L'objectif de l'étude est d'analyser la victimisation à la cyberescroquerie.

II- Méthodologie

Sites et participants à l'enquête

La ville d'Abidjan a servi de cadre d'étude. Elle est composée de dix (10) communes : Abobo, Adjamé, Attécoubé, Yopougon, Plateau, Cocody, Koumassi, Port-Bouët, Treichville et Marcory. Leur choix se justifie par le fait que selon la Plateforme de Lutte Contre la Cybercriminalité (PLCC), elles enregistrent de nombreuses victimes et les cyberdélinquants y sont disséminés. La population d'étude a été diversifiée. L'on a interrogé cent treize (113) usagers d'Internet ; vingt-cinq (25) fonctionnaires de police ; cent (100) victimes, quarante (40) cyberescrocs et deux (02) entretiens réalisés avec des responsables de la PLCC. Au total deux cents quatre-vingts (280) individus (sexes et âges confondus) ont composé l'échantillon et ont été interrogés. Cet échantillon est arbitraire mais ciblé du fait des liens directs des enquêtés avec l'objet d'étude.

Instruments de collecte des données

La combinaison de trois (03) différents instruments mais complémentaires ont facilité la collecte d'informations essentielles. Il s'agit de l'étude documentaire, du questionnaire et de l'entretien semi directif. En effet, l'étude documentaire est la recension de tout élément matériel constituant une source d'informations sur le phénomène étudié et permettant de cerner la portée des concepts en jeu et de découvrir les théories les plus explicatives des faits observés et de faire ressortir les aspects du problème. Les documents consultés se composent de revues scientifiques, technologiques et économiques, des rapports et des articles en ligne sur l'escroquerie en ligne, les risques du numérique et la victimisation criminelle. Le questionnaire consiste à poser une série de questions aux enquêtés pour analyser le rôle causal des victimes à partir des informations recueillies, de les quantifier et de procéder à des analyses de corrélation. L'administration du questionnaire s'est faite de façon directe et indirecte avec les enquêtés (cyberescrocs, victimes, usagers et fonctionnaire de police de la PLCC) de sorte à recueillir des informations claires et précises sur les attitudes et agissements victimaires des utilisateurs d'Internet dans la manifestation de la cyberescroquerie. L'entretien semi-directif consiste à un entretien oral avec un ou des participants à l'enquête avec quelques questions définies en guise de repère et permettant à ceux-ci de s'exprimer plus librement sur un sujet donné. La réalisation

des entretiens semi-directifs avec les responsables de la PLCC a permis d'obtenir des informations sur les formes de la cyberescroquerie à laquelle sont exposés les usagers et/ou les victimes et le profil des victimes.

Analyse des données

Elle s'est appuyée sur l'analyse qualitative et l'analyse quantitative. De façon pratique, l'analyse qualitative a permis de mettre un accent sur le vécu des victimes, des cyberescrocs et des fonctionnaires de police de sorte à cerner les processus qui se développent entre victimes et cyberescrocs et les significations qu'ils leur attribuent. Quant à l'analyse quantitative, elle a permis d'observer les fréquences des réponses sur les facteurs explicatifs, de les analyser et de les interpréter et d'établir les caractéristiques sociodémographiques.

III Résultats

Les résultats de l'étude portent sur la victimisation des personnes ciblées par la cyberescroquerie via les formes, le profil des victimes, les attitudes et les agissements victimaires et les conséquences dans l'expansion de la cybercriminalité. Elle propose des solutions sous la forme de recommandations.

3-1 Formes de cyber escroqueries

De nombreux actes de cyber escroqueries se déroulent dans le cyberespace. Il y ressort différentes formes qui émergent à Abidjan. Ainsi, a-t-on des formes basées sur des relations amoureuses et sexuelles et des formes basées sur l'acquisition de biens financiers.

3-1-1 Formes de cyber escroqueries relevant des relations amoureuses et sexuelles

Ce sont les actes d'escroquerie dans lesquels les cyberescrocs nouent de fausses relations affectueuses avec leurs victimes ou font croire à leurs correspondants qu'ils vivent une relation amoureuse de sorte à les solliciter fréquemment pour la résolution de différents problèmes sociaux afin de leur soutirer des biens financiers. Ces faux sentiments mis en œuvre impliquent tacitement une certaine prise en charge de l'être aimé dans la subvention tantôt de ses besoins primaires, tantôt dans l'apport d'un secours pour toute difficulté soumise à l'amoureux ou l'amoureuse. La vie de l'un des amoureux est totalement prise en charge dans une certaine mesure par l'autre. Une sorte de relation de dépendance se noue entre eux. *« J'étais en relation sentimentale avec un certain Florent Dubois habitant au Togo qui me sollicitait souvent pour régler des problèmes divers et je ne trouvais aucun inconvénient à aider mon amoureux. Mais je me suis rendu compte bien tardivement que j'étais victime d'arnaque, lorsque je n'arrivais plus à entrer en contact avec lui via Facebook ni par téléphone. Jamais,*

je n'aurai cru tomber dans un tel piège, tout était si vrai... Voilà que j'y suis tombée, plus de 30000 euros partis (19 650 000 f cfa). Je suis détruite, anéantie. Je pense souvent à la mort tellement j'ai honte. Et les banques me taxent encore plus… », affirme la victime N. B., de sexe féminin. Par ailleurs, cette forme les cyberescroquerie met en actes un autre artifice basé sur les sentiments amoureux pour disposer de films et/ou de photographies à caractère pornographique de leur « soi-disant amoureux ou amoureuse » pour la faire chanter. Le désir de faire l'amour avec le correspondant est au centre de leurs nombreuses conversations de façon à emmener la victime à faire l'amour par la webcam et la piéger. Les sentiments amoureux (et le sexe) sont le fondement de la pratique de cette forme de cyber escroquerie. Car, le désir d'être aimé et de nouer une relation amoureuse (et/ou de satisfaire des besoins sexuels) animant tout individu ayant un compte sur les plateformes et forums de rencontre sont usités par les cyberdélinquants pour soutirer des sommes d'argent à leurs victimes. « *Les escroqueries basées sur les relations amoureuses sont celles qui sont les plus mises en œuvre par les cyberdélinquants dans le cyberespace ivoirien ; ils profitent des sites de rencontres, de Facebook pour nouer des relations amoureuses avec leurs correspondants et les soumettent à des demandes incessantes jusqu'à ce que le correspondant se rend compte qu'il est victime d'arnaque ou ils font chanter ceux-ci. Ces escroqueries sont pratiquées particulièrement par tous les cyberdélinquants d'Abidjan Nord et Sud* », explique l'adjudant de police T. R. de la PLCC, de sexe masculin.

3-1-2 Formes de cyber escroqueries relevant de l'acquisitions de biens financiers

C'est un ensemble d'actes de cyber escroquerie dans lesquels les cyberescrocs mettent en œuvre des subterfuges fondés sur des donations, des legs, des héritages, des dédommagements et des achats/ventes de tout article ou objet en ligne. Dans la mise en œuvre de ces actes, ils jouent sur la cupidité, l'attrait à la facilité et la volonté de dédommagement d'un préjudice de certaines victimes pour abuser d'elles. Ils mettent à profit ces « mauvaises » habitudes et agissements des internautes pour les transformer en comportements exploitables pour disposer d'eux. Ils incitent ou motivent les internautes à agir en fonction de leur but recherché, celui de leur soutirer de l'argent tout en leur faisant miroiter qu'ils sont ceux qui s'en sortiront avec un profit considérable dans les différents subterfuges élaborés. Les cyberescrocs usent ainsi de ces dispositions et attitudes des internautes pour leur porter préjudice. Dès lors que ces préjudices sont causés, les victimes se culpabilisent de n'avoir pas pu déceler les supercheries. Dans cette forme, les cyberescrocs établissent un ensemble de faux documents administratifs et/ou commerciaux pour attester ou prouver un droit. Ils fabriquent entre autres

des actes de donations, de legs, d'héritages, de loteries ou encore différents documents de dédommagement des victimes et/ou de commerce, etc. qui sont souvent soumis au paiement de frais pour l'établissement des dits actes dans les administrations des pays des donateurs (des cyberdélinquants), des institutions octroyant les loteries pour conduire leurs victimes à s'acquitter du paiement de ces frais pour entrer en possession soit de ces dons, ces legs, ces héritages, ces lots de loterie ou encore faciliter les transactions. Les victimes potentielles se soumettent à toutes les démarches indispensables leur présentées par les cyberescrocs pour entrer en possession de leur dû. Ainsi, ne lésinent-ils pas sur les moyens à débourser pour acquérir ces différents biens sans se soucier qu'ils peuvent être victime d'escroquerie. Ces agirs conduisent les victimes à la remise de sommes considérables. Cette forme nécessite plus de minutie de la part des cyberescrocs dans leurs échanges avec les victimes. Les biens (les sommes d'argent) enjeux sont plus ou moins très importants et leur obtention y dépend. Le cyberescroc T. K., de sexe masculin, de la commune de Cocody, explique que : « la brou [1]*par scan permet d'avoir gros mais il faut être patient et prendre son temps ; quand le client tombe, il va payer jusqu'à ah ah ah ah…. Car il croit qu'il va avoir les dons, l'héritage qui lui est promis. Il n'y a pas beaucoup de barasseurs*[2] *qui sont dans ça. A baby (Abidjan Nord et Sud), c'est le Love tchat et Pervers qui font fort* ».

3-1-3 Mode opératoire

Dans l'accomplissement des actes, les cyberescrocs sont en étroite interaction avec les victimes. Ils posent envers elles des actions les amenant à la remise de biens financiers. Ces actions constituant des interactions entre victimes et cyberescrocs peuvent se résumer en six grandes étapes quelle que soit la forme de cyber escroquerie dans laquelle l'on se retrouve. Elles ont en commun trois grandes étapes : la relation de la mise en confiance de la victime par le cyberescroc, l'acte de l'envoi d'argent vers le cyberescroc par la victime et le retrait d'argent de la victime par le cyberescroc. Celles-ci sont basées sur les agirs et comportements des victimes qui mettent en exergue leur implication dans la réussite de la cyberescroquerie. Ces étapes sont enserrées par trois autres étapes qui diffèrent sensiblement en fonction de la forme de cyber escroquerie par les sollicitations ; création de faux profils/fausses annonces ou l'envoi de « faux » mails du cyberescrocs à la victime, la recherche de victime par l'envoi d'invitation

[1] Ce terme est le diminutif du broutage dans l'univers cybercriminel signifiant cyberdélinquance ou cybercriminalité. Ici, il met l'accent sur le mode opératoire et l'outil utilisé par le cyberdélinquant dans la cyberescroquerie

[2] Ce terme est une autre appellation des brouteurs, des cyberdélinquants ou cyberescrocs, dérivant du dialecte malinké Bara (Travail). Ici, l'accent est mis sur l'activité cybercriminelle comme étant une activité « licite » et les individus la pratiquant exercent une activité « licite » comme tout autre.

et les divers échanges (Echange de photos intimes-Relation sexuelle par Cam Suivi-de menace de publication ; Fausses sollicitations ; Acceptation de la victime par le paiement de frais). L'escroquerie au dédommagement, l'escroquerie à l'héritage et legs et l'escroquerie à la loterie relevant des escroqueries d'acquisition de biens ont le même procédé comparativement à l'escroquerie à l'achat/vente. Quant aux escroqueries au chantage à la vidéo et aux faux sentiments, elles obéissent visiblement au même procédé mais diffèrent dans certaines phases d'exécution (Echange de photos intimes-Relation sexuelle par Cam-Suivi de menace de publication et Fausses sollicitations). Elles ont le même procédé mais diffèrent. Les comportements et habitudes des victimes sont plus ou moins déterminants. Ils permettent de connaître ces personnes victimes, leurs perceptions, leurs appropriations et de savoir leur rôle causal ou de percevoir leur engagement actif et/ou passif. Cette pratique résulte d'une interaction cyberescrocs-victimes.

3-2 Profil des victimes

Les victimes jouent un rôle plus ou moins important dans la réalisation de la cyberescroquerie. Elles disposent d'un ensemble de traits qui les caractérisent et sont relativement en rapport avec leur statut. Ces traits sont entre autres leurs caractéristiques socio-démographiques, professionnelles et leur rôle dans la survenance du crime.

3-2-1 Caractéristiques socio-démographiques et professionnelles

Les victimes sont à la fois des hommes et des femmes de plus d'une vingtaine (20) d'année et exerçant dans l'administration publique, les entreprises privées et le secteur informel. Elles disposent de revenus, de comptes mails, de compte sur les réseaux sociaux et les forums de rencontre, les sites commerciaux. Les victimes issues des secteurs public et privé sont nombreuses que celles du secteur informel. Car elles disposent d'une certaine connaissance dans l'usage des services numériques. Celles du sexe masculin sont autant victimes que celles du sexe féminin. Les victimes provenant, par ailleurs, de l'Europe (France, Allemagne, Espagne, Belgique, Suisse) et d'Amérique du Nord (Canada) sont plus nombreuses comparativement à celles provenant de l'Afrique. Toutefois, des usagers de nationalité ivoirienne et nigériane sont davantage victimes. Ils sont maintenant des cibles des cyberescrocs de sorte que « *le broutage n'est plus des actes dirigés contre les occidentaux uniquement mais vers des clients nationaux et tous ceux qui peuvent être escroqués en ligne* » selon le sergent-chef de police T. K. de la PLCC, de sexe masculin.

3-2-2 Rôle causal des victimes

Les victimes jouent un rôle plus ou moins non négligeable. Elles ont des attitudes et/ou des agirs déclenchants, actualisants en étroite relation avec cette activité délictueuse. Les victimes sont tantôt « catalyseuses », tantôt « influencées ». Leurs rôles ainsi que leurs attitudes et comportements sont déterminants dans la survenance du crime.

3-2-2-1 Victimes catalyseuses

Ce sont celles qui ont tendance à diffuser leurs pensées les plus intimes, leurs photographies personnelles ainsi que tous les évènements de leurs vies quotidiennes sur les réseaux sociaux, sur leurs profils ou leurs comptes (Facebook, forums de rencontre) sans la prise réelle de précaution. C'est-à-dire elles rendent publics leurs différents profils à des tiers. En effet, dans certaines formes de cyberescroquerie, la recherche de victime se fait par les visites des différents profils ou comptes de ceux-ci. Lorsque ces profils ou ces comptes sont animés et que le propriétaire (détenteur) interagit avec plusieurs personnes et dispose d'une bonne qualité (situation socio-professionnelle), il est systématiquement la cible de cyberescrocs. Une demande d'ami lui est envoyée et il est fort probable qu'elle accepte afin que se déclenche les actes de cyberescroquerie. Par ailleurs, il y a celles s'inscrivant sur des sites de rencontre (soit payant ou soit gratuit) à la recherche de partenaire ou d'âme sœur. Leurs désirs de faire des rencontres et si possible d'avoir des relations amoureuses avec leurs correspondants inhibent leurs capacités d'attention et de méfiance. Elles ont une trop grande confiance en ces plateformes et tous leurs correspondants, et de fait, elles interagissent sans prise minime de mesures de sécurité, de vigilance et sont pour la plupart les victimes. Les victimes catalyseuses sont celles qui facilitent le déclenchement et la réalisation de ce crime. Ainsi, selon l'ex responsable de la PLCC, l'officier de police J. R., de sexe masculin, de la commune de Treichville (zone d'Abidjan Sud), « *lorsqu'elles sont en correspondance avec les cyberdélinquants ils leur aient aisé de savoir (connaître) qu'elles vont payer* ». Ces victimes sont prisées en ce sens qu'elles leur facilitent la tâche dans leur quête de correspondants sur la toile. Elles prennent plaisir à interagir avec ces derniers (cyberescrocs) et de façon habile ceux-ci les conduisent à poser des actes allant dans le sens d'extorsion d'argent.

3-2-2-2 Victimes influencées

Ce sont celles qui, dans la recherche des cyberescrocs, sont influencées par divers subterfuges dans leurs correspondances. Elles ne sont pas choisies sur des critères, mais bien plus par le coup du sort. Elles sont celles à qui sont envoyées des courriels pour leur indiquer

qu'elles ont été lauréates d'une loterie, qu'elles ont été choisies pour disposer d'un legs, d'un héritage ou encore qu'elles aient été victimes d'une escroquerie via Internet et qu'elles vont être indemnisée. Elles vont être influencées par l'usage de différents documents administratifs frauduleux et de logos officiels d'institution usurpés par les cyberescrocs pour leur faire croire à la sincérité des faits. Dans les correspondances, ils font intervenir des personnes ayant de « fausses » qualités dans l'administration occultant ainsi plus ou moins toute suspicion. Ces personnes sont entre autres des huissiers de justice, des avocats, des magistrats, des officiers de police, des notaires, etc. pour crédibiliser les actions d'extorsion de fond. Leur dextérité est telle qu'il est plus ou moins difficile de déceler la supercherie, les falsifications d'actes ou de documents administratifs portant la signature de l'autorité compétente. Elles sont induites en erreur par le formate[3] dans lequel les faux documents administratifs sont mis en avant pour persuader celles-ci et les amener à poser des actes allant dans le sens de la remise de fonds. La majorité des victimes ne font pas assez attention à la qualité des actes leur transmis et aux faux organismes ayant pris contact avec eux. Elles se laissent ainsi abuser pour se faire soutirer de l'argent. « *Il y a des victimes qui sont responsables des préjudices qu'elles subissent ; ceux qui sont victimes de l'escroquerie à l'héritage et legs, donation, à l'achat/vente, à la loterie...qui laissent s'exprimer leur cupidité, leur attrait du gain facile. Comment un individu qui n'a participé à aucun jeu peut être un lauréat ? Comment quelqu'un peut croire à une assistance de déblocage de fonds soumis à une commission de la somme à débloquer ? Il faut reconnaître que les victimes de certains types d'escroquerie sont responsables de leur propre victimisation...* », explique l'officier de police P. K. de la PLCC, de sexe masculin.

3-3 Facteurs liés à la victimisation

La victimisation des personnes ciblées dans la cyberescroquerie est sous-tendue par une interaction des logiques psychosociales et structurelles. Celles retenues dans l'étude sont : la surexposition sur Internet, l'attirance pour les gains faciles, la quête affective et l'appropriation des technologies numériques.

[3] Ce terme signifie dans la sous culture des cyberdélinquants, l'usage de faux documents et de fausses pièces administratives pour tromper ou persuader les victimes de la véracité de toutes leurs correspondances de sorte qu'elles se soumettent à toutes leurs sollicitations

Tableau N°1 : Répartition des facteurs explicatifs de la victimisation des personnes ciblées dans la cyberescroquerie

	Fréquence	Pourcentage	Pourcentage accumulé
Autres	00	00	00
Surexposition sur Internet	75	27%	27%
Attirance pour les gains faciles	63	22%	49%
Quête affective	65	23%	72%
Appropriation des technologies numériques	77	28%	100%
Total	280	100%	

Source : Enquête, réalisée à Abidjan, en 2023

Il ressort de l'analyse des données recueillies sur les facteurs explicatifs que la surexposition sur Internet (27% des réponses), l'attirance pour les gains faciles (23% des réponses), la quête affective (23%réponse) et l'appropriation des technologies numériques (28% des réponses) sont en lien avec le processus de victimisation à la cyberescroquerie. Ces attitudes et agissements victimaires sont exposés dans l'espace virtuel de sorte que dans l'expression des formes d'escroquerie sur Internet, les cyberescrocs en usent pour affiner leurs différents subterfuges et échanges étroits avec celles-ci. Sans ceux-ci, ils seraient périlleux aux cyberescrocs de réaliser ces actes de cyberescroquerie, malgré leur degré de compétences psychosociales et techniques, et leur Co-délinquance (VEH, 2019 ; ETTIEN, 2022). Les victimes interagissant différemment dans la manifestation de ce crime laissent entrevoir ces logiques psychosociales et structurelles dans leurs échanges dynamiques avec les cyberescrocs et leurs actions ont une portée prépondérante à chaque étape dans le monde virtuel et dans la vie réelle. Elles jouent divers rôles concourant à l'accomplissement de ces actes dans le cyberespace, mettant en lumière les caractéristiques socio-démographiques et leur profil. La surexposition sur Internet (partage excessif de photo/vidéo personnelles, divulgation d'informations privées, publication fréquente d'opinions sensibles et activités en temps réel, navigation, etc.), l'attrait pour le gain facile (désir de sortir de la précarité, modèle de réussite rapide, croyance aux histoires de leg et donation, influence des réseaux sociaux), la quête d'affection (nature humaine, manques affectifs, influence des réseaux sociaux, sites et forum de rencontre) et l'appropriation des technologies numériques (forte dépendance, usages des TIC en lien avec la personnalité, les

besoins et perceptions, un détournement de l'usage critique du numérique) conduisent les victimes à agir en fonction de leurs attentes, qui reflètent les agissements et comportements qu'elles extériorisent dans le monde virtuel. *Le « sextorsion » revêt un caractère pervers et met en cause une certaine moralité des individus victimes qui se manifeste par l'exhibitionnisme de leur nudité via la webcam dans le cyberespace quel que soit le statut socio-professionnel et matrimonial de ceux-ci*, explique l'officier de police Mme K. D. de la PLCC, de sexe féminin.

3-4 Conséquences de la victimisation à la cyberescroquerie

Elles sont nombreuses tant sur le plan psychologique, social que financier ; et sont d'une gravité avérée dans le monde physique et virtuel.

3-4-1 Sur le plan psychologique

Ce sont tous les ressentiments et sensations de dégout, de peur, de crainte que les personnes vivent, notamment la culpabilité, la perte de l'estime de soi, la perte de confiance en Internet, le traumatisme émotionnel. En effet, la culpabilité que ressentent les victimes n'est pas une émotion en soi. Elle procède d'une mauvaise expérience vécue qui vient mettre à mal des valeurs ou principes moraux. L'ensemble des victimes ressent celles-ci. Elles s'accusent d'avoir été plus ou moins responsables de ce qu'elles ont subi par leur manque d'attention, de vigilance, leur naïveté ou leur cupidité. Elles s'en veulent de ce que durant leurs interactions de n'avoir pas pu se rendre compte de la manipulation ou du faux marquant leurs différents échanges. « *La cybercriminalité non seulement me crée des ressentiments, mais aussi une remise en cause de ma personne ; je crois que ce qui m'arrive est en partie de ma faute. Comment j'ai pu me laisser avoir ? Je peux même plus regarder les gens en face »*, affirme la victime K. A. de sexe féminin. Elles ont une perte de l'estime de soi. Celle-ci est basée à la fois sur la personnalité et les capacités intellectuelles. Elle les conduit à un mal être et entraine des difficultés dans les relations avec leurs proches, leurs amis, leurs collaborateurs et/ou toute autre personne avec laquelle elles sont en relation. Cela se constate chez les victimes de la forme de cyberescroquerie relevant des relations amoureuses et sexuelles (du chantage à la vidéo et de faux sentiments). Elles souffrent terriblement de leurs agirs. Ce qui provoque un problème dans leur épanouissement et bien-être personnel, comme l'atteste les propos de la victime V. A. de sexe masculin, *« tout le monde peut tomber sur le coup de la tentation et être faible à tout moment. J'ai pensé que cela n'arrivait qu'aux autres...aujourd'hui je suis une victime et je n'en*

reviens pas. Ç'a changé négativement ma personne ; je ne suis pas contente de moi ». Les victimes n'arrivent plus à supporter le regard de leur environnement et tout geste de celui-ci est mal interprété par ces dernières. Cela conduit certaines victimes à la dépression et/ou à l'anxiété. Ce sont des moments ou des périodes difficiles que traversent les victimes et donc pouvant les conduire à des agirs peu valorisants tels que la marginalisation de soi, la réclusion de soi etc. En outre, les victimes évitent d'avoir recours à tout service immatériel offert par Internet. Il n'est pas rare de les voir fermer définitivement leurs différents comptes sur les réseaux sociaux, forums et site de rencontres et de ne plus recourir aux achats en ligne via les sites commerciaux. Elles éprouvent de l'aversion envers le médium Internet et refusent d'avoir recours dorénavant à celui-ci. Il en résulte une non-acceptation de l'usage du numérique. Leurs intentions étant influencées par leurs attitudes, leurs croyances et les caractéristiques de l'outil, elles rejettent l'outil. Aussi ressentent-elles un traumatisme émotionnel. Elles vivent relativement mal cette expérience et sont impuissantes face à tout ce qui leur arrive dans le cyberespace et dans le monde réel. Les victimes sont abattues et stressées par ce qu'elles vivent. Le regard inquisiteur de l'autre renforce le traumatisme. Elles n'arrivent pas à oublier cet épisode triste de leur vie. Elles semblent apparaître étiquetées à vie en ce sens que dans le cyberespace tout n'est que flux d'informations numérisées et une suppression d'élément ne signifie pas que la menace a été endiguée totalement. Ainsi, les victimes sont en stress permanent conduisant plus ou moins à long terme à des séquelles et à un déséquilibre mental.

3-4-2 Sur le plan économique et social

Ce sont l'ensemble des effets négatifs de l'activité délictueuse sur la vie sociale et économique des victimes. Ce sont les abus sexuels et la perversité, le suicide et les pertes financières. En effet, certaines victimes subissent des abus sexuels de la part de cyberescrocs spécialistes en escroquerie de chantage à la vidéo et aux faux sentiments. Ceux-ci prennent un malin plaisir à nouer une relation et à réaliser leurs fantasmes et leurs vices sur celles-ci en leur proposant des ébats sexuels au risque de diffuser ou publier via Internet des vidéos ou photographies intimes d'elles. Les victimes se soumettent de facto à ces exigences et sont embarquées dans un cercle d'abus. Lorsque le désir de réaliser ces fantasmes se déclenche, le cyberescroc entre en contact avec sa victime et lui intime l'ordre de prendre toutes les dispositions (la prise d'une chambre d'hôtel à sa charge, le paiement du transport du cyberdélinquant et des repas/boissons), pour le réaliser et celle-ci s'exécute. En gardant le

silence, la victime se fait, malgré elle, l'alliée de celui-ci, puisque la seule chose qu'il redoute, c'est d'être dénoncé. Le fait de devenir ainsi, bien involontairement, son alliée, renforce le mépris qu'elle a d'elle-même et sa culpabilité. Elle devient à la limite un objet sexuel. La victime P. C. de sexe féminin, l'atteste par ces propos : « *Je suis victime de chantage à la vidéo. Voici deux mois maintenant que je suis objet d'abus sexuel de mon cyberdélinquant. La peur de voir ma nudité sur internet m'a amené à toujours répondre favorablement à toutes les demandes en argent et rapports sexuels, de mon cyberdélinquant. Car, je suis une femme mariée, mère de famille et institutrice et cela n'est pas du tout bon pour moi si mes images venaient à être diffusées. C'est ce qui m'a amenée à faire tout ce qu'il me demandait jusqu'au jour où je me suis confiée à une sœur qui en a parlé à son ami policier et nous sommes venus ici à la PLCC porter plainte* ». L'abus se poursuit souvent sous un silence plus ou moins coupable. Par ailleurs, d'autres victimes envisagent ou se suicident dans bien des cas. Elles sont dissuadées si elles ont confié ce sentiment à des tiers. Quand celui-ci survient, il est dû à la question de l'honneur, de l'honorabilité, du chantage et de la dépression. La manipulation des victimes, la publication des images ou des vidéos de leur intimité et leur chantage, les poussent à la commission de l'irréparable en ce sens qu'elles vacillent entre le virtuel et le réel. Il est vrai que le taux de suicide des victimes de cette pratique est faible. Mais, il n'est pas négligeable. Les victimes subissent aussi des préjudices financiers très importants. Elles se rendent compte de la supercherie quand elles n'ont plus de ressources pour faire face aux différentes sollicitations ou exigences des cyberescrocs. Elles enregistrent des pertes financières énormes dans leurs différentes interactions avec ceux-ci. Ces pertes sont évaluées à plus de cinq milliards de francs CFA (ANSSI ; 2024) ; et l'on s'interroge sur le chiffre noir de cette activité délictueuse. L'on s'aperçoit qu'ils arrivent à soutirer des sommes considérables à leurs victimes et du coup à porter atteinte à leurs biens. Les victimes font face à des pertes financières dont l'évaluation demeure relative mais l'on convient que ces pertes sont considérables. Tous les acteurs de lutte sont d'avis qu'il est difficile de savoir avec précision l'impact financier de cette activité cybercriminelle. Les victimes provenant de la France, de la Côte d'Ivoire et du Canada cumulent le plus grand nombre de préjudice financier (PLCC 2014 ; 2015 ; ANSSI, 2024).

3-5 Propositions de mesure

Elles sont en direction des usagers d'internet, de l'Etat et des entreprises afin de réduire la victimisation à la cyberescroquerie et de garantir la sécurité numérique sur les réseaux de

communication et d'information et changer positivement les attitudes et les agissements des usagers.

- **Au niveau des usagers**

- Sensibiliser et éduquer les usagers aux bons réflexes, à l'éthique et aux valeurs ;
- Eviter une surexposition sur Internet ;
- Eviter de développer des comportements addictifs ;
- Protéger la vie privée ;
- Valoriser l'estime de soi ;
- Entretenir la santé mentale ;
- Vérifier la légitimé et la sécurité d'un site (adresse électronique, la sécurité) ;
- Se méfier des offres alléchantes et vigilant pendant la navigation sur Internet ;
- Être informé des risques et des crimes via Internet ;
- Renforcer la sécurité personnelle des comptes sur les sites, les réseaux sociaux et forums ;
- Signaler toute tentative ou préjudice à la PLCC.

- **Au niveau des entreprises**

- Renforcer la sécurité des comptes, forums, sites de rencontres et commerciaux ;
- Envoyer des alertes sécuritaires et d'informations ;
- Collaborer à la suppression ou la suspension des comptes incriminés ;
- Publier une charte de bon usage des sites, forums et plateformes ;
- Faire une veille technologique sur les sites, forums et plateformes.

- **Au niveau de l'Etat**

- Renforcer la coopération policière régionale et internationale et les capacités de police ;
- Signer des collaborations avec les grandes firmes numériques des réseaux sociaux ;
- Adapter la politique criminelle ;
- Concevoir une politique de cybersécurité ;
- Prendre en charge psychologiquement les victimes ;
- Mener des campagnes de sensibilisations sur la cybercriminalité ;
- Sensibiliser les populations au signalement d'attitudes déviantes à la police ;
- Faire du Marketing Social.

IV- Discussion et conclusion

L'étude sur le rôle causal des victimes dans l'escroquerie sur Internet a été mené auprès d'une population diversifiée, au nombre de deux cent quatre-vingts (280) participants. Les entretiens et questionnaires ont permis de collecter les données et les modèles d'analyse quantitative et qualitative de les quantifier et les interpréter. L'objectif de l'étude est de chercher à analyser la victimisation à la cyberescroquerie. Le traitement et l'analyse des données ont facilité la description du processus de victimisation, de déterminer les logiques, d'en tirer les conséquences et de proposer quelques mesures sous forme de recommandation. De nombreux actes de cyber escroqueries se déroulent dans le cyberespace. Différentes formes se manifestent notamment celles basées sur des relations amoureuses et sexuelles et l'acquisition de biens financiers. Elles résultent d'interaction victimes-cyberescrocs dans laquelle les victimes sont plus ou moins enclines à s'investir pour sa réussite face aux différentes étapes à franchir. Les victimes sont à la fois des hommes et des femmes de plus d'une vingtaine (20) d'années, exerçant dans l'administration publique, les entreprises privées et le secteur informel. Elles disposent de revenus, de comptes mails, de compte sur les réseaux sociaux et explorent les forums de rencontre et les sites commerciaux. Elles proviennent de l'Europe (France, Allemagne, Espagne, Belgique, Suisse) et d'Amérique du Nord (Canada) ainsi que de l'Afrique (Côte d'Ivoire et Nigéria). Elles sont tantôt « catalyseuses », tantôt « influencées ». Elles sont celles qui par leurs agirs provoquent, initient ou facilitent le crime et/ou celles qui se laissent manipuler par des artifices des cyberescrocs pour être induite en erreur. L'analyse des données expose des logiques psychosociales et structurelles en interaction favorisant la victimisation à l'escroquerie via Internet. Elles sont entre autres la surexposition sur Internet, l'attrait pour le gain facile, la quête affective et l'appropriation du numérique. Les attitudes et agissements victimaires entrainent diverses conséquences tant aux plans psychologique, économique que social, à savoir la culpabilité, la perte de l'estime de soi, le traumatisme émotionnel, le préjudice financier, le suicide, etc. L'hypothèse de la recherche selon laquelle « *la victimisation à la cyberescroquerie à Abidjan s'explique non seulement par une surexposition sur Internet, mais également par une attirance pour le gain facile, renforcée par une quête affective dans un contexte d'appropriation progressive du numérique* » est confirmée. Dans la pratique de la cyberescroquerie, les interactions victimes-cyberescrocs procèdent de l'exposition de la vie

privée des victimes sur la toile (réseaux sociaux, site de commerciaux, forums) qui sont des données immatérielles dont usent les cyberescrocs pour configurer, modeler et personnaliser leurs différentes approches et scénarios pour nouer les contacts. Celle-ci est source de risques. En effet, la publication d'informations personnelles sur Internet, sans une prise de mesures de sécurité ou du moins de précaution, expose les utilisateurs. C'est à dire que la diffusion de photographies personnelles, de contacts, de qualité (fonction), de statut matrimonial, d'idéologies, de centres d'intérêts, d'hobbies ainsi que tous les évènements de leur vie quotidienne sur les réseaux sociaux, les forums, font des usagers des cibles idéales pour les cyberescrocs. L'adoption de telles conduites est directement associée à une augmentation du risque de victimisation sur le plan individuel (A-M. COTE, 2014). Ces agissements et attitudes liés aux TIC est un moment d'exposition au risque (…) et d'occasions d'être victime, (PAUWELS ET SVENSSON, 2011). Ceux-ci laissent des traces immatérielles inconsciemment ou consciemment que des personnes mal intentionnées (cyberescrocs) pourraient y avoir recours à des moments insoupçonnés (TANO, 2015) ; l'exposition de la vie privée se traduit en des données personnelles et contenus préjudiciables générés par les utilisateurs (victimes potentielles) qui présente un certain nombre de risques en termes de contacts (REPC, 2019) avec certaines personnes (cyberescrocs), à des fins criminelles alors que les concepteurs des systèmes d'information, n'avaient jamais pensé à ce type d'usage détourné (KOFFI, 2022). Cela montre aussi l'importance de la théorie de l'appropriation sociale des technologies (MICHEL DE CERTEAU, 1990) et des usages des utilisateurs (PLANTARD & Al., 2020) de sorte à les rendent vulnérables face à cette forme de cybercriminalités. Leurs usages quotidiens du numériques sans éducation critique les conduisent à s'exposer dans le cyberespace par l'assignation de nouveaux usages aux plateformes, forums, comptes en ligne, sites marchands qui induisent des vulnérabilités. Ceux-ci vont être par la suite utilisés par les cyberescrocs. Ainsi, les victimes voient leur identité être associée frauduleusement à des actes de cyber escroquerie. Il s'agit notamment, de renseignements personnels relatifs à leur nom, adresse, numéros de téléphone, date de naissance et logo. On parle alors d'usurpation d'identité. On retrouve ce type de victimisation dans les cas d'arnaques à la loterie (les noms de banques où de grandes entreprises sont associées à l'escroquerie) (GUEU, 2013). Les usages vont, en outre, exposer des besoins affectifs qui seront des vulnérabilités émotionnelles dans l'espace virtuel notamment sur les sites de rencontre et comptes personnels associés. Les relations humaines virtuelles étant perçues dorénavant comme plus accessibles, possibles et convenables,

influencent les attitudes et agirs des utilisateurs en quête d'âmes sœurs à avoir recours à Internet et à s'y investir. La volonté de satisfaire ces besoins d'appartenance (MASLOW, 1954) influence les émotions sur la prise de décision en usant des plateformes proposant des rencontres à cet effet. Des usagers vont s'inscrire sur ceux-ci en (..) pour chercher par cette voie, des amis à travers l'Occident pour un projet de mariage (et de relations amoureuses). Les pourparlers se déroulent normalement et les échanges de photos sont faits et le futur mari ne trouvera pas d'inconvénient pour faire venir à son « âme sœur », les moyens nécessaires pour les préparatifs du mariage, bien attendu, ce mariage n'aura jamais lieu (GUEU, 2013). A ces actes s'ajoutent des agissements traduisant une certaine économie comportementale des usagers tant sur les sites marchands que dans la réception de mails non désirés (proposant des legs, donations, loteries etc.). Des comportements irrationnels face à la promesse de gains rapides et de bonnes affaires se perçoivent sur la toile. Ceux-ci signifient que des usagers agissent dans leurs interactions avec les cyberescrocs en fonction de leurs émotions, leurs croyances et leurs sentiments de sorte à les faire dévier de la rationalité humaine lorsqu'il s'agit de recevoir des gratifications financières et donations en échange d'aide, d'un acquittement de frais transactionnels très souvent appréciable comparativement au pourcentage à recevoir ; ils se verront soutirer de l'argent. Les victimes exposent ainsi leurs attraits pour les gains faciles et/ou les profits dans l'escroquerie 419 (GUEU, 2013). L'étude remet en perspective l'attribution singulière du rôle de victime comparativement au cyberescroc. Bien qu'il existe une interaction entre les deux statuts, les attitudes et agissements des victimes ne peuvent être éclipsés dans la compréhension de la cyberescroquerie. Les risques de victimisation varient en fonction des caractéristiques des individus, du contexte et de l'environnement. Il serait judicieux de renforcer l'éducation numérique, de disposer de programmes de prévention en ligne, de prendre en charge psychologiquement les victimes et à l'Etat de s'approprier le marketing social etc. Toutefois, l'on relève quelques limites dans l'étude. La méthode d'échantillonnage (échantillon arbitraire mais ciblé) ne permet pas de réduire les sources de variabilité de la représentativité de la population cible. La sélectivité des acteurs clefs atténue, toutefois, ces limites de sorte à généraliser les résultats. La prévention de la victimisation à l'ère du numérique s'impose afin de réduire le développement insidieux de la cybercriminalité. Une série de bonnes pratiques doit être adoptée par les usagers du numérique. La priorité doit être de prévenir les préjudices plutôt que d'éviter les risques. Une certaine exposition aux risques est bonne pour la résilience.

Références bibliographiques

Aebi F. & Linde. A. (2020). La criminologie comparée à l'heure de la société numérique : Les théories traditionnelles peuvent-elles expliquer les tendances de la cyber-délinquance ? Revue internationale de criminologie et de police technique et scientifique

Aebi, M. F. & Caneppele, S., (2019). Baisse de la criminalité ou échec des enregistrements policiers ? Sur le lien entre la diminution de la criminalité hors ligne et l'augmentation des crimes en ligne et hybrides. Policing : A Journal of Policy and Practice, 13(1), 66-79 Agence National des Systèmes de Sécurité de l'Informatique (2024). Rapport d'activité.

Anon N., (2014). La pratique de la cybercriminalité en milieux scolaire et universitaire de Côte d'Ivoire. Cas des élèves et étudiants du district d'Abidjan. European Scientific Journal, ESJ, 10(31). https://doi.org/10.19044/esj.2014.v10n31p%p, consulté le 10 juillet 2025.

Baumard (2014) La cybercriminalité comportementale : historique et régulation. RFCDP N°3.

Bogui, J.J. (2010). La cybercriminalité, menace pour le développement : les escroqueries internet en Côte d'Ivoire. Afrique contemporaine, n°234, 155-167.

Côté A-M, (2014). La victimisation en milieu scolaire : une analyse des facteurs individuels, contextuels et environnementaux. Mémoire présenté à la Faculté des études supérieures en vue de l'obtention de M.Sc. en criminologie. Canada.

Cissé, A. (2011). Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorités de recherche. Centre de recherche pour le développement international.

Ettien F-S. A. (2022). Les brouteurs d'Abidjan, RESET [En ligne], 11 |, consulté le 24 septembre 2025. URL : http://journals.openedition.org/reset/4038 ; DOI : https://doi.org/10.4000/reset.4038

De Certeau, Michel. 1990. L'invention du quotidien. 1. Arts de faire. Éditions Gallimard. Folio essais. Paris. 349 p.

Dufour, & al. (2019). La prévention de l'utilisation problématique d'internet : exploration du point de vue des jeunes. Revue québécoise de psychologie, 40(2).

Guarnieri F. & Przyswa E. (2012). Cyber criminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières. Revue Cognition, communication, politique 63 (2).

Michael J. Ghernaouti-Hélie Solange & Dufour Arnaud, (2012). Cybercriminalité et cybersécurité. Dans : Solange Ghernaouti-Hélie (D) éd., Internet (pp. 94-108). Paris cedex 14 : PUF.

Gonzales, C. & Dechanet, J. (2015). L'essor du numérique en Afrique de l'Ouest : Entre opportunités économiques et cybermenaces. Les notes stratégiques.

Gueu, D. (2013). La cybercriminalité à Abidjan, un phénomène de mode ou une nouvelle guerre contre les finances en Côte d'Ivoire ? European sicentific journal, vol. 9 (1), 93-106.

Granjon, F. & Denouël, J. (2011). Penser les usages sociaux des technologies numériques d'information. Communiquer à l'ère numérique. Regards croisés sur la sociologie des usages, collection Sciences Sociales et de communication. Paris : Presses des Mines.

Handelang M. J., Michael R. Gottfredson & Garofalo J. (1978). Les victimes d'actes criminels personnels : fondement empirique d'une théorie de la victimisation personnelle. Éditeur Société d'édition Ballinger, Code ISBN 0884107930, 9780884107934

Kahneman D. & Tversky A. (1979). Théorie des perspectives : une analyse de la décision sous risque. Econometrica : mars, volume 47, numéro 2. https://www.jstor.org/stable/1914185 p. 263 à 292. Consulté le 10 juillet 2025.

Maslow A. (1954). Motivation et personnalité. Genre : Psychologie.

Koffi H. B. I. (2022), Révolution numérique et lutte contre la cybercriminalité en Côte d'Ivoire, revue Échanges, n° 18, juin 2022.

Latzko-Toth, G., et Proulx S. (2015). Appropriation des technologies. Sciences, technologies et sociétés de A à Z, édité par Frédéric Bouchard et al., Presses de l'Université de Montréal, 2015, https://doi.org/10.4000/books.pum.4256.

Pauwels, L., & Svensson,14 : (2011). Explorer la relation entre la délinquance et la victimisation : quel est le rôle des modes de vie à risque et du manque de maîtrise de soi ? Un test dans deux échantillons urbains, European Journal of Criminal Policy & research.

Plantard, Le Boucher C., Perret D., (2020), Les enseignants et le numérique : modèles pédagogiques vs modèles d'appropriation des technologies numériques ? in Bulletin de Veille n°1.

Plateforme de Lutte contre la Cybercriminalité. (2015). Rapport d'activité.

REPC (2019). Boîte à outils du REPC N°15 Prévenir la victimisation des mineurs à l'ère du numérique : sensibilisation et changement de comportement. Bruxelles.

Schlanger, S. & al. (2015). Enjeux et difficultés de la lutte contre la cybercriminalité. Rapport du Groupe de diagnostic stratégique n°6 - 26e Session nationale « Sécurité et Justice ».

Tano-Bian J-A., (2015), La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'Ouest. Droit. Thèse de Doctorat, Université Sorbonne Paris Cité, Français. ffNNT : 2015USPCB067ff. fftel-01249586f.

Veh G. A. L. (2017). La fraude sur le porte-monnaie électronique en Côte d'Ivoire. Revue Africaine de Criminologie. N° 21 décembre 2017 ISSN 1819-0650.

Veh G. A. L. (2019) La cyberescroquerie à Abidjan. Thèse unique en Criminologie-Non publiée. Abidjan : Université Félix Houphouët-Boigny.