L'escroquerie sentimentale sur Internet et les réseaux sociaux

La menace et son organisation par les réseaux criminels

Daniel GUINIER

Docteur ès Sciences, CISSP Emeritus
Expert de justice honoraire
Ancien expert en cybercriminalité et crimes financiers devant la Cour pénale internationale de La Haye

L'escroquerie sentimentale[1] représente une cybermenace en forte croissance. Elle vise à établir une relation virtuelle avec la victime au travers d'interactions en ligne, généralement via les sites de rencontres sur l'Internet et les réseaux sociaux. Bien qu'elle cible des personnes vulnérables, elle affecte un large public, surtout dans les pays occidentaux. Les victimes, croyant avoir trouvé l'amour, se retrouvent dans des situations souvent délicates, parfois désastreuses. L'article en explore l'environnement du phénomène et ses conséquences.

Introduction

Les motifs d'escroquerie ont toujours trait à l'extorsion de sommes d'argent, comme c'est le cas des rançongiciels depuis plus de 45 ans, où il n'est nullement question de sentiments…

"AIDS" est considéré comme le premier rançongiciel de l'histoire, et son auteur, le Dr J. Popp *"le père du ransomware"*. Apparu fin 1989, il se distingue des variantes modernes par le mode de déploiement, sous la forme d'environ 26 000 disquettes expédiées par courrier postal depuis Londres, et de paiement des 189 $ pour une licence d'un an, ou 378 $ pour un accès à vie, à une boîte postale au Panama. Bien que Popp ait été rapidement arrêté, il n'a jamais purgé de peine du seul fait que les disquettes ont été expédiées depuis le Royaume-Uni, qui ne disposait pas de lois à cet égard à l'époque. Aujourd'hui, les variantes modernes sont sans commune mesure. Elles exploitent les vulnérabilités des systèmes en réseaux et la valeur médiane des

[1] Encore qualifiée d'escroquerie romantique ou amoureuse, ou en Anglais de *"online romance fraud (ORF).*

demandes mondiales est établie à 2 millions de dollars en 2023[2]. Ce qui change aussi c'est le mode de paiement par cryptomonnaie[3], et le concept de *"Ransomware-as-a-Service"[4],* permettant à quiconque de se livrer à une telle activité criminelle simplement en louant les outils nécessaires trouvés sur un *darknet* en versant des droits d'affiliés à leurs créateurs.

C'est aussi le cas de l'escroquerie appelée *"fraude nigériane"* qui se fonde sur une sollicitation par courriel, à l'origine en provenance du Nigéria. La démarche exploite le degré d'appétence de la victime pour l'argent. Elle se présente comme une proposition d'affaires urgente strictement confidentielle. L'escroc explique qu'il possède une somme importante et son besoin de la transférer rapidement vers un compte à l'étranger, évoquant divers prétextes, en échange de quoi il offre un pourcentage de la somme. Si la victime accepte le transfert sur son compte, elle devra cependant avancer des frais de notaires ou autres, avant que la transaction soit effective. Evidemment, cette dernière opération ne sera jamais réalisée.

Des variantes sont observées concernant des placements financiers prometteurs, où les escrocs se présentent souvent comme des entreprises légitimes ou des consultants. L'opportunité est vérifiable dans les premiers versements de façon à inciter la victime à prendre plus de risque. Lorsque la somme versée est devenue suffisamment conséquente, ou après qu'un nombre suffisant de victimes aient investi, les escrocs disparaissent naturellement avec les fonds puisqu'ils ont la main sur le compte d'investissement. Aujourd'hui, l'Autorité des marchés financiers (AMF) rend attentif à ce que l'intermédiaire des transactions avec les cryptomonnaies doit obligatoirement figurer sur la liste des prestataires de services sur actifs numériques (PSAN) après un agrément opérationnel, étant donné les litiges fréquents, les escroqueries diverses et la fragilité des portefeuilles virtuels *("wallets").*

Concernant le lien entre l'extorsion et les sentiments relatifs à des personnes dépourvues ou atteintes de maladies graves, il faut citer les demandes relatives aux fausses chaînes de solidarité[5] avec des courriels adressés collectivement en masse, bien avant les sollicitations plus personnelles sur un besoin pressant d'argent ou l'escroquerie sentimentale que nous allons maintenant détailler.

L'escroquerie sentimentale à son tour relève d'un phénomène inquiétant qui connait une forte augmentation[6] à l'ère cyber. Depuis plusieurs années, des milliers de Français en ont été les victimes[7]. En Côte d'Ivoire, elle fait une partie intégrante du tissu économique local et vise essentiellement des personnes francophones en Europe et en Amérique du Nord.

Cette forme d'escroquerie exploite les vulnérabilités psychologiques des victimes en manipulant leurs émotions profondes pour extorquer des sommes importantes. Contrairement à la fraude voisine aux frais anticipés qui se base juste sur des demandes d'argent pour des frais supposés nécessaires à la réalisation de projets ou à la libération de fonds, l'escroquerie sentimentale utilise les émotions en établissant des relations amoureuses fictives sur des sites de rencontre en ligne. Ces arnaques sont d'autant plus complexes qu'elles reposent sur

[2] Source : Livre blanc Sophos sur L'état des ransomwares, avril 2024.

[3] Voir D. Guinier (2014) concernant les monnaies virtuelles, et les liens en rapport à la cybercriminalité et au blanchiment.

[4] Tels que LockBit 3.0, Blackcat, Hive, etc.

[5] Que nous avions décrites en 1997 dans les Dernières Nouvelles d'Alsace, n° 215, 4 sept. : *Politique, rubrique Opinions,* p. 2.

[6] En 2023, la plateforme *Cybermalveillance.com* a connu une augmentation de 91% des demandes d'assistance, avec 1 200 contacts de victimes, contre 600 en 2022, allant en deçà de la réalité, puisqu'il est estimé que seulement 10 % des cas sont signalés.

[7] Selon McAfee, un Français sur deux aurait cherché l'amour en ligne et 65 % des personnes interrogées disent avoir été ensuite contactées par des inconnus avec, dans la moitié des cas, des demandes d'argent.

une ingénierie sociale sophistiquée et que les réseaux criminels qui les orchestrent sont organisés au niveau international, rendant leur identification et leur poursuite particulièrement ardues.

Vocabulaire autour de l'escroquerie sentimentale

Le terme *"scammer",* ou escroc, désigne de façon générale une personne qui trompe quelqu'un en opérant sur l'Internet et sur les réseaux sociaux, dans le but d'obtenir de l'argent ou des informations de manière malhonnête. La dénomination *"brouteur", issue* du Français de Côte d'Ivoire, est souvent employée en référence au mouton, qui se nourrit sans effort. Les *"brouteurs"* se trouvent essentiellement en Côte d'Ivoire, au Bénin, au Cameroun, au Ghana, et au Nigeria, où ils sont dénommés *"Yahoo Boys"*. Ils se qualifient parfois entre eux de *"barasseurs"*, utilisant l'expression *"bara"*, qui se traduit par travail en Nouchi, pour s'appliquer à l'arnaque d'un *"client"*.

Les *"scammers"* africains utilisent souvent le terme *"mugu"* pour désigner leurs victimes, lequel vient d'un jargon nigérian qui signifie littéralement *"idiot"* ou *"dupe"*. Il est utilisé de manière péjorative pour désigner une personne naïve ou facile à manipuler, qui peut être exploitée financièrement ou émotionnellement. Ceci reflète le mépris qu'ont les escrocs pour leurs victimes, qu'ils considèrent comme de simples sources de profit.

Stratégies et techniques de l'escroquerie sentimentale

Les arnaques sentimentales s'appuient sur l'établissement d'une relation émotionnelle forte entre l'escroc et la victime. L'escroc, souvent sur des plateformes de rencontre, crée un profil fictif qu'il met régulièrement à jour pour maintenir la séduction. En se présentant comme un partenaire attentionné et prêt à engager une véritable relation amoureuse, il exploite les émotions de la victime pour la rendre dépendante. Une fois cette relation établie, il demande de l'argent sous divers prétextes *(frais médicaux, urgences, problèmes personnels)*, de manière de plus en plus pressante. Dès lors que la victime réalise qu'elle a été manipulée et comprend que la situation est une duperie, elle cesse d'envoyer de l'argent. La victime, d'abord choquée puis honteuse, hésite souvent à signaler le problème et à déposer une plainte auprès des autorités.

Les escrocs de base, appelés *"brouteurs"*, manipulent psychologiquement leurs victimes en commençant par des demandes modestes pour instaurer une relation de confiance, avant d'augmenter progressivement les sommes demandées sous des prétextes urgents. Ceux situés en Afrique se sont dirigés vers les systèmes de paiement en ligne et les cryptomonnaies, où il est facile de recevoir de l'argent des victimes sans avoir à justifier de son identité réelle et de la provenance des fonds, après que les contrôles de sécurité ont été renforcés par les banques et les organismes de transferts financiers internationaux[8].

Cette relation est purement virtuelle et aucun contact physique n'a lieu. Souvent issus de pays où la cybercriminalité est perçue comme un moyen de survie économique, les escrocs exploitent des émotions humaines, comme la solidarité et l'empathie, pour convaincre leurs victimes de l'urgence de la situation, leur faisant croire que cet argent est absolument nécessaire, voire vital.

L'ingénierie sociale est au cœur de l'escroquerie, reposant sur une manipulation subtile étendue sur plusieurs mois. Les escrocs utilisent des émotions puissantes, telles que l'espoir, l'amour et la culpabilité, pour influencer la victime. Ils créent des récits émotionnels personnalisés, adaptés aux vulnérabilités de chaque cible, afin de

[88] Les victimes rapportent qu'ils ont envoyé plus d'argent en utilisant des virements bancaires et des cryptomonnaies que par tout autre moyen, dans plus de 60 % des cas, contre 24 % de recours aux cartes-cadeaux.

renforcer leur lien affectif. Ces échanges réguliers, souvent accompagnés de promesses d'amour ou de soutien, nourrissent la confiance et l'attachement, ce qui rend les victimes, souvent isolées ou en quête de relations, particulièrement vulnérables.

Les escrocs exploitent également des technologies sophistiquées pour rendre leurs profils et récits plus crédibles. Des logiciels de modification d'images ou de voix sont utilisés pour améliorer l'apparence des profils en ligne et rendre les conversations plus convaincantes. Cette utilisation de la technologie rend l'escroquerie plus difficile à détecter. Parfois, des personnalités publiques sont eux-mêmes dupés, renforçant la crédibilité de l'escroquerie et augmentant la confiance des victimes.

Dans certains cas, les escrocs recourent à la sextorsion. Après avoir convaincu leurs victimes de se dénuder lors de conversations en ligne, ils enregistrent des vidéos ou prennent des photos compromettantes, qu'ils utilisent ensuite pour extorquer de l'argent sous la menace de diffuser ces images. Ce phénomène connaît une forte hausse et touche principalement les jeunes adultes de 18 à 29 ans, avec comme méthode de contact les réseaux sociaux, principalement *Instagram* et *Snapchat*.

Structure et organisation des réseaux criminels

Les auteurs de ce type d'escroquerie sont rarement des individus isolés mais relèvent plutôt de structures sophistiquées, opérant souvent depuis plusieurs pays. Ces réseaux criminels organisés en *"gangs"* fonctionnent comme des entreprises. Des mules financières complètent de façon supervisée le dispositif en servant d'intermédiaires pour transférer les fonds et rendre la traçabilité encore plus complexe. Pour F. K Andoh-Baidoo, *et al*.(2024), l'escroquerie sentimentale depuis l'Afrique est généralement organisée par des *syndicats* criminels composés chacun de 150 à 200 personnes réparties en trois niveaux où les *"brouteurs"* sont supervisés par des cadres qui rendent compte à leur tour à leur supérieur.

Le *"président" (bosu),* au plus haut niveau de la hiérarchie, supervise les opérations et gère des équipes qui peuvent être réparties sur différents continents. Sous son autorité, 10 à 15 *"managers"* sont à la tête de *"cellules"* opérationnelles de 10 à 15 personnes, *en général des jeunes hommes rarement scolarisés et souvent sans emploi âgés entre 15 et 35 ans*, qu'ils recrutent, forment, et coordonnent, en leur fournissant les outils nécessaires, en particulier pour mieux manipuler les victimes, garantir l'anonymat et éviter les traçages par l'usage de technologies avancées pour masquer leur localisation.

Le *"président"* assure aussi la gestion globale du réseau, la répartition des gains, et la supervision d'opérations. Il étaye les stratégies d'escroquerie et veille à ce qu'elles soient correctement mises en œuvre. En outre, il prend les décisions cruciales concernant les grandes lignes et la conduite à tenir en cas de découverte par les autorités, et à une échelle plus large, veille aux relations et liens avec les *"présidents"* d'autres *syndicats*. Il en résulte un système très efficace qui permet de disperser les activités criminelles et rend difficile l'identification et le démantèlement des réseaux. De plus, la connaissance des lois et régulations locales permet de déplacer rapidement les activités entre différentes juridictions pour échapper aux autorités.

La sévérité est d'usage. Un "*brouteur"* qui perd un client précieux ou ne rapporte pas les sommes attendues subit des sanctions pouvant aller d'un avertissement jusqu'à l'expulsion. S'il rencontre des difficultés, il peut cependant demander de l'aide à son *"manager"*. Dans un tel cas, ses gains seront partagés avec ce dernier selon un ratio convenu. D'une façon générale, la distribution des gains est déterminée par le *"président"* en fonction du nombre de participants *"ès-qualités"*.

Les mules financières et le blanchiment

Une mule financière est une personne qui sert d'intermédiaire pour transférer des fonds illicites, à son insu ou contre rémunération. Elle est responsable de recevoir les fonds de victimes et de les transférer via des virements bancaires, des services de transferts de fonds *(ex. Western Union)*, ou des crypto-monnaies *(ex. BitCoin)*. Le rôle des mules financières est essentiel pour dissimuler les traces et compliquer les investigations, mais aussi pour transférer l'argent à d'autres comptes vers des pays de non droit ou non coopératifs.

Toute personne peut être approchée par courriel, sur les réseaux sociaux, ou via des sites de rencontre, avec des arguments séducteurs homologues à ceux de l'escroquerie sentimentale pour la convaincre. Il s'agit d'établir une relation qui l'amène à accepter de participer à une opportunité d'affaires ou à un transfert d'argent soi-disant légitime, sans avoir conscience qu'elle est impliquée dans des activités criminelles, ayant été manipulée pour croire à son rôle dans une cause noble. Dans d'autres cas il s'agit de menace ou de chantage, y compris en la rendant peu susceptible de signaler cette activité aux forces de l'ordre. En effet, bien que certaines mules soient des victimes ou non conscientes du caractère pénal de l'activité, elles peuvent être poursuivies pour blanchiment d'argent ou complicité et recel d'escroquerie, ce qui pourrait conduire à des sanctions pénales. Enfin, des comptes bancaires peuvent être ouverts en usurpant l'identité de tiers, et, ce qui est le comble, celle de la victime elle-même, la rendant ainsi complice involontaire !

Les mules financières jouent un rôle clé. Elles ne sont pas autonomes mais supervisées à plusieurs niveaux pour les transferts de fonds, le blanchiment d'argent et la récupération des profits en apparence légitimes. Elles sont supervisées par des personnes compétentes, les *"superviseurs de mules"* en contact direct avec les *"managers"*. Ceux-ci les coordonnent, en leur fournissant des stratégies de dissimulation des fonds, et en contrôlant les flux financiers de façon à éviter des erreurs pouvant mener à une détection d'activités illégales. Le *"président",* à qui les *"managers"* rendent compte en permanence, dispose d'une vision d'ensemble.

Le blanchiment des fonds résultants de l'escroquerie est essentiel pour rendre l'argent apparemment *"légal"* et difficilement traçable par les autorités. Il pourra être fait appel à des individus spécialistes en manipulation financière ayant connaissance des méthodes pour dissimuler l'origine criminelle de l'argent[9]. Des responsables financiers pourront ensuite être chargés de la gestion des fonds, une fois transformés pour ne pas éveiller les soupçons des autorités. Elles seront alors responsables de la distribution des profits et de la coordination des transferts vers des comptes sécurisés. En les contrôlant de façon centralisée pour en tirer le maximum, le *"président"* est le véritable bénéficiaire des profits maintenant difficilement traçables tirés des activités. Les *"managers",* au sommet de la hiérarchie, bénéficient à leur tour d'une part importante, tandis que celles allouées aux autres participants[10] sont généralement bien inférieures.

L'orientation vers un engagement délinquant et le recrutement

La compréhension de l'orientation s'engager dans la voie de la délinquance est complexe. Le comportement peut pourtant s'expliquer par la jointure de théories criminologiques détaillées dans D. Guinier (2014). Elles mettent en lumière des motivations personnelles, des influences sociales, et le recours à des techniques de justification, mais aussi la rationalisation de leurs actions en niant le risque à la fois pour la victime comme pour

[9] Comptes bancaires dans des paradis fiscaux, recours à des cartes pré-payées, aux crypto-monnaies, achat et vente de biens de luxe, transfert vers des entreprises légitimes en quête de trésorerie, jeux de casinos, etc., voir E. Vernier (2013).
[10] Escrocs de base dénommés *"brouteurs"*, mules financières et leurs superviseurs, blanchisseurs, etc.

eux-mêmes. A leur tour M. Offei, *et al.* (2020), sur la base de telles théories, confirment que le déni du risque opéré par un mécanisme de rationalisation modère la relation entre le déni de la victime, une technique de justification, et l'intention de commettre une escroquerie sentimentale.

Pour favoriser l'enrôlement sous prétexte de les aider à piéger des Européens ou des Américains, considérés d'amblée comme riches, les *"managers"* distribuent des billets de banque dans des soirées en discothèque ou dans des quartiers populaires. En outre, le caractère ostentatoire de la richesse clairement affichée au travers d'objets de luxe par les escrocs, notamment ceux élevés dans la hiérarchie, attire et favorise le recrutement de personnes motivées par l'argent facilement gagné. De plus, des personnes connues peuvent involontairement encourager les escrocs, par leurs propos ou actions. Il en est de même de l'inaction d'autres qui bénéficient du respect ou qui ont de l'influence dans la société. En particulier, plusieurs artistes africains ont abordé le thème général de l'escroquerie sentimentale. C'est le cas en Côte d'Ivoire, d'Alpha Blondy qui traite de fausses promesses d'amour dans ses chansons.

Les cybercafés jouent également un rôle important, d'abord en offrant l'accès à un ordinateur et une connexion Internet stable. Ensuite, le contexte permet aux utilisateurs de se former entre eux en partageant leur expérience et en se prodiguant des conseils, constituant ainsi une pépinière de candidats aptes au recrutement.

Les étapes de l'escroquerie sentimentale

Le processus d'escroquerie sentimentale comporte plusieurs étapes au cours desquelles chaque *"brouteur"* peut demander l'aide de son *"manager"*.

L'étape de repérage de victimes, dénommées *"clients",* est le fait d'un *"brouteur"* en navigant par l'Internet sur les sites de rencontres ou au travers des réseaux sociaux comme *Facebook*, *X*, *Instagram* et *Snapchat*. Pour le contact virtuel il dispose d'éléments de langage propres à la tromperie, d'une connexion en réseau privé virtuel *(VPN)* pour masquer sa localisation, et de quelques outils logiciels de retouches d'images, de synthèse vocale, et parfois d'IA pour la création d' hypertrucages, également appelés "*deepfakes".*

L'étape préparatoire consiste, à la suite du contact virtuel avec une victime, à établir une relation de confiance en la manipulant psychologiquement, en la séduisant ou en la rassurant, afin de la rendre plus vulnérable. L'escroc cherche d'abord à créer un lien émotionnel fort, souvent sous forme de relation amoureuse en ligne, avant de passer à l'acte. Il opère évidemment sous un profil et une adresse électronique créés à cette fin sous une fausse identité, voire une identité usurpée, assortis de photos volées et manipulées. Il use de patience pour ne pas rentrer frontalement sur les sujets d'argent.

L'étape d'extorsion initiale fait référence à des tactiques de manipulation pour demander de l'argent ou des services, en utilisant des mensonges. Cette étape marque une manipulation ou une pression exercée très tôt dans les relations pour soutirer de l'argent ou des ressources à une victime, ou plus généralement en exploitant ses émotions de manière à l'amener à commettre des actions qui servent les intérêts de l'escroc. A ce stade les montants demandés sont modestes et oscillent entre 100 € et 1 000 €. L'application *Taptap Send* permet l'envoi l'argent à partir de la carte de crédit de la victime vers des comptes *Mobile Money* situés en Afrique, sinon *World Remit* à l'étranger en général. Sur la base des informations obtenues subtilement de sa victime, l'escroc peut

par la suite ouvrir des comptes bancaires en usurpant l'identité de celle-ci, laquelle pourrait être incriminée pour recel[11] d'escroquerie … pour avoir encaissé à son insu les sommes d'argent escroquées à d'autres victimes.

L'étape d'escalade débute lorsque l'escroc intensifie la pression de ses demandes à mesure que la victime devient plus impliquée émotionnellement et se retrouve dans une situation où elle se sent obligée de répondre positivement aux demandes de l'escroc. Cela peut inclure des demandes d'argent de plus en plus importantes ou l'utilisation de menaces ou de pressions plus fortes pour obtenir ce qu'il veut. Dans cette étape délicate, l'escroc fera parfois fait appel à son *"manager"*. Il pourra utiliser *ManyCam*, une caméra virtuelle facile à utiliser avec un logiciel de *streaming* en direct pour créer des vidéos professionnelles sur les plateformes de *streaming*. Il pourra créer des profils ou des comptes fictifs, sur des sites de rencontres ou des réseaux sociaux et les gérer pour se faire passer pour des hommes ou des femmes séduisantes trouvés sur l'Internet (*scam girls)*. Pour sa sécurité, il pourra recourir à un réseau privé virtuel *(VPN)*, à l'application *RealTyme* pour organiser et contrôler ses communications, et aux réseaux sociaux alternatifs[12], comme *Telegram*, *Signal*, etc., pour les chiffrer.

L'étape de capture marque un tournant dans la manipulation, où la victime a passé une frontière psychologique. L'escroc est parvenu à s'immiscer dans la vie de sa victime et a réussi à l'amener à un point où elle devient émotionnellement impliquée et commence à se comporter de façon à aligner ses actions sur les objectifs de l'escroc, en l'incitant à envoyer beaucoup plus d'argent, *avec des montants courants de plusieurs dizaines d'euros, pouvant atteindre un total de plusieurs centaines de milliers d'euros*, et à accomplir d'autres actions qui profitent à l'escroc, notamment en s'engageant dans des prêts à la consommation pour disposer d'argent[13], en participant à des escroqueries en ouvrant des comptes et en devenant acteur du blanchiment. A cette étape interviennent les *"brouteurs"*, leur *"manager"*, et le *"président"*, mais aussi les mules financières pour des virements bancaires et les opérations de blanchiment.

L'escroquerie prend fin, dès que la victime a conscience que la situation est une duperie et cesse d'envoyer de l'argent.

Les victimes après la découverte de l'escroquerie

Les victimes, d'abord choquées hésitent à signaler le problème et à déposer plainte. Pour les autorités, il est utile au renseignement criminel. Pour les victimes, il permet de démarrer l'enquête au plus tôt en préservant les preuves, mais aussi de les protéger d'une implication éventuelle dans des actes délictueux qui auraient pu être réalisés, notamment à leur insu. Dans ce cadre, le ministère de l'Intérieur, en collaboration avec Cybermalveillance.gouv.fr, a récemment lancé *"17cyber"*, un guichet unique pour aider les victimes d'infractions numériques. Ce service offre une aide pour comprendre rapidement le type de menace et obtenir des conseils adaptés à la situation. Ce type d'escroquerie représente 7% des plaintes et, comme l'indique la commissaire divisionnaire Cécile Augeraud, *Chef adjoint de l'Office anti-cybercriminalité (OFAC*), *"…le préjudice moyen tel qu'il est établi sur la plateforme Thésée est d'environ 150 000 € pour chacune des victimes"*.

[11] Comme l'escroquerie elle-même, en France, le recel est puni de 5 ans d'emprisonnement et de 375 000 € d'amende (Art. 321-1 du CP), et puni de 10 ans d'emprisonnement et de 750 000 € d'amende, lorsqu'il est commis en bande organisée.
[12] Voir D. Guinler (2024).
[13] *"On a vu des gens se faire liquider des montants de plusieurs dizaines, voire plusieurs centaines de milliers d'euros. Des victimes qui n'avaient pas de gros moyens sont même allées jusqu'à faire des prêts à la consommation ou hypothéquer leur maison pour payer l'escroc"*, (selon les déclarations du directeur de l'expertise pour *Cybermalveillance.gouv.fr*).

Les victimes peuvent éprouver de la colère lorsqu'elles réalisent qu'elles ont été exploitées parfois sur plusieurs mois, ce qui a pu entraîner des conflits familiaux, des pertes de réputation et des conséquences sociales. Au-delà des pertes financières, souvent considérables, elles subissent un choc émotionnel intense, de la honte, de la culpabilité, entraînant parfois des dépressions sévères. L'isolement social, la perte de confiance en soi et les troubles anxieux sont des conséquences courantes. Un profond sentiment de trahison, peut affecter leur perception des relations humaines et leur capacité à faire confiance à autrui à l'avenir. Certains cas extrêmes peuvent mener au suicide, bien que de telles tragédies soient rares.

Cas représentatif 1 *(Source : Libération, 16 mars 2024)* - Une habitante de Torcy (Seine-et-Marne) inscrite sur un site de rencontres a été victime d'une escroquerie sentimentale avec un préjudice financier de 158 000 €. Elle avait entretenu une relation virtuelle de 2019 à 2020 était en fait un escroc. Profitant de l'influence qu'il avait sur elle, il lui avait fait croire que sa fille était gravement malade et qu'il ne pouvait pas payer les frais médicaux. Elle lui a envoyé différentes sommes sur différents comptes dont certains basés en Côte-d'Ivoire, avant de porter plainte. Les investigations ont conduit à l'arrestation d'un ressortissant ivoirien de 33 ans qui a été condamné à 30 mois de prison.

Cas représentatif 2 *(Source : Var-matin, 8 octobre 2024)* - Une habitante de St-Raphaël inscrite sur le site de rencontres *"DisonsDemain"* a été victime d'une escroquerie sentimentale avec un préjudice financier de plus de 150 000 €. Elle a été séduite par *"René Williams"*, un Anglais d'une soixantaine d'années originaire de Manchester, ne parlant pas bien le Français, mais brassant des millions dans le domaine de l'immobilier. Pendant trois mois, elle a versé sans compter l'argent qu'il lui a demandé sous divers prétextes, dont une partie émanait d'un prêt obtenu auprès de son père. Ce n'est qu'après ce laps de temps qu'elle a commencé à avoir des doutes et finalement bloqué un dernier virement de 25 000 €. Aujourd'hui, elle se trouve en grande difficulté et ne parvient pas à rembourser son père, déclarant : *"Je suis dans une panade incroyable (…) Mes amis m'avaient mise en garde, mais je ne voulais pas les croire… En réalité, ce n'était que du pipeau".*

Cas extrême : quand le pire est arrivé *(Source : Le Parisien, 12 mars 2024)* - Le 28 janvier 2024, le cadavre d'une femme était découvert dans le Pas-de-Calais. Après deux mois d'enquête, son compagnon, un homme âgé de 29 ans est mis en examen pour assassinat et placé en détention provisoire. Lors de ses auditions, le suspect Nicolas H. a expliqué avoir prémédité son geste pour concrétiser une relation affective virtuelle qu'il entretenait sur l'Internet, par amour d'une maîtresse qui n'était en réalité qu'un escroc aux sentiments.

La répression de l'escroquerie sentimentale

En France, du fait des manœuvres employées, des poursuites peuvent être engagées des chefs d'escroquerie *(Art. 313-1 du CP),* d'abus frauduleux de l'état d'ignorance ou de la situation de faiblesse (Art. 223-15-2 du CP), de blanchiment *(Art. 324-1 du CP),* et de chantage *(Art. 312-10 du CP)*[14]*.* A ceci, il faudrait y ajouter le délit d'usurpation d'identité *(Art. 226-4-1 du CP)*[15]*.*

Les réseaux d'escroquerie drainent des millions de dollars chaque année, affectant les économies locales et internationales. De nombreux pays manquent de moyens pour traquer efficacement ces réseaux, et le cadre juridique, variable d'un pays à l'autre, complique la coopération internationale et l'extradition des suspects. Les

[14] Les peines encourues sont de 5 ans d'emprisonnement et de 375 000 € d'amende, et doublées lorsque les faits sont commis en bande organisée, sauf en ce qui concerne le chantage qui est puni de 5 ans d'emprisonnement et de 75 000 € d'amende, avec une peine portée à 7 ans d'emprisonnement et à 100 000 € d'amende lorsque le chantage est exercé par un service de communication au public en ligne, ou au moyen ou en vue d'obtenir d'images ou de vidéos à caractère sexuel.

[15] Cette infraction est punie d'un an d'emprisonnement et de 15 000 € d'amende, et des mêmes peines lorsqu'elle est commise sur un réseau de communication.

pressions politiques et diplomatiques des pays occidentaux sur les nations d'où proviennent ces activités et la collaboration sont des éléments moteurs de la lutte contre ces réseaux et de leur démantèlement.

Leur démantèlement est complexe et nécessite des efforts continus et coordonnés sur le plan international. Des progrès significatifs ont été réalisés, malgré le fait que les réseaux criminels évoluent constamment, obligeant les autorités à s'adapter en permanence. Il se déroule en plusieurs étapes. A la suite de dépôts de plainte de victimes ou à des signalements fournis par les banques, les autorités commencent à enquêter en collaboration entre les services des pays concernés pour identifier les acteurs et coordonner leur arrestation, avec l'aide d'Interpol, d'Europol, et du FBI selon que des citoyens américains ou européens sont concernés. Les forces de l'ordre interviennent pour arrêter les suspects, leurs équipements : *ordinateurs, téléphones, cartes SIM, cartes bancaires, etc.*, éventuellement des espèces, et geler les preuves et les fonds liés aux escroqueries. La dissolution des structures financières et le blocage des canaux financiers sont alors requis pour prévenir d'autres escroqueries. A la fin de l'instruction les suspects sont traduits devant la justice.

La Côte d'Ivoire a intensifié ses efforts pour démanteler les réseaux de *"brouteurs"* impliqués dans l'escroquerie sentimentale et d'autres formes de cybercriminalité, à la fois intégrées au tissu économique local et liées à des réseaux internationaux. La collaboration des autorités avec d'autres pays a permis de démanteler des groupes organisés. Les condamnations qui s'en sont suivies montrent l'intention d'éradiquer ce phénomène, malgré des complicités[16]. Il reste cependant difficile à éliminer à cause de son caractère virtuel, de l'insuffisance de moyens techniques et humains, et des méthodes et procédures différentes selon la législation territoriale. A ceci s'ajoute la motivation des escrocs et l'efficacité de la structure des *syndicats* criminels.

Depuis 2018, après diverses interpellations, il est vu des condamnations d'escrocs ivoiriens à des peines allant de 4 à 6 ans d'emprisonnement. L'opération Scorpion menée par Interpol et les autorités ivoiriennes en 2019 a ciblé des réseaux opérant depuis la Côte d'Ivoire et conduit à l'arrestation de 40 suspects, en même temps qu'à une réduction significative de l'activité des *brouteurs* de la région d'Abidjan. En 2020 un réseau d'escrocs opérant en Côte d'Ivoire a été démantelé. Les membres se faisaient passer pour des hommes d'affaires, des militaires ou des diplomates étrangers à la recherche de relations sérieuses. Ils utilisaient des plateformes de rencontre en ligne pour entrer en contact avec leurs victimes, principalement des femmes résidant en Europe et en Amérique du Nord. En 2023, la police ivoirienne a démantelé un réseau composé de 29 brouteurs, essentiellement des migrants, opérant dans le pays. Cette opération a mis en évidence l'implication de migrants dans les activités de *brouteurs* en Côte d'Ivoire, soulignant la dimension transnationale de ces réseaux, opérant en Côte d'Ivoire à cause de l'insécurité et de la pénurie d'électricité dans leur pays d'origine qui représentaient un frein à leurs activités…

Entre avril à juillet 2024, dans le cadre de l'opération *"Jackal III",* Interpol a coordonné une vaste opération visant à lutter contre la criminalité financière en Afrique de l'Ouest, incluant la Côte d'Ivoire. Le démantèlement a conduit à l'arrestation de 300 individus, le blocage de 720 comptes bancaires et la saisie de 3 millions de dollars.

[16] Deux *"brouteurs"* sortis du milieu témoignent de l'existence de complices dans les banques et les forces de l'ordre en Côte d'Ivoire, en précisant : *"Un policier t'arrête, tu as 5 millions de francs CFA sur toi, tu lui en donnes 2, en sachant qu'il ne les gagne même pas en un mois !"* (Étant précisé qu'un million de F CFA représente environ 1500 Euros). Selon eux, d'autres complices se trouvent notamment en France, en Belgique, en Suisse, et au Maroc.

Ces opérations illustrent les efforts continus des autorités ivoiriennes et de leurs partenaires internationaux pour combattre les réseaux de *brouteur*s et protéger les victimes potentielles de ces escroqueries en ligne, et démontrent l'efficacité de la coopération internationale dans la lutte contre les réseaux

Discussion

Les escrocs adaptent en permanence leurs méthodes pour contourner les efforts des autorités. Le recours aux cryptomonnaies et aux transactions anonymes complique considérablement les enquêtes, car les fonds circulent souvent via des plateformes décentralisées, rendant la traçabilité plus complexe. De plus, l'intelligence artificielle (IA) permet la création des profils plus nombreux et plus réalistes, et la réalisation de vidéos et audios falsifiés, sous forme de *"deepfakes"*, rendant la détection des escroqueries encore plus difficile. Ceci invite les autorités à développer des outils puissants, comme des systèmes de détection automatisée aussi basés sur l'IA, pour en contrer la sophistication.

La prévention des escroqueries sentimentales rencontre plusieurs obstacles majeurs. L'un des principaux défis réside dans la difficulté de la coopération internationale, car les réseaux criminels opèrent souvent au-delà des frontières, rendant l'application des lois locales complexe. De plus, la régulation des plateformes de rencontre et des réseaux sociaux reste insuffisante, permettant aux escrocs de se dissimuler derrière l'anonymat en ligne. Enfin, bien que des efforts de sensibilisation soient menés, de nombreuses victimes ne reconnaissent pas les signes avant-coureurs et se retrouvent piégées avant de pouvoir réagir. Les victimes non seulement ne verront jamais l'objet de leurs fantasmes, mais risquent de vider leur compte bancaire, sur cette illusion.

Conclusion et perspective

L'escroquerie sentimentale repose sur des techniques sophistiquées combinant manipulation émotionnelle, technologies avancées et exploitation des désirs humains les plus profonds. Son impact sur les victimes est dévastateur, tant sur le plan financier qu'émotionnel et psychologique.

Pour y faire face, une approche coordonnée à l'échelle internationale, un renforcement de la régulation des espaces numériques et une meilleure éducation du public sont essentiels. De plus, une vigilance accrue sur les plateformes en ligne et un soutien psychologique aux victimes sont également cruciaux.

À l'avenir, il est nécessaire de renforcer la coopération entre autorités, entreprises technologiques et institutions financières pour en améliorer la détection et la prévention. L'IA pourra offrir de nouvelles solutions, mais il est aussi vital de consacrer davantage de ressources à la prévention et à l'éducation, et de renforcer les systèmes de détection sur les réseaux sociaux et les sites de rencontres. Enfin, un soutien ciblé aux victimes, tant financier que psychologique, est indispensable pour les aider à surmonter les traumatismes ainsi causés.

Bibliographie sélective

Andoh-Baidoo F. K., *et al.* (2024) : How do real cybercrime syndicates operate. IEEE Security & Privacy, vol.22, n°4, juillet - août, pp. 124-128.
Fletcher E. (2023) : Romance scammers' favorite lies exposed. Federal Trades Commission (FTC), 9 Février.
Guinier D. (2014) : *"Hackers"* en devenir et en repentir - Quand les talents s'orientent différemment… et sont recrutés. *La Revue du GRASCO*, le Groupe de recherches actions sur la criminalité organisée, *Doctrine Sciences criminelles*, n° 8, février, pp. 36-48.

Guinier D. (2015) : Monnaies virtuelles - Le cas Bitcoin - Risques et rapports à la cybercriminalité et au blanchiment. *Expertises,* n° 400, mars, pp. 96-100.
Guinier D. (2017) : Manipulations et cybercriminalité - La part humaine qui fait de nous des victimes … Bulletin 2017 de la Société des Membres de la Légion d'Honneur (SMLH) - Section dépt. du Bas-Rhin, juillet, pp. 22-26.
Guinier D. (2024) : Les réseaux sociaux alternatifs *"Alt-Techs"* - De la liberté d'expression à l'usage par des groupes extrémistes radicaux et criminels. *Expertises*, n°502, juin, pp. 27-31.
Offei M. *et al.* (2020) : How do individuals justify and rationalize their criminal behaviors in online romance fraud? Inf. Syst. Frontiers, vol. 24, n°2, pp. 1–17.
Vernier E. (2013) : Techniques de blanchiments et moyens de lutte. Dunod, 3ème Ed., 292 pages.