LA TECHNOLOGIE DU SUIVI OCULAIRE À L'ÉPREUVE DE L'ARNAQUE AUX SENTIMENTS DANS LA CYBERSÉCURITÉ

Josselin Wilfred AZI
ajosselinwilfred@gmail.com
Université Félix Houphouët-Boigny (Côte d'Ivoire)
&
Angèle Ouraga ALELEY
angeleouraga@gmail.com
Université Félix Houphouët-Boigny (Côte d'Ivoire)
&
Konan Jean-Yves Guérin YAO
YaoKonanguérin@gmail.com
Université Félix Houphouët-Boigny (Côte d'Ivoire)
&
Mouroufié Paul Bini KOFFI
binikmp@gmail.com
&
Fulgence Guy ZAPKA
fgzapka@gmail.com
Université Félix Houphouët-Boigny (Côte d'Ivoire)

Résumé : Cette étude quantitative a pour objectif de proposer le suivi oculaire comme une technique de lutte contre les arnaques aux sentiments. La technique d'échantillonnage par quotas a permis de sélectionner 40 cybercriminels. Apres expérience, les observations montrent que plusieurs caractéristiques liées au profil numérique, conduisent les cyberescrocs à prendre pour cibles certains internautes. Ce sont : la couleur de peau, la langue parlée, l'âge, le statut matrimonial, l'activité numérique, le mode de vie, les informations personnelles sur le profil de la victime. Les caractéristiques les plus importantes sont liées à la couleur de peau et à la langue parlée. Les conclusions de cette recherche peuvent aider les internautes à assurer leur cybersécurité.
Mots-clés : Broutage – Cybercriminalité – Cybersécurité – Suivi oculaire – Internautes

EYE-TRACKING TECHNOLOGY PROOFS ROMANCE SCAMS IN CYBERSECURITY

Summary : This quantitative study aims to propose eye tracking as a technique to combat sentiment scams. The quota sampling technique made it possible to select 40 cybercriminals. After experience, observations show that several characteristics linked to the digital profile lead cybercrooks to target certain Internet users. These are : skin color, language spoken, age, marital status, digital activity, lifestyle, personal information on the victim's profile. The most important characteristics are related to skin color and spoken language. The findings of this research can help Internet users maintain their cybersecurity.
Keywords : Chatter – Cybercrime – Cybersecurity – Eye tracking – Internet users

I- Introduction : Cadre théorique

L'utilisation des technologies du numérique en Côte d'Ivoire a évolué de manière exponentielle ces dernières années, au point d'avoir acquis une très grande importance pour notre société. En 1970, face à l'évolution de la criminalité, Szabo cité par Yebouet (2015) avait estimé que le phénomène criminel, par les formes qu'il prenait, serait davantage, au 21e siècle, une criminalité astucieuse, non violente, par laquelle les victimes subiraient de lourds préjudices financiers avec peu de dommages physiques. A cette époque, la Côte d'Ivoire devenait une république indépendante jeune de 10 ans et confrontée à une forme de criminalité violente. Selon Touré et Kouamé (1994), cette criminalité violente se composait des vols, d'agressions de personnes sur la voie publique, de coups et blessures volontaires, d'homicides volontaires et de viols. Mais, à la lumière des réalités de notre monde, ces prévisions de la criminalité se sont révélées exactes en 2024 avec la dynamique prégnante du phénomène de la cybercriminalité. Pour corroborer le développement de cette nouvelle forme de criminalité, la Plateforme de Lutte Contre la Cybercriminalité (2021), relève que le nombre de plaintes s'élève à 5000 pour un préjudice financier de 6 milliards FCFA en Côte d'Ivoire. L'insécurité liée à la cybercriminalité qui en résulte est devenue depuis quelques années, un phénomène de société, objet de multiples travaux scientifiques.

En se référant à la loi n°2013-451 relative à la lutte contre la cybercriminalité, la taxonomie des infractions cybercriminelles permet de distinguer d'abord les infractions spécifiques aux technologies de l'information et de la communication (accès frauduleux à un système d'information, le vol d'information, l'introduction frauduleuse de données dans un système). Ensuite, les infractions liées aux technologies de l'information et de la communication (menace en ligne, pornographie infantile, racisme, xénophobie, diffamation et terrorisme sur les réseaux). Enfin, les infractions facilitées par les technologies de l'information et de la communication (escroquerie en ligne, usurpation d'identité, arnaques). Ainsi, s'intéressant aux infractions facilitées par les technologies de l'information et de la communication, notre regard sera porté sur le phénomène de la cyberescroquerie communément appelé « broutage » en Côte d'Ivoire. Selon Akadjé (2011), le broutage est en fait de l'escroquerie via Internet. Une escroquerie qui consiste à soutirer des biens ou de l'argent à des personnes physiques ou morales par des manœuvres frauduleuses. Dans le jargon ivoirien, l'expression brouteur fait référence aux jeunes qui prospèrent grâce au broutage.

L'insécurité produite par le broutage est de nature plurielle. En d'autres termes, elle touche plusieurs secteurs. Les travaux d'Anon (2014) montrent que les auteurs du broutage sont les élèves, étudiants et des chômeurs. Dans la dynamique d'insécurité occasionnée par le broutage, intervient en premier plan l'insécurité numérique, faisant un point d'honneur aux vols et à l'usurpation d'identité. Ballo et Azi (2021) relèvent l'ampleur du vol et l'usurpation d'identité dans le cyberespace. Le vol et l'usurpation d'identité qui ont lieu engendrent chez les internautes un sentiment de cyberinsécurité. Cette insécurité liée au broutage peut être aussi financière. A ce propos, les rapports de la PLCC (2019-2021) sur le préjudice financier sont en effet illustratifs. Par exemple en 2019 le préjudice financier s'élève à 4.919.102.133 FCFA, en 2021 on enregistre un préjudice financier de 6 milliards FCFA. De plus, cette insécurité

financière touche au blanchiment d'argent. Dans ce sens, Akadjé et al. (2019) soulignent que les brouteurs font des investissements dans lesquels ils réinjectent le fruit de leur escroquerie via-internet. Ils blanchissent ainsi des sommes d'argent dans la création d'entreprises de transport, des agences de transfert de fonds et de cybercafés et sont actionnaires dans diverses structures de vente de téléphones. Pour Bollo (2015), cette délinquance à d'importantes répercussions dans le domaine financier et plus précisément sur les institutions financières. La cyberescroquerie favorise donc l'émergence d'une économie criminelle qui infiltre insidieusement le tissu économique.

La cyberescroquerie engendre également une insécurité relative aux droits de l'homme et de l'enfant en Côte d'Ivoire. Cette insécurité se manifeste par des sacrifices humains, des rituels, le prélèvement d'organes humains…L'ordinateur n'est plus l'unique complice des cybercriminels, il y a aussi les marabouts, les féticheurs et autres détenteurs de pouvoirs magiques. Akadjé (2014) soutient que le recours à ces pratiques peut conduire les cyberescrocs à des comportements criminels en vue de faire prospérer leurs activités. Dans le même sens, tout en recadrant les réflexions sous une approche systémique, Nebi et al (2017) affirment que la cyberescroquerie en lien avec les crimes rituels qui à court sur le territoire d'Abidjan participent à l'ampleur du phénomène d'enlèvement des enfants, et d'autres formes de mutilations observées. L'ensemble de ces pratiques menace le droit à l'épanouissement et à la vie.

Ce phénomène menace aussi les fondamentaux d'éducation et les valeurs de notre société. La cyberescroquerie touche à nos valeurs sociales, perturbe nos habitudes de vie et tient à remettre en cause les rapports de la vie en société. Cette insécurité qui en résulte conduit les jeunes se livrer à la prostitution, la consommation d'alcool ou de drogue, des grossesses indésirées sans oublier le nombre d'avortements qui en découle (Bamba, 2013) ; l'homosexualité, le décrochage et les échecs scolaires. Dans l'élan de ces travaux, Karamoko (2015) note que l'intérêt de la philosophie dans l'étude de la cyberescroquerie est de parvenir à une éducation à la culture numérique par la promotion d'une éthique des technologies chez les jeunes au regard de ses distorsions morales.

L'insécurité se rapportant au broutage n'est pas seulement l'apanage des rapports humains et sociétaux. Elle intéresse également la pratique langagière avec son corolaire de faits de langues à l'instar de l'insécurité linguistique. Meike Wernicke (mars 2021), en prélude à une conférence, explique que « l'insécurité linguistique est une impression, une croyance ou un sentiment à l'effet que la variété de langue qu'on utilise ou la façon dont on parle n'est pas légitime ou valorisée par la société. Les gens évaluent généralement leurs propres pratiques linguistiques en les comparant à une norme perçue comme étant supérieure ». Prenant en compte ces spécificités de l'insécurité linguistique, Adjeran (2017), s'intéresse à l'argot des cybercriminels au Bénin. L'étude révèle que leur argot est fait d'un ensemble de pratiques cryptiques et identitaires, dans le cadre du français et du *fɔngbè*, caractérisées essentiellement par un ensemble lexical produit par des procédés de désémantisation et de resémantisation spécifiques. L'argot des cybercriminels est donc à l'origine des formes linguistiques dérivées de la langue commune qui permettent la communication dans un groupe restreint, celui des pairs, et il constitue une réponse linguistique à un besoin, celui de secret, d'opacité. Ces constructions linguistiques représentent une insécurité au regard

des normes et exigences de la langue française enseignée. Le bilan de ces travaux scientifiques montre que la cyberescroquerie est à l'origine de plusieurs formes d'insécurité.

Quelle que soit la nature de l'insécurité, il y a lieu de s'inquiéter de sa persistance. Ainsi, convaincu de l'urgence d'une politique criminelle en la matière, Yebouet (2015) proposait déjà une stratégie de politique criminelle axée sur le renforcement de l'engagement de l'Etat, la mise en place d'une stratégie adaptée basée sur la collaboration des opérateurs de la chaîne internet. Malgré les efforts entrepris, permettant à quelques niveaux la dissuasion et l'arrestation de quelques cybercriminels, il n'en demeure pas moins qu'ils restent bien encore sans effet probant sur l'ampleur du phénomène. La lutte contre la cyberescroquerie connaît des limites importantes qui nécessitent d'autres approches cybersécuritaires. L'inventaire de ces approches permet de voir avec Dupont (2019) que la cybersécurité comprend un large éventail de moyens techniques, politiques ou consister en des pratiques sociales. Cette contribution s'intègre dans les moyens techniques de lutte et pose la problématique de la cybersécurité des internautes face à la cyberescroquerie. Elle répond à la question principale suivante : comment la technique du suivi oculaire peut-elle contribuer à la lutte contre la cyberescroquerie ? Cette contribution est adossée à un paradigme en sociologie des TIC qui convoque ici la théorie des comportements protecteurs développée par Rogers (1975). Cette théorie appliquée à la cybersécurité suggère que les individus prendront des mesures protectrices s'ils perçoivent une menace comme grave et probable, et s'ils croient que des actions spécifiques peuvent réduire ce risque. En lien avec la technique du suivi oculaire, cette théorie offre un cadre d'analyse pour améliorer la sécurité des internautes. L'objectif de cet article est donc de proposer la technique du suivi oculaire dans la lutte contre le broutage. Il importe, pour une meilleure appréhension du sujet, d'apporter quelques précisions à travers une note méthodologique permettant de recentrer les contours de cette étude de criminologie préventive.

II- Méthodologie de la recherche

1- Site et participants à l'enquête

Cette étude s'effectue à Abidjan plus précisément dans la commune de Yopougon. Le choix de cette commune se justifie par le fait qu'elle abrite, en général, de nombreux cybercriminels. La population d'enquête est constituée uniquement de cyberescrocs sélectionnés suivant trois critères. Les critères d'admissibilité étaient 1) être un brouteur ayant 10 ans d'expérience dans la pratique du broutage ; 2) être âgé d'au moins 25 ans et plus ; et 3) avoir déjà arnaqué un montant total supérieur ou égal à 10.000.000 FCFA. Notre expérience[1] de chercheur dans le domaine des TIC et de la cybercriminalité a facilité l'accès aux participants. Par ailleurs, le choix du montant déjà arnaqué a été retenu par simple déclaration des enquêtés. Au travers de la technique d'échantillonnage par quotas, 40 participants (brouteurs) ont été retenus.

[1] Azi Josselin Wilfred est Docteur de Criminologie, chercheur dans le domaine de la cybercriminalité et cybersécurité. L'ensemble de ses travaux universitaires et recherches traitent fondamentalement des questions d'insécurité publique liées aux TIC. Il est auteur et coauteur d'une dizaine d'articles scientifiques sur les manifestations de l'usage des TIC en générale et en particulier sur la cybercriminalité.

2- Exposé expérimental et technique de recueil des données

Nous avons principalement eu recours, dans le cadre de cette recherche à l'expérience du suivi oculaire. Cette technique expérimentale constitue l'ancrage de cette recherche dans la lutte contre la cyberescroquerie. Selon Granka (2004), l'eye tracking en anglais, aussi appelé l'oculométrie ou suivi oculaire désigne les techniques d'étude du regard ou comportement oculaire. Il permet de suivre ce qu'une personne regarde ou observe. Le postulat repose sur une vision de l'objet d'étude qui part du principe selon lequel chaque cyberescroc partage une observation personnelle. Sous cet angle, l'expérience permet de porter une analyse sur les éléments observés en vue d'en dégager les caractères les plus significatifs. La vue est un sens très sollicité, qui déclenche un processus d'acquisition et traitement de l'information. L'œil capte l'image, la transforme en message nerveux à destination du cerveau qui l'interprète. Sur la base de cette interprétation, l'individu ressent des émotions, prend des décisions et effectue des actes. Cette expérience révolutionnaire et scientifique est utilisée dans de nombreux domaines de la science, surtout en psychologie. Dans le domaine de la criminologie, elle est très peu utilisée selon les sources consultées sur internet.

La mise en expérience nécessite un équipement adapté appelé eye tracker. Concrètement, il s'agit d'un testeur ou d'un capteur posé sur la tête des participants (brouteurs) mis face à des sites internet ou des profils de femme ou d'homme. Cet équipement enregistre les mouvements du regard, les caractéristiques des différents profils qui focalisent l'attention. L'expérience du suivi oculaire coûte relativement cher. Or, la difficulté à trouver ou bénéficier d'un financement reste et demeure un frein à la recherche dans les pays en voie de développement. Cependant, en l'absence de cet équipement (eye tracker), l'étude a consisté à une mise en expérience visuelle des participants. Il s'est agi de visualiser différents profils de victimes et de dire avec précision les éléments décisifs dans le choix de la victime. A défaut de capteur et afin de réduire les risques de biais, l'expérience a été répétée. Chaque participant a été soumis 03 fois à l'expérience avec un délai de trois jours d'intervalle entre les observations. Nous disposons d'un ordinateur, d'une connexion internet et de plusieurs profils d'homme et de femme. Le brouteur est isolé dans une salle car selon le test, le participant doit avoir toute son attention sur ce qu'il observe. S'il est distrait, ou s'il interrompt sa tâche, le test est biaisé. Dans ces conditions, le brouteur observe ces profils et nous informe oralement. Chaque expérience est filmée, donnant la possibilité d'être exploitée à des fins d'analyse.

A cette expérience, on associe le questionnaire qui a été conçu afin de répondre aux exigences d'une enquête quantitative. Il a servi à dégager des constantes ou des régularités au sein de l'échantillon d'étude. Il est constitué d'une série de questions qui permet une exploitation aisée et rapide des réponses fournies par les participants. Dans le contexte présent, nous avons fait usage de questions fermées. L'enquête a duré un semestre c'est-à-dire de janvier à juin 2023. Ce questionnaire comprend trois questions principales qui sont :

1) Quels est vôtre d'identité selon ces caractéristiques d'identification ?
2) Sur quelles caractéristiques vous vous fondez dans le choix de la victime ?
3) Pouvez-vous rangez ces caractéristiques par ordre d'importance ?

Cette démarche méthodologique objective une étude expérimentale de la technique du suivi oculaire permettant d'apporter une réponse cybersécuritaire aux arnaques aux sentiments qui sévissent sur les réseaux sociaux numériques.

3- Méthode d'analyse des données

Au regard de la technique de collecte de données utilisée, cette étude fait recours ici à une analyse quantitative. Pour Marchand (2001), l'analyse quantitative a pour objet la description et l'analyse des phénomènes sociaux au moyen de méthodes empruntées à la statistique en les quantifiant afin de déterminer le sens et la force unissant les différentes variables. Ce type d'analyse a été d'une utilité importante dans la mesure où, elle a permis de regrouper les données issues du questionnaire à l'aide de l'outil informatique. Les logiciels informatiques Microsoft Excel 2010 et sphinx ont aidé dans l'analyse et le traitement de ces données. Par l'entremise de ces logiciels, les données collectées ont été transformées en statistiques descriptives. À partir de calculs, de tableaux statistiques, l'objet d'étude a été explicité.

Au terme des précisions méthodologiques, il convient de souligner les conditions sociales de réalisation de cette l'étude. Ainsi, la réalisation de ce travail a fait face à de nombreux obstacles. Les conditions sociales de l'étude seront présentées essentiellement, en 02 types de difficultés. Ce sont les difficultés logistiques et les difficultés liées à la documentation.

La finalisation de cette étude s'est heurtée à d'énormes difficultés matérielles. Dans un premier temps, il fallait équiper la salle d'expérience de caméra afin de filmer à tour de rôle les participants. Dans un second temps, il nous manquait l'équipement destiné à réaliser l'expérience (eye tracker). Dans ce sens, malgré les courriers adressés à certains laboratoires ophtalmologiques, à l'effet de mettre à notre disposition cet équipement, nous n'avons pas obtenu gain de cause. Dans un troisième temps, la mauvaise qualité de la connexion internet due aux intempéries météorologiques (fortes pluies) retardait les différents passages des participants.

La problématique de l'accès aux documents s'est posée avec acuité. Nous avons sillonné certaines bibliothèques dans les facultés de médecine et en science de la communication pour s'approprier des connaissances sur cette technique. Le champ lexical de ces connaissances a été un exercice difficile. Toutefois, ces difficultés ont pu être surmontées et ont permis d'aboutir aux résultats dont les lignes qui suivent présenteront. La structure du présent article résume les grandes analyses issues de l'expérience.

III- RESULTATS

Les résultats de cette étude s'effectuent autour de trois axes. Dans un premier temps, la présentation et l'analyse des caractéristiques socioéconomiques des participants (1), dans un second temps, l'exploitation des données de l'expérience (2) et dans un troisième temps l'élaboration d'une stratégie cybersécuritaire adaptée (3).

1- Présentation et l'analyse des caractéristiques socioéconomiques des participants

La présentation des caractéristiques socioéconomiques des participants selon les éléments d'identification a permis de dégager un profil faisant référence au sexe, à l'âge, au logement, au niveau d'instruction, et à l'activité professionnelle.

Tableau 1: Répartition des participants selon leur sexe, l'âge, le logement, le niveau d' instruction et l'activité professionnelle

Indicateurs	Modalités	Effectifs	Pourcentages
Sexe	Masculin	38	95 %
	Féminin	02	05 %
Total		**40**	**100 %**
Age	25 à 30	21	52,5 %
	30 à 35	13	32,5 %
	35 à 43	06	15 %
Total		**40**	**100 %**
Situation de logement	Vie en famille	05	12,5 %
	Indépendant	25	62,5 %
	Cohabite entre amis	10	25 %
Total		**40**	**100%**
Niveau instruction	Primaire	00	00%
	Secondaire	14	35 %
	Supérieur	26	65 %
Total		**40**	**100 %**
Activité professionnelle	Elève	03	7,5 %
	Etudiant	05	12,5 %
	Sans emploi	20	50 %
	Déscolarisé	12	30 %
Total		**40**	**100 %**

Source : résultat de notre enquête réalisée à l'aide de Microsoft Excel

Ce tableau est représentatif des différents indicateurs d'identification susmentionnés. Ainsi, les participants de sexe masculin représentent 95 % de l'effectif total et ceux du sexe opposé 5 %. Les jeunes qui ont un âge compris entre 25 ans et 30 ans représentent 52,5% de l'effectif total tandis que les jeunes dont l'âge est compris entre 30 ans et 35 ans représentent quant à eux 32,5% et ceux de la dernière catégorie c'est-à-dire ceux dont l'âge est compris entre 35 ans et 43 ans représentent 15 %.

La situation de logement de ces jeunes montre que nombreux sont ceux qui sont independants c'est-à-dire louent une maison. Leur pourcentage est estimé à 60, 5 %. Ceux qui cohabitent entre amis et ceux qui vivent en famille ont des pourcentages respectifs estimé à 25% et 12, 5 %. L'expérience menée, a permis de dégager certaines caractéristiques permettant de décrire plus généralement les auteurs de

cyberescroquerie. Elle en Côte d'Ivoire est l'œuvre majoritairement de jeunes, dont les caractéristiques présentent une certaine hétérogénéité.

2- Exploitation des données de l'expérience

2-1- Présentation et analyse des évocations selon les brouteurs

Les résultats obtenus grâce à l'expérience et au questionnaire, portent sur 40 sujets. A la question : « *Sur quelles caractéristiques vous vous fondez dans le choix de la victime ?* », l'analyse des réponses nous permet de noter 07 évocations citées par les brouteurs. Il s'agit des évocations suivantes : la couleur de peau, la langue parlée, l'âge, le statut matrimonial, l'activité numérique, le mode de vie, les informations personnelles du profil de la victime.

Tableau 2 : Récapitulatif des évocations des brouteurs

Evocations	la couleur de peau	la langue parlée	l'âge	le statut matrimonial	l'activité numérique	le mode de vie	les informations personnelles
Total des réponses selon 40 participants	40	25	39	37	39	34	40
Pourcentage (%)	100 %	62,5 %	97,5 %	92, 50 %	97,5 %	85 %	100 %

Source : résultat de l'expérience réalisée à l'aide de Microsoft Excel

Le tableau 2 ci-dessus présente les évocations des brouteurs à l'issue de l'expérience. L'évocation « couleur de la peau » renvoie à la race. Ici, il s'agit en général d'Homme blanc (masculin ou féminin). 100 % des réponses des brouteurs désignent cette caractéristique. L'analyse qui ressort de cette évocation est justifiée par des croyances collectives chez la plupart des brouteurs. Ces croyances sont structurées autour d'une terre d'abondance européenne où la figure du blanc pauvre est inconcevable ou refoulée. « La langue parlée » est également une caractéristique pour des raisons évidentes de communication. Cette caractéristique cumule un score de 25 réponses soit 62,5 %. Aujourd'hui, les logiciels de traduction et la division des tâches dans les réseaux cybercriminels facilitent la communication. Ce qui justifie le faible score de cette caractéristique. Par la suite, intervient l'âge avec un score de 39 soit 97,5 %. Selon les brouteurs l'âge est un facteur important. Il permet aux brouteurs de présenter à la victime une photo de profil en rapport avec l'âge de la victime. 37 brouteurs soit 92, 50 % des réponses observent le « statut matrimonial ». Cette caractéristique demeure facultative car selon eux, l'on peut rencontrer ou trouver l'amour de sa vie partout. « L'activité numérique » et les « les informations personnelles » sont des caractéristiques recherchées dans le profil des victimes. On observe respectivement 39 et 40 réponses soit 97,5 % et 100 %. Pour les cyberescrocs, il est important que la victime soit active sur internet et les réseaux sociaux. Cette activité numérique montre que la victime existe. Les informations personnelles permettent de mieux connaitre la victime (date d'anniversaire, nombre d'enfants, préférence…). « Le mode de vie »

avec 85 % de réponses permet de découvrir s'il s'agit d'une personne isolée, bien entourée, festive…

2-2- Organisation des évocations par ordre d'importance

A la suite de nos analyses, il a été souligné que 07 évocations ressortaient pendant l'expérience. Il s'agit de : la couleur de peau, la langue parlée, l'âge, le statut matrimonial, l'activité numérique, le mode de vie, les informations personnelles du profil de la victime. (cf. tableau 2). En vue d'évaluer le niveau d'importance de chaque évocation, il a été proposé aux participants de classer les évocations par ordre d'importance. Ainsi, à la question : « *Pouvez-vous rangez ces caractéristiques par ordre d'importance ?* » On obtient le tableau 3 ci-dessous

Tableau 3 : Classement des évocations par ordre d'importance

ordre d'importance	Nb. cit.	Fréq.
Non réponse	1	2,5%
la couleur de peau	18	45,0%
la langue parlée	9	22,5%
l'âge	4	10,0%
le statut matrimonial	4	10,0%
l'activité numérique	2	5,0%
le mode de vie	0	0,0%
les informations personnelles	2	5,0%
TOTAL OBS.	40	100%

Moyenne = 2,26 Ecart-type = 1,65

Source : **résultat de l'expérience réalisée à l'aide du logiciel sphinx**

La question est à réponse unique sur une échelle. Les paramètres sont établis sur une notation de 1 (la couleur de peau) à 7 (les informations personnelles). Les calculs sont effectués sans tenir compte des non-réponses. Selon l'ordre du tableau, les caractéristiques les plus déterminantes sont la couleur de peau et la langue parlée avec des pourcentages respectifs de 45% et 22,5%. Ces caractéristiques prédominantes observées sur le profil de la victime, conduisent les brouteurs à choisir ces personnes pour cibles. Les valeurs rapportées au niveau de la moyenne et l'écart-type sont 2,26 et 1, 65. Ces tendances indiquent que la dispersion des résultats est centrée autour de la moyenne. En d'autres termes, les tendances centrales se situent autour de la couleur de peau et la langue parlée.

Le phénomène du broutage engendre d'énormes coûts, tant pour les structures de lutte que pour l'ensemble des internautes. Le broutage se développe sur les réseaux sociaux numériques. Il serait nécessaire d'organiser des actions de lutte propre à l'univers de ces réseaux numériques.

3- Elaboration d'une stratégie cybersécuritaire adaptée.

Pour Larrieu (2010 : 83) « c'est une chimère de croire qu'on peut tuer la cybercriminalité dans un pays par le contrôle, nous devons créer une société avec des chances égales et un niveau de vie acceptable pour que les jeunes ne voient pas dans l'ordinateur un moyen de se faire de l'argent rapidement ». La diversité des propositions antérieures à cette étude demeure indispensable. Elles se résument d'abord par l'élaboration de loi de plus en plus stricte, ensuite le renforcement des capacités techniques et opérationnelles des acteurs de lutte et enfin la sensibilisation des masses surtout les plus jeunes.

Cette étude propose une stratégie cybersécuritaire adaptée. En effet, l'avantage de l'expérience du suivi oculaire réside dans un procédé de mise en examen du cyberescroc dans le contexte de son activité criminelle. Dès lors, les propositions qui découlent des résultats sont pratiques et prompts à être exécutées par les victimes. Mieux, la victime peut désormais assurer elle-même sa cybersécurité en agissant directement sur ses profils numériques. Au nombre des caractéristiques observées par les cyberescrocs, la couleur de peau, la langue parlée sont les plus déterminants dans le choix de la victime.

La couleur de peau nécessite que le brouteur ait accès à votre photo de profil. Dans ce sens, l'utilisation d'avatar comme photo de profil réduit les chances du brouteur de remarquer votre profil sur les réseaux sociaux numériques. A cette mesure, s'ajoute la sensibilisation à l'endroit des internautes sur la nécessité de publier de moins en moins de photo sur internet. La langue parlée fait appel à un besoin de communication qui ne peut pas être occulté dans nos rapports sur les réseaux sociaux. Toutefois, les cyberescrocs qui participent à l'expérience relèvent qu'il faut être méfiant des profils qui s'expriment dans toutes les langues. Il s'agit le plus souvent des brouteurs. Concernant l'âge, le statut matrimonial, l'activité numérique, le mode de vie et les informations personnelles, il faudrait rendre ces informations confidentielles au public des internautes. Ces mesures pourraient contribuer à lutter contre les arnaques aux sentiments.

IV- Discussion et conclusion

Le domaine de la cybersécurité n'échappe pas au processus de la division du travail qui fait émerger une foule de spécialistes, chacun se concentrant sur un segment du travail visant à produire de la sécurité. Cette loi sociologique est valable dans la lutte contre la cyberescroquerie. De plus en plus, la cybersécurité tend à être transdisciplinaire, donnant l'occasion à des spécialistes de différents domaines d'intervenir. L'étude porte sur le phénomène de l'arnaque aux sentiments. Dans ce sens, l'ensemble des travaux scientifiques participent à la lutte contre ce phénomène. Cette étude s'inscrit dans le même paradigme tout en privilégiant une nouvelle approche cybersécuritaire.

L'expérience du suivi oculaire s'avère être un moyen de lutte parmi tant d'autres proposés par nos prédécesseurs. L'objectif de cet article a été de proposer cette technique dans la lutte contre la cyberescroquerie. L'analyse des caractéristiques socioéconomiques des participants présente une description hétérogène du profil. Selon les participants à l'expérience, plusieurs caractéristiques sont susceptibles d'encadrer le choix de la victime. Ces caractéristiques sont : la couleur de peau, la langue parlée, l'âge, le statut matrimonial, l'activité numérique, le mode de vie, les informations personnelles du profil de la victime. L'expérience montre en outre que les caractéristiques les plus déterminants dans le choix de la victime sont : la couleur de peau et la langue parlée. Cette approche cybersécuritaire en général, donne la possibilité aux internautes de se protéger contre les arnaques aux sentiments en agissant directement sur leur profil. Cette protection passe par l'utilisation des avatars, la publication de moins en moins de photos et la confidentialité des informations personnelles.

Les résultats présentés ne contredisent pas ceux de Yebouet (2015). En réalité, l'auteur montre que la proximité linguistique est un facteur important dans le choix de la victime. Ces résultats sont également en conformités avec les travaux de Koenig (2014) qui précise que sous un angle anthropologique, les africains en général et en particulier les jeunes cyberescrocs ont une représentation idéale de l'homme blanc. Cette perception conduit les brouteurs vers ces derniers. L'âge, le statut matrimonial, l'activité numérique, le mode de vie, les informations personnelles du profil de la victime sont autant de caractéristiques qui n'échappent pas à la vigilance des cyberescrocs. L'ensemble de ces données personnelles a fait l'objet d'étude par Ballo et Azi (2021) qui relèvent la cyberinsécurité relative au vol et à l'usurpation d'identité qui se produisent sur internet. Les résultats de cette contribution semblent pertinents au regard des travaux de ces auteurs précités.

Toutefois, la valeur d'une recherche scientifique est en grande partie dépendante de l'habileté du chercheur à montrer les limites de ses découvertes. Ainsi, des limites d'ordre analytique sont à remarquées. La rareté ou l'indisponibilité des travaux scientifiques sur l'expérience du suivi oculaire dans le domaine de la criminologie. Cette absence de travaux rend moins objective la discussion des résultats. Sur le plan méthodologique, malgré la prudence et les exigences dans la mise en expérience du suivi oculaire afin d'éviter les biais, des limites sont remarquables. D'abord, l'absence du matériel d'expérience (eye tracker). Ensuite, l'expérience ne permet pas une explication rationnelle quant à l'utilisateur qui porte son regard à tel endroit ou à tel autre endroit. Enfin, son utilisation dans les conditions optimales est appuyée d'un test d'utilisabilité. Toutes ces irrégularités méthodologiques sont à considérer dans l'appréciation de ces résultats. *In fine*, au regard des conclusions de cette étude, par rapport à d'autres travaux scientifiques, nous rejoignons la pensée du célèbre moraliste Joseph Joubert (1954) pour qui le but ultime de l'argumentation ou de la discussion ne devrait pas être la victoire, mais plutôt le progrès de la science. Les résultats des analyses et conclusions de cette étude ne sauraient être considérées comme une finalité, mais plutôt comme une base de réflexion sur cette technique de lutte pour adresser sous un angle nouveau, la question de la lutte contre les arnaques aux sentiments.

Références bibliographiques

Akadjé, A. M. & René S. Sahi And Mouli H. (2018). Utilisation du gain issue du broutage à Abidjan. International journal of current Research, 12, 76704- 7613

Akadjé, A. M. (2011). Cybercriminalité et ''broutage'' en Côte d'Ivoire. Revue Internationale de Criminologie et de Police Technique et Scientifique, 3, 299-310.

Akadjé, A. M. (2014). Cybercriminalité et pratiques magiques en Côte d'Ivoire. Revue internationale de recherches et d'études pluridisciplinaires, 1, 64- 78.

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, (10) 31, 178-195

Ballo Y. & Azi J. W., (2021). Cybercriminalité à Abidjan : vol, usurpation d'identité et cyberinsécurité, Revue des sciences du langage et de la communication (Rescilac) – Revue pluridisciplinaire en sciences sociale et humaine, n°14, vol.1, ISSN : 1840-8001, 338- 350.

Bamba, B. (2013). Représentation sociale, pratique de la cybercriminalité et comportements délinquants de la jeunesse à Abidjan. Thèse de Doctorat unique en psychologie option : psychologie sociale et du travail (non publiée). Abidjan : département de psychologie.

Bollo E. F. (2015). Institutions financières et cybercriminalité, Revue d'économie financière, 120, 181-198.

Ditt-plcc (2019 et 2021). Rapport d'activité annuel de la Direction Informatique et des Traces Technologiques- Plateforme de Lutte Contre la Cybercriminalité, Côte d'Ivoire.

Dupont B. (2019). L'écologie de la cybersécurité. In nouveau traité de sécurité intérieure et sécurité urbaine, sous la direction de Maurice Cusson, Olivier Ribaux, Étienne Blais, Michel Max Raynaud. Éditions Hurtubise

Granka, L. (2004).Eye-R: Eye-Tracking analysis of user Behavior in online Search. Masters Thesis, Cornell University Library Press

Joseph Joubert (1954) in les révoltes du Québec, image d'archive sur le site de l'Université du Quebec http://www.université du québec.fr/doc/ahess_0395 26491969 num 4398564

Karamoko, T. (2015). La société digitale et les racines de la cybercriminalité, Revue Ivoirienne de philosophie et de sciences sociales, 9, 1-19

Koenig B. (2014). Les économies occultes du « broutage » des jeunes Abidjanais : une dialectique culturelle du changement générationnel, Presses de Sciences Autrepart, 71,195-215.

Larrieu J. (2010). Droit de l'Internet, Paris, Ed. Ellipse

Marchand A. (2001). L'analyse quantitative des données hiérarchiques avec les modèles multiniveaux. Québec : Presses de l'Université du Québec

Montillot F. et Pernes C., (2002) La Démocratie en danger, Paris, éd. Prat Europa.

Nebi R. B. & Bamba L. & Dolle K. (2017). Cybercriminalité ou Broutage et Crimes Rituels à Abidjan : Logiques des Acteurs et Réponses au Phénomène Cas des Communes de Yopougon et d'Abobo, European Scientific Journal, (13), 23, 178-195.

République de Côte d'Ivoire, Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, JO RCI du 12 août 2013

Rogers, R. W. (1975). Une théorie de la motivation de protection des appels à la peur et du changement d'attitude 1. Le Journal de psychologie, 91 (1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Touré, I .Kouamé G. (1994). La violence urbaine en Côte d'Ivoire : Le cas de la ville d'Abidjan In Urban Violence in Africa. Osaghae, Eghosa E. Olawade Isaac Albert, Touré Ismael, Jinmi Adisa et N'guessan Koumé. Pilot Studies (South Africa, Côte-d'Ivoire, Nigeria). p. 59-108

Yebouet, B. C. P-H, (2015). La politique criminelle ivoirienne en matière de cybercriminalité, Revue Internationale de Criminologie et de Police Technique et Scientifique. Genève, 458-469