L'impact des nouvelles technologies sur les tendances criminelles et les méthodes d'enquête en côte d'ivoire

Gogoué Jean Claude DANHOUE
Maître-Assistant à l'UFR Criminologie
Université Félix HOUPHOUET Boigny, Abidjan Cocody, Côte d'Ivoire
(225) 07 07 60 32 90
danhouejeanclaude@gmail.com
ORCID : 0000-0001-2345-6789
Djagbré Esaïe OKOU
Maître-Assistant à l'UFR Criminologie
Université Félix HOUPHOUET Boigny, Abidjan Cocody, Côte d'Ivoire
Jean Richard TIBE BI
Docteur à l'UFR Criminologie
Université Félix HOUPHOUET Boigny, Abidjan Cocody, Côte d'Ivoire

Résumé

L'étude examine l'impact des nouvelles technologies sur les tendances criminelles et les méthodes d'enquête en Côte d'Ivoire. L'apparition des technologies a engendré de nouvelles formes de criminalité et a facilité la perpétration de crimes traditionnels. Les enquêteurs ont dû adapter les méthodes d'enquête à ces nouvelles technologies pour améliorer leur efficacité dans la traque et l'arrestation des criminels. Néanmoins, il est constaté que les systèmes informatiques sont vulnérables, laissant ainsi prendre de la proportion avec des répercussions significatives sur les individus, les entreprises et la société dans son ensemble. La lutte contre le phénomène nécessite une collaboration entre l'État, les autorités sécuritaires et les entreprises privées de sécurité. L'article recommande une dotation en nouveaux outils informatiques, une formation approfondie et un renforcement des compétences des enquêteurs dans l'utilisation des technologies et des méthodes d'investigation numérique les plus récentes afin de détecter et prévenir les activités criminelles.

Mots-clés : Impact, Nouvelles technologies, Tendances criminelles, Méthodes d'enquête, Criminalité numérique.

Abstract

The study examines the impact of new technologies on criminal trends and investigation methods in Côte d'Ivoire. The emergence of technologies has led to new forms of crime and facilitated the perpetration of traditional crimes. Investigators have had to adapt their investigation methods to these new technologies to improve their effectiveness in tracking and arresting criminals. However, it is noted that computer systems are vulnerable, thus leading to significant repercussions on

individuals, businesses, and society as a whole. Combating this phenomenon requires collaboration between the state, security authorities, and private security companies. The article recommends the provision of new computer tools, thorough training, and strengthening the skills of investigators in the use of the latest technologies and digital investigation methods to detect and prevent criminal activities.

Keywords: Impact- New technologies - Criminal trends- Methods of inquiry - Digital crime.

Introduction

La technologie est définie par Stiegler B [1] comme un ensemble d'outils, de dispositifs et de méthodes utilisés pour recueillir, stocker, traiter, transmettre et échanger des informations. Selon Goodman M[1], l'évolution rapide des technologies de l'information, de la communication et du commerce électronique a eu un impact important sur tous les aspects de notre vie quotidienne, y compris la criminalité et l'application de la loi. En raison du manque de données empiriques disponibles, il est difficile de déterminer l'ampleur des infractions liées aux nouvelles technologies, telles que la fraude, le vol, l'escroquerie, le vol d'identité, la fraude en ligne, le piratage informatique et d'autres délits (Menn J., 2019).

Toutefois, en 2019, une étude réalisée par Organisation des Nations Unies a révélé une augmentation annuelle de plus de 1 000 milliards de dollars des pertes mondiales causées par la criminalité numérique. En effet, pendant la crise du COVID-19, le nombre de cyberattaques est monté à 600%, selon le Centre de Plaintes pour les Crimes sur Internet (IC3) du FBI. Les pertes financières liées aux fraudes en ligne ont dépassé les 4 milliards de dollars en 2020, ce qui représente une augmentation de 69% par rapport à l'année précédente. De plus, les attaques de ransomware ont augmenté de 300% en 2020 par rapport à l'année précédente. Ces chiffres soulignent l'augmentation des crimes cybernétiques et la menace grandissante qu'ils constituent pour les particuliers, les entreprises et les gouvernements dans le monde.

[1]Goodman M. (2015).

Cybercrime Magazine prévoit que les coûts mondiaux des cybercriminals dépasseront les six million de dollars d'ici 2030.

Avant l'arrivée des nouvelles technologies, les enquêteurs utilisaient plusieurs moyens comme l'interrogatoire des suspects, des témoins et des victimes, la collecte d'éléments matériels sur les lieux du crime, la surveillance pour obtenir des preuves matérielles et une résolution efficace des affaires (Enyegue P., 2024) Aujourd'hui, les outils numériques tels que les caméras de surveillance, les drones, les logiciels de reconnaissance faciale et les analyses de données ont considérablement amélioré les pratiques d'enquête (Dufresne D., 2021).

Pour Bogaert O[2], ces outils permettent aux autorités compétentes de collecter rapidement de grandes quantités d'informations, ce qui permet de détecter des tendances, des modèles et des liens entre les différentes entreprises. La collaboration entre les organismes de sécurité est également facilitée par les plateformes numériques qui permettent un échange d'informations en temps réel, très important pour la résolution des crimes.

Concernant l'évaluation de l'efficacité des nouvelles technologies dans les enquêtes policières, le FBI a observé une amélioration significative de l'efficacité des forces de l'ordre. En effet, cela s'est traduit par une hausse du taux de règlement des affaires, une diminution du délai de règlement d'une affaire et une hausse du taux de condamnation des coupables. En utilisant de nouveaux outils de sécurité, certaines municipalités ont enregistré une baisse de 20 % des crimes violents, selon une étude réalisée par le Bureau de la justice statistique des États-Unis. Il n'est donc pas douteux que les nouvelles technologies ont grandement amélioré la précision des éléments de preuve collectés dans le cadre d'enquêtes criminelles, donnant ainsi des résultats fiables (Toubiana V., 2021).

Le FBI a établi que l'utilisation de technologies de pointe par les forces de l'ordre a accru leur efficacité dans la résolution d'affaires, réduit le temps nécessaire pour résoudre une affaire et augmenté le

[2] Bogaert O. (2021, p.123).

taux de condamnation des criminels. En outre, les nouvelles mesures de sécurité ont eu un effet important sur la délinquance, avec une diminution de 20 % des crimes de violence dans certaines villes, selon une étude du Bureau de la justice statistique des États-Unis. Ces nouvelles technologies ont certes amélioré la fiabilité des données de preuve recueillies dans le cadre d'enquêtes criminelles, permettant ainsi d'obtenir des résultats plus précis et fiables à des coûts avantageux recueillis dans le cadre d'enquêtes criminelles. En plus, les enquêteurs utilisant les nouvelles technologies ont toujours respecté les droits des personnes en protégeant la confidentialité des informations recueillies.

Malgré l'efficacité des outils technologiques disponibles pour les enquêtes criminelles, leur utilisation est limitée par des failles qui entravent la résolution des enquêtes et la sécurité publique (Zuboff S.,2022). D'après diverses études menées par des organismes connus tels que l'Association Internationale des Chefs de Police, l'Institut de Recherche sur la Criminalité et la Justice et l'Organisation Internationale de Police Criminelle (Interpol), 70% des organismes de maintien de l'ordre à l'échelle mondiale rencontrent des difficultés en stockage, partage et utilisation des informations relatives aux crimes. On remarque donc que plus de 30% de ces agences ne possèdent pas de bases de données standardisées, ne sensibilisent pas suffisamment leurs agents aux outils technologiques disponibles et n'établissent pas de protocoles efficaces de partage d'information avec d'autres organismes. De nombreux organismes estiment qu'ils ne disposent pas des ressources financières nécessaires pour investir dans ces outils.

Bounaamane B et Zined D. (2023)[3], mettent en évidence que l'incompatibilité des outils informatiques utilisés pour résoudre certaines affaires criminelles a des effets importants et variés. D'un point de vue économique, cette situation entraîne de lourdes pertes pour les particuliers, les entreprises et les gouvernements, liées aux détournements de données et aux cyberattaques. Ce qui se traduit par des frais de réparation élevés et une perte de confiance dans les systèmes numériques. La cybercriminalité peut avoir des

[3] Bounaamane B et Zined. (2023, p.451).

conséquences désastreuses sur la vie sociale des personnes en mettant en péril leur vie privée et en les exposant au vol d'identité et au harcèlement virtuel. L'ensemble de la société peut être affecté par la diffusion illicite de contenus sur internet, tels que la pornographie infantile ou les discours haineux. En favorisant le terrorisme, la cybercriminalité constitue aussi un grave danger pour la sécurité des États.

Selon Grégoire D[4], pour lutter de manière efficace contre les méfaits liés aux avancées technologiques, les nations investissent davantage dans les nouvelles technologies de pointe et forment plus d'enquêteurs dans la détection des infractions liées aux avancées technologiques. En outre, elles s'associent à des spécialistes de la technologie et de la cybercriminalité pour tenter de résoudre ces crimes. Elles établissent également des partenariats constructifs avec des experts en technologie et en cybercriminalité, sensibilisent le public aux dangers de la cybercriminalité et aux bonnes pratiques à suivre, en accord avec les lois actuelles sur la sécurité informatique et la protection des données personnelles (Lachaux J.,2020)

La Côte d'Ivoire, tout comme de nombreux autres États, se trouve confrontée à une montée en puissance des actes délictueux associés aux avancées technologiques. Les autorités étatiques ainsi que leurs collaborateurs dans le secteur de la protection des biens et des personnes s'emploient à mettre en place diverses stratégies afin de contrer cette criminalité persistante (Koffi K.,2021).

L'objet de cette étude est d'analyser l'influence des nouvelles technologies sur les tendances criminelles et les techniques d'enquête. Cette étude met en évidence l'impact considérable des nouvelles technologies sur les comportements des délinquants et les stratégies des enquêteurs ivoiriens. Il convient de mettre en évidence les points forts et les points faibles que ces évolutions entraînent, ainsi que les retombées qu'elles engendrent. Les mesures visant à lutter contre ces nouvelles formes de criminalité sont également examinées.

[4] Grégoire D. (2019).

1. La méthode conceptuelle

La théorie de la cybercriminalité en évolution (Wall, 2024) est abordée dans l'approche théorique.

1.1. Théorie de la cybercriminalité en évolution

La théorie de la cybercriminalité en évolution de (Wall, 2024) est utilisée pour étudier l'impact des nouvelles technologies sur les tendances criminelles et les pratiques d'enquête. Selon cette théorie, la cybercriminalité est un phénomène en mutation constante qui se caractérise par l'utilisation des technologies de l'information et de la communication pour commettre des actes répréhensibles. Les avancées technologiques récentes ont considérablement facilité la commission de ces crimes en offrant aux délinquants de nouveaux outils et moyens pour mener à bien leurs activités illicites. Les méthodes d'investigation utilisées par les autorités pour lutter contre la cybercriminalité ont également été affectées par les avancées technologiques. Les enquêteurs doivent constamment s'adapter aux nouvelles technologies pour suivre les traces numériques laissées par les criminels. La doctrine sur la cybercriminalité souligne l'urgence d'une coopération entre les forces de l'ordre, les entreprises privées et les organisations internationales. Cette collaboration s'avère cruciale dans le partage d'informations et de ressources pour une meilleure prévention et répression de la cybercriminalité. Les tendances suspectes dans ce secteur évoluent rapidement, ce qui nécessite une vigilance permanente de la part des autorités et des entreprises pour prévenir et faire face aux nouvelles menaces. Il est crucial de se tenir informé des dernières tendances et techniques utilisées par les cybercriminels pour mieux les combattre.

En somme, la théorie de la cybercriminalité souligne l'importance de saisir et d'analyser l'impact des avancées technologiques sur les tendances criminelles et les méthodes d'investigation, afin de mieux lutter contre ce phénomène en constante évolution.

2. L’approche méthodologique

2.1. Terrain d’étude et participants

La ville d’Abidjan a été choisie comme lieu d'étude pour évaluer L’influence des progrès technologiques sur les activités délictueuses et les pratiques d'enquête. L'arrivée des smartphones, des réseaux sociaux et des systèmes de surveillance ont considérablement modifié les plans d'action des malfaiteurs travaillant à Abidjan pour préparer leurs actes et se soustraire aux autorités. Les autorités ivoiriennes ont également eu recours aux nouvelles technologies pour lutter contre la criminalité. Des recherches approfondies sont nécessaires pour comprendre l'influence des nouvelles technologies sur la délinquance et les méthodes d'enquête, afin d'améliorer la prévention et la sanction des crimes. Pendant trois mois, une enquête a été menée auprès d'un échantillon diversifié de la population d’Abidjan.

Cette population est constituée des forces de l'ordre telles que la Police et la Gendarmerie Nationale, qui ont pour mission de surveiller et d'analyser les nouvelles technologies utilisées par les criminels pour commettre des cybercrimes, afin de pouvoir lutter efficacement contre ces derniers. Elle inclut aussi des experts des Directions de l'Informatique et des Traces Technologiques (DITT), qui sont chargés d'analyser les nouvelles technologies employées par les criminels pour perpétrer des délits, dans le but de concevoir des outils et des méthodes d'investigation adaptés à ces nouvelles formes de criminalité. En outre, des agents de la Plateforme de Lutte Contre la Cybercriminalité (PLCC) participent à cette étude, jouant un rôle crucial dans la prévention et la répression des infractions en ligne. Leur mission consiste à surveiller les évolutions technologiques et à élaborer des stratégies d'investigation appropriées pour lutter contre la cybercriminalité. Il y a aussi, des agents de l'Unité de l’Industrie et de la Technologie (UIT) sont investis de la mission de surveiller l'évolution des technologies et de formuler des recommandations en vue de renforcer la lutte contre la criminalité en ligne et d'améliorer les dispositions d'enquêtes des forces de l'ordre. De même, les agents de l'Autorité de Régulation des Télécommunications/TIC de Côte d’Ivoire (ARTCI) s'emploient à renforcer la sécurité des réseaux de télécommunications. Les cybercriminels, quant à eux, fournissent des

informations précieuses sur les nouvelles menaces, contribuant ainsi à améliorer la sécurité des systèmes informatiques. Enfin, les victimes jouent un rôle crucial en partageant des informations essentielles sur les méthodes employées par les criminels pour commettre des infractions, ainsi que sur les conséquences de ces actes sur leur vie.

L'échantillonnage stratifié est la méthode la plus appropriée pour l'étude en question. Cette approche consiste à segmenter la population en sous-groupes homogènes selon des critères pertinents tels que la nature des crimes commis ou le degré technologie utilisé. Ensuite, les échantillons sont prélevés de manière aléatoire au sein de chaque sous-groupe pour assurer une représentation adéquate de la diversité des activités criminelles et des techniques d'enquête. Cette méthode a fourni des informations plus précises et pertinentes pour étudier l'influence des nouvelles technologies dans ces secteurs particuliers. Par conséquent, 250 personnes ont été choisies avec soin pour cette étude.

2.2. Techniques de recueil de données

Nous avons utilisé l'approche mixte, alliant la méthode quantitative à celle qualitative pour saisir le fait étudié. L'approche comprend la recherche documentaire et les enquêtes de terrain. Dans la recherche documentaire, nous avons consulté des études déjà menées sur la problématique à l'étude. L'examen de documents tels que les rapports de police, les études académiques, les articles de presse et les rapports gouvernementaux a permis d'obtenir des informations sur les tendances en matière de criminalité et d'enquêtes liées aux progrès technologiques. Nous avons aussi mené des entretiens avec des spécialistes éminents de la criminalistique, de la police scientifique, de la cybercriminalité et de la sécurité informatique. Cette démarche nous a permis d'obtenir des informations précieuses quant aux progrès technologiques et à leur incidence sur les activités délictueuses.

Au niveau des enquêtes de terrain, une 'observation directe des activités criminelles et des méthodes d'enquête ont permis d'acquérir des informations précieuses sur la façon dont les progrès technologiques sont exploités dans le cadre de ces activités. Un examen des données chiffrées, telles que les données de communication électronique, de localisation et financières, a été élaboré permettant de mettre en lumière des schémas et des tendances

associés aux activités délictueuses et aux méthodes d'enquête. Nous avons, par ailleurs, fait l'étude de cas particuliers, tels que les affaires de cybercriminalité ou d'investigation numérique, afin d'appréhender de manière approfondie l'incidence des progrès technologiques sur ces domaines d'activité.

Un questionnaire a été adressé aux différents enquêtés, ce qui également a contribué à l'appréhension des modalités d'utilisation des nouvelles technologies par les criminels en vue de perpétrer des infractions, ainsi qu'à la manière dont les enquêteurs exploitent ces outils numériques pour résoudre les affaires.

3. Méthodes d'analyse des données

Cette démarche a intégré l'emploi de méthodes quantitatives afin d'analyser les données relatives aux infractions commises et aux technologies employées, ainsi que des méthodes qualitatives en vue de saisir les motivations des délinquants et les obstacles auxquels les enquêteurs sont confrontés.

4. Résultats

4.1. Analyse des nouvelles technologies et tendances criminelles

Pour Jean-Meire[5], l'avancée technologique a eu de l'influence sur la société humaine. Cette évolution a facilité la vie quotidienne, rapproché les gens du monde entier et devenu un outil incontournable pour l'enseignement et la diffusion de l'information. Néanmoins, il est important de noter que l'utilisation d'ordinateurs a également causé des problèmes de délinquance.

En Côte d'Ivoire, certains délinquants utilisent les nouvelles technologies pour commettre des crimes, en particulier dans la capitale, Abidjan. Les techniques les plus courantes sont le Phishing, qui implique l'envoi de messages trompeurs pour obtenir des données personnelles, et le Vishing, une fraude virtuelle où les cybercriminels dérobent des informations personnelles ou financières en se faisant passer pour des organismes légitimes comme des banques, des sociétés de cartes de crédit ou des organismes gouvernementaux.

[5] Jean-Meire C. (2016).

Dans le même ordre que ces différentes techniques, il faut parler aussi du Ransomware, une technique utilisée par des cybercriminels pour infecter les ordinateurs de leurs victimes avec des logiciels malveillants. Il s'agit de chiffrer les fichiers des utilisateurs afin d'obtenir une rançon en échange de la clé de déchiffrement. Les individus ont eu recours à des logiciels de manipulation d'images pour altérer des documents officiels tels que des cartes d'identité, des passeports ou des actes de naissance, dans le but d'obtenir divers avantages, tels que des emplois, des prestations sociales ou des droits de vote. Un enquêté a ainsi affirmé : « Depuis l'apparition de ces logiciels, il m'est plus facile de faire des bénéfices importants, car on peut manipuler les autres et leur imposer des sommes d'argent sans craindre d'être arrêté par la police ».

Un autre répondant enchéri en ces mots : « Avec le Web, de nouveaux crimes ont émergé, à côté des crimes déjà existants qui ont aussi augmenté. Tout est possible aujourd'hui avec une connexion et un ordinateur ».

Le piratage informatique est une pratique malveillante qui s'infiltre dans les bases de données des institutions publiques pour manipuler les informations relatives à la nationalité, les documents administratifs, les données personnelles et financières de leurs victimes. Les données sensibles telles que les numéros de cartes bancaires, les mots de passe et les données de géolocalisation peuvent être utilisées par ces individus, ce qui leur permet de falsifier des documents officiels et de contourner les dispositifs de sécurité. En outre, ils utilisent les médias sociaux pour détecter, suivre et préparer leurs attaques contre leurs cibles, et diffusent de fausses informations pour les insérer.

Les chiffres de la PLCC, de l'UIT, de la police nationale, de la gendarmerie nationale, de l'ARTCI et de la DITT révèlent la criminalité liée aux nouvelles technologies dans le pays et notamment dans la ville d'Abidjan.

En 2021, la PLCC a enregistré 840 infractions liées à la cybercriminalité, dont 181 cas d'abus de confiance et 659 cas de falsification et d'utilisation frauduleuse de cartes bancaires. La même année, on a recensé 753 cas de contrefaçon, 115 cas de fraude à la nationalité et 203 passeports falsifiés.

En 2022, 550 incidents d'abus sexuels sur Internet ont été signalés, dont près de 78% concernent la publication ou la possession d'images pornographiques représentant des enfants. Le rapport de la DITT de 2022 a recensé 753 cas de contrefaçon, 115 cas de fraude liée à la nationalité et 203 cas de fraude sur les passeports.

Au cours de la même année, 241 infractions ont été signalées concernant les systèmes de traitement automatisé de données, dont la plupart ont été causées par des accès frauduleux impliquant des altérations, des suppressions ou des modifications de données. Les autorités compétentes ont signalé 972 cas de violation des droits individuels en matière de collecte, de traitement non autorisé, de divulgation, de conservation ou de détournement de données personnelles, ainsi que 671 cas de violation des fichiers, des libertés et des correspondances électroniques.

Des écoutes téléphoniques sur les victimes ont signalé des actes de vol à main armée entre 2022 et 2023. 45 cas de ce type ont été identifiés par les forces de l'ordre national et la gendarmerie, ce qui a coûté des sommes considérables.

En 2023, l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) a recensé 723 cas d'atteinte à la dignité et à la personnalité, comprenant des actes d'injure publique et de diffamation injustifiée envers des individus, ainsi que 396 cas de provocation à la haine ou à la discrimination. Par ailleurs, 109 injures ont été recensées en raison des opinions politiques des victimes. Selon la Plateforme de Lutte Contre la Cybercriminalité (PLCC) et la Direction des Technologies de l'Information et de la Communication (DIT), les pertes financières liées aux fraudes en ligne ont causé 3,3 milliards de francs CFA en Côte d'Ivoire.

4.1.1. Étude des pratiques d'enquête en rapport avec les nouvelles technologies.

Pour Rees M.[6], les progrès technologiques dans le domaine de l'enquête ont facilité la collecte, l'analyse et la conduite d'enquêtes de manière plus efficace et rapide.

En Côte d'Ivoire, la loi N° 2013-451 du 19 Juin 2013 vise à lutter contre la criminalité liée aux nouvelles technologies en mettant à

[6] Rees M. (2020).

disposition des autorités des outils numériques pour mener des enquêtes criminelles. Parmi ces outils figurent les systèmes de reconnaissance faciale et de géolocalisation, qui permettent de détecter les criminels en cavale et de suivre les mouvements des suspects.

Les autorités utilisent divers outils numériques, tels que l'analyse des données téléphoniques, pour repérer les mouvements et les interactions des suspects en examinant leurs appels, messages et localisations. L'analyse des données informatiques permet aux enquêteurs de trouver des preuves numériques liées à des crimes en examinant des ordinateurs, des disques durs, des clés USB et d'autres appareils électroniques. Les méthodes numériques ont révolutionné notre façon d'enquêter sur le crime. Les avancées technologiques permettent maintenant de collecter et d'analyser les données de manière considérablement plus efficace, ce qui permet une résolution plus rapide et précise des affaires. Grâce à ces techniques, les traces numériques laissées par les délinquants peuvent être retrouvées et les crimes identifiés. « Cet outil est indispensable dans notre arsenal d'investigation, Les enquêtes numériques sont devenues indispensables et sont de plus en plus employées pour résoudre des affaires et traduire les délinquants devant la justice » affirme un répondant.

En Côte d'Ivoire, certains individus malveillants ont recours aux avancées technologiques pour perpétrer des actes délictueux, notamment dans la ville d'Abidjan. Les méthodes les plus fréquemment employées sont le Phishing, qui consiste à envoyer des messages frauduleux afin d'obtenir des informations personnelles, et le Vishing, une forme de fraude en ligne utilisée par des cybercriminels pour obtenir des renseignements personnels ou financiers en se faisant passer pour des entités légitimes telles que des banques, des sociétés de cartes de crédit ou des organismes gouvernementaux.

En parallèle de ces diverses méthodes, il convient également d'évoquer le Ransomware, stratagème employé par des individus malveillants afin d'infecter les ordinateurs de leurs victimes au moyen de programmes malveillants. Ce procédé vise à chiffrer les fichiers des utilisateurs pour ensuite exiger une rançon en échange de la clé de déchiffrement. Ces individus ont recours à des logiciels de

manipulation d'images pour altérer des documents officiels tels que des cartes d'identité, des passeports ou des actes de naissance, dans le dessein frauduleux d'obtenir divers avantages tels que des emplois, des prestations sociales ou des droits de vote. Un enquêté a ainsi déclaré : « Depuis l'avènement de ces outils informatiques, il m'est devenu plus aisé de générer des profits substantiels, car il est possible de manipuler autrui et de leur extorquer des fonds sans craindre d'être appréhendé par les forces de l'ordre ».

Un autre répondant a renchéri en ces termes : « Avec l'avènement d'Internet, de nouvelles formes de délits ont vu le jour, en sus des crimes préexistants qui ont également connu une recrudescence. Tout peut désormais s'accomplir au moyen d'une simple connexion et d'un ordinateur ».

Les malfaiteurs s'adonnent également au piratage informatique, une pratique malveillante visant à s'introduire dans les bases de données des institutions publiques afin de manipuler les informations relatives à la nationalité, aux documents administratifs, aux données personnelles et financières de leurs victimes. Ces individus peuvent ainsi mettre la main sur des données sensibles telles que les numéros de cartes bancaires, les mots de passe et les données de géolocalisation, leur permettant ainsi de falsifier des documents officiels et de contourner les dispositifs de sécurité. De plus, ils exploitent les réseaux sociaux pour repérer, surveiller et planifier leurs attaques contre leurs cibles, tout en diffusant de fausses informations afin de les piéger.

Les données recueillies par la PLCC, l'UIT, la police nationale, la gendarmerie nationale, l'ARTCI et la DITT mettent en évidence l'ampleur de la criminalité liée aux nouvelles technologies dans le pays, en particulier dans la ville d'Abidjan.

En 2021, les services de la PLCC ont enregistré 840 infractions liées à la cybercriminalité, comprenant notamment 181 cas d'abus de confiance et 659 cas de falsifications et d'utilisation frauduleuse de cartes bancaires. Cette même année, 753 cas de contrefaçon, 115 cas de fraude liée à la nationalité et 203 faux passeports ont été signalés.

En 2022, 550 cas d'atteintes sexuelles commises sur Internet ont été rapportés, dont près de 78% impliquent la diffusion ou la détention d'images pornographiques mettant en scène des mineurs. De plus, 753 cas de contrefaçon, 115 cas de fraude liée à la nationalité et 203 cas de

fraude sur les passeports ont été recensés selon le rapport de la DITT de 2022.
Durant la même année, il a été recensé 241 infractions à l'encontre des systèmes de traitement automatisé de données, avec des incidents principalement liés à des accès frauduleux entraînant des altérations, des suppressions ou des modifications de données. Par ailleurs, les autorités compétentes ont rapporté 972 cas de violation des droits individuels en matière de collecte, de traitement non autorisé, de divulgation, de conservation ou de détournement de données personnelles, ainsi que 671 cas de violation des fichiers, des libertés et des correspondances électroniques.

Entre les années 2022 et 2023, des actes de vol à main armée ont été signalés suite à des écoutes téléphoniques effectuées sur les victimes. Les forces de l'ordre nationales et la gendarmerie ont identifié 45 cas de ce type, impliquant des sommes d'argent considérables.
En 2023, l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) a répertorié 723 cas d'atteintes à la dignité et à la personnalité, comprenant des actes d'injure publique et de diffamation injustifiée envers des individus, ainsi que 396 cas de provocation à la haine ou à la discrimination. De plus, 109 cas d'injures ont été enregistrés en raison des convictions politiques des victimes. Selon la Plateforme de Lutte Contre la Cybercriminalité (PLCC) et la Direction des Technologies de l'Information et de la Communication (DIT), le préjudice subi en Côte d'Ivoire s'élève à 3,3 milliards de francs CFA, dont plus de 700 millions de francs CFA de pertes financières liées aux fraudes en ligne.

4.1.2. Analyse des méthodes d'enquête liées aux nouvelles technologies.

Selon Rees M. (2020)[7], les progrès technologiques dans le domaine de l'enquête ont rendu la collecte, l'analyse et la conduite d'enquêtes plus efficace et rapide.

En Côte d'Ivoire, la loi N° 2013-451 du 19 Juin 2013 a pour objectif de combattre la délinquance liée aux nouvelles technologies en

[7] REES M. (2020).

fournissant aux autorités des outils numériques pour l'enquête criminelle. Les systèmes de reconnaissance faciale et de géolocalisation sont parmi ces outils qui permettent de détecter les criminels en cavale et de suivre les mouvements des suspects.

Les autorités utilisent aussi d'autres moyens numériques, tels que l'analyse des données téléphoniques, pour repérer les mouvements et les interactions des suspects en examinant leurs appels, messages et localisations. Les données informatiques permettent aux enquêteurs de découvrir des preuves numériques de crimes à l'aide d'ordinateurs, de disques durs, de clés USB et d'autres appareils électroniques. Notre façon d'enquêter sur le crime a été révolutionnée par les méthodes numériques. La collecte et l'analyse des données sont maintenant plus efficaces grâce aux avancées technologiques, ce qui permet une résolution plus rapide et précise des affaires. Les traces numériques laissées par les délinquants peuvent être retrouvées et les crimes identifiés grâce à ces techniques. Un répondant déclare que « cet outil fait partie de notre arsenal d'enquête, les enquêtes numériques sont devenues essentielles et sont de plus en plus utilisées pour résoudre des affaires et traduire les délinquants devant la justice ».

4.2. Avantages et faiblesses des méthodes d'enquête liées aux nouvelles technologies

4.2.1. Avantages des méthodes d'enquête liées aux nouvelles technologies

Les méthodes de travail des forces de l'ordre et des services d'enquête ont été fortement modifiées par la révolution numérique. Les avancées dans le domaine du traitement informatique ont permis aux enquêteurs d'accéder à des données inatteignables, renforçant ainsi la lutte contre la cybercriminalité. Le nombre de plaintes traitées sur le site spécialisé dans la lutte contre la cybercriminalité est passé de 5 000 à 15 000, ce qui démontre l'importance des outils numériques dans la résolution des affaires criminelles.

En 2022, 4 265 plaintes ont été enregistrées et 176 individus coupables de cyberescroquerie ont été condamnés à une peine d'emprisonnement ferme. En 2009, 980 signalements ont été faits, 76 personnes ayant été arrêtées pour cyberescroquerie. 37 des accusés ont été reconnus coupables et condamnés à des peines de prison ferme. En

2020, le nombre de dénonciations a augmenté de 1 766, avec 68 condamnations prononcées par les autorités judiciaires ivoiriennes. En 2021 et 2022, 914 dénonciations ont été recensées et 6 personnes ont été condamnées. De plus, 69 personnes ont été arrêtées, 51 personnes ayant comparues devant le Parquet.

La police a répondu à l'augmentation de la criminalité numérique en Côte d'Ivoire, en particulier à Abidjan, pour mettre fin à ces pratiques qui menacent la sécurité publique et la réputation du pays. Cette réponse s'est traduite par l'instauration d'une régulation du cyberespace ivoirien. En 2012, un décret a été promulgué pour identifier les abus de services de télécommunication et renforcer les structures de lutte contre la cybercriminalité. L'ARTCI a été créé par l'État ivoirien pour limiter l'utilisation des nouvelles technologies de l'information et de la communication sur le territoire national.

Les enquêteurs utilisent maintenant des données numériques provenant de diverses sources pour surveiller les agissements des suspects, recueillir des éléments de preuve et reconstituer les scènes de crime. Les nouvelles technologies permettent également d'analyser les données des délits enregistrés tous les jours, ce qui permet de prédire les crimes à venir et de cibler les zones et les moments présentant les risques les plus importants pour renforcer les patrouilles.

En 2019, les autorités ivoiriennes ont aussi utilisé des outils numériques pour combattre le grave trafic de personnes entre les pays voisins et la belle Côte d'Ivoire, ce qui a permis d'identifier les personnes impliquées dans ce trafic criminel.

En 2020, les forces de l'ordre ivoirien ont mis en place des techniques de surveillance numérique pour détecter les transactions financières suspectes de certains hommes d'affaires étrangers, afin de lutter contre le blanchiment d'argent et de préserver l'intégrité de notre économie florissante.

En 2021, les forces de sécurité ivoiriennes ont utilisé ces précieux outils pour surveiller les activités en ligne des groupes terroristes et démasquer les individus égarés dans l'extrémisme. Les autorités ivoiriennes ont utilisé la technologie pour collecter des preuves de fraudes en matière de nationalité et de passeports biométriques. Le réseau de fausses déclarations sur les Attestations de Concession Définitives a été démantelé grâce à la surveillance des

communications électroniques et à l'analyse des données numériques, ainsi que des bandes de coupeurs de routes, fléau de notre société paisible.

L'exploitation des nouvelles technologies a permis aux autorités compétentes de mettre fin en 2023 aux actes de chantage à des fins pécuniaires et à d'autres activités criminelles en ligne. Les pratiques de sécurité dans l'administration ont été profondément modifiées par la révolution numérique, en intégrant les outils numériques dans les enquêtes judiciaires pour lutter plus rapidement et efficacement contre la criminalité. Les enquêteurs peuvent s'adapter aux nouvelles formes de délinquance grâce à un arsenal de dispositifs juridiques novateurs.

4.2.2. Failles des nouvelles méthodes numériques d'enquête

Les avancées technologiques dans le domaine des enquêtes criminelles posent des questions sur la protection de la vie privée et sur l'intégrité des éléments de preuve. Les enquêteurs peuvent être abusifs quant à leurs droits individuels en utilisant des dispositifs tels que la surveillance électronique et la reconnaissance faciale.

Les documents de preuve numériques peuvent être manipulés ou déformés, ce qui nécessite une plus grande vigilance de la part des enquêteurs pour garantir leur fiabilité. Ces nouvelles pratiques peuvent être partiales, ce qui fait craindre l'équité et la justice des enquêtes criminelles. En fin de compte, l'utilisation de ces nouvelles technologies dans les enquêtes criminelles peut entraîner des erreurs d'évaluation et des décisions injustes.

Il est possible que les enquêteurs soient trop dépendants de ces instruments et négligent les méthodes classiques d'investigation, ce qui pourrait compromettre la résolution des crimes en laissant des lacunes dans l'analyse des éléments de preuve. Il est nécessaire de mettre en place des mesures de sécurité adéquates pour éviter toute fuite d'informations en utilisant les données sensibles recueillies lors des enquêtes.

En outre, les coûts d'acquisition et d'entretien de ces technologies peuvent être élevés, ce qui rend difficile l'accès à ces outils pour certaines agences responsables de l'application de la loi.

Les pertes liées à la cybercriminalité ont atteint près de 200 milliards de dollars en 2022, soit une hausse considérable par rapport aux chiffres de 2020 qui étaient de seulement 20 milliards de dollars.

Un rapport de la Plateforme de Lutte Contre la Cybercriminalité (PLCC) révèle que le détournement de fonds à partir de portefeuilles électroniques est en croissance constante dans tout le pays. Il peut y avoir des problèmes liés à la fiabilité des preuves numériques, à la protection des données personnelles et à la compétence des enquêteurs dans l'utilisation des nouvelles technologies dans certaines affaires criminelles.

Les détournements sur Internet ont atteint 2,35 millions d'euros en 2022, soit plus d'un quart de l'ensemble des fraudes électroniques recensées. L'escroquerie a augmenté considérablement cette année-là, avec 1014 cas recensés au premier semestre, contre 227 pour la même période l'année précédente. Des enlèvements d'enfants ont été signalés à Abidjan par les personnes impliquées dans ces actes répréhensibles, communément appelés "brouteurs".

Le ministère de l'Intérieur et de la Sécurité a indiqué que vingt et un enfants avaient été enlevés en moins de deux mois en 2023. Malgré l'utilisation de nouvelles technologies d'enquête, un seul enfant a été retrouvé sain et sauf. Malheureusement, les autres ont subi des mutilations ou ont perdu leur sang. À noter que le pays possède tous les outils pour combattre la cybercriminalité, mais les cybercriminels utilisent tous les jours les réseaux pour cibler leurs victimes et leur imposer des sommes frauduleuses, parfois jusqu'à violer et tuer.

La criminalité numérique est fortement sous-estimée en Côte d'Ivoire, car les citoyens sont peu conscients et ne prennent pas en compte les mesures de protection à prendre. Les autorités ivoiriennes ont de temps en temps, l'obligation de mettre en place des outils et des compétences techniques pour lutter efficacement contre ce phénomène transnational. Il y a peu de coopération internationale pour lutter contre la cybercriminalité. La législation en vigueur en matière de cybercriminalité limite les pouvoirs des autorités, ce qui semble insuffisant pour faire face à cette menace croissante.

5. Conséquences des tendances criminelles liées aux nouvelles technologies

Selon Boucher D.[8], les nouvelles technologies jouent un rôle important dans les tendances criminelles mais, aussi dans la société et les individus.

Les tendances criminelles sont fortement affectées par les avancées technologiques, avec des délinquants qui utilisent de plus en plus des moyens sophistiqués pour commettre des infractions traditionnelles et de nouvelles formes de criminalité. Ces pratiques ont une grande incidence sur le vol d'identité, la fraude en ligne, la cyberintimidation, le harcèlement en ligne et d'autres crimes difficiles à détecter et à punir.

La facilité d'accès aux armes et aux outils de piratage en ligne a aussi favorisé l'accroissement des crimes violents et des fraudes. L'essor de la cybercriminalité présente plusieurs enjeux tels que la dégradation de la réputation du pays et de ses ressortissants à l'étranger, les pertes financières pour les entreprises locales et les particuliers, les menaces pour la sécurité des particuliers et des entreprises.

Les sociétés de télécommunication et les fournisseurs d'accès Internet sont les plus durement touchés puisque leurs adresses IP sont fréquemment liées à la cybercriminalité. Il est crucial de renforcer les mesures de sécurité et de coopération internationale pour lutter efficacement contre les nouvelles formes de criminalité et protéger la société dans son ensemble. Les outils technologiques permettent aux criminels d'utiliser des méthodes plus complexes pour combattre les crimes classiques et les crimes modernes. Ces pratiques ont des effets considérables tels que le vol d'identité, la fraude en ligne, la cyberintimidation, le harcèlement en ligne et les crimes difficiles à déceler et à punir.

La facilité d'accès aux armes et aux outils de piratage en ligne a aussi contribué à l'augmentation des crimes violents et des fraudes. La montée en puissance de la cybercriminalité pose de nombreux défis, tels que la dégradation de l'image du pays et de ses citoyens à

[8] Boucher D. (2014, p.23).

l'étranger, les pertes financières pour les entreprises et les hommes d'affaires locaux, ainsi que les risques pour la sécurité des individus et des entreprises. Les entreprises de télécommunication et les fournisseurs d'accès à Internet sont les plus touchés puisque leurs adresses IP figurent régulièrement sur les listes noires de certains sites occidentaux de transactions commerciales. De plus, la jeunesse des cybercriminels pose un problème éducatif de premier plan. La confidentialité et la sécurité nationale peuvent être compromises par la cybercriminalité.

6. Lutte contre ce phénomène

La loi a été améliorée pour combattre les crimes liés aux nouvelles technologies de l'information et de la communication. La création de nouveaux délits pénaux a permis d'adapter les infractions traditionnelles aux NTIC. Les transgressions récentes ont été prises en compte dans la procédure pénale. L'usurpation d'identité est désormais très réprimée avec des peines allant jusqu'à cinq ans de prison et des amendes allant jusqu'à 10 000 000 de francs CFA. Il existe également des amendes pouvant aller jusqu'à 20 000 000 de francs CFA en cas de détournement de données d'identification.

La loi ivoirienne punit fortement la cybercriminalité avec une peine allant de cinq à dix ans d'emprisonnement et une amende de 5.000.000 Francs CFA à toute personne menaçant de destruction, dégradation ou dégradation de biens. En outre, une peine de 1 à 10 ans de prison et une amende de 500 000 à 100 000 Francs CFA sont prévues pour violation de la propriété intellectuelle par l'intermédiaire d'un système d'information, ainsi que pour toute communication interceptée, révélée ou exploitée sans autorisation.

Une campagne de sensibilisation aux dangers de la cybercriminalité a été mise en place en 2014 pour sensibiliser et former les jeunes à l'utilisation légale des technologies de l'information et de la communication. Un atelier stratégique a été organisé en Côte d'Ivoire par le réseau FRANCOPOL et la Police nationale ivoirienne pour lutter contre ce fléau et mettre en place des actions concrètes de coopération.

Grâce à une initiative des États-Unis, les agents de police ivoiriens ont pu suivre une formation intensive en langue anglaise axée

principalement sur la sécurité des technologies de l'information et de la communication. Dans le cadre de la collaboration franco-ivoirienne, des formations ont eu lieu en Côte d'Ivoire pour combattre la cybercriminalité. En 2012, 25 policiers et gendarmes de la direction de l'informatique et des traces technologiques ont participé à un stage visant à combattre les fraudes en ligne. En avril 2013, 18 enquêteurs ivoiriens ont bénéficié d'une formation spécialisée offerte par l'Office central de lutte contre la criminalité dans le domaine des technologies de l'information et de la communication.

En janvier 2012, le gouvernement ivoirien a lancé un projet ambitieux en créant l'Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC) pour combler le manque de professionnels qualifiés dans le domaine des nouvelles technologies de l'information et de la communication en Côte d'Ivoire. L'ESATIC est le centre d'excellence des TIC en Afrique du ministère de la Poste, des télécommunications et des Technologies de l'information et de la communication (MPTIC) Elle possède un centre de recherche sur la gestion et la régulation des NTIC, ce qui permet de lutter contre la cybercriminalité en développant les compétences des acteurs des NTIC. Le corps professoral compétent de la Côte d'Ivoire et sa collaboration avec des institutions renommées à l'échelle internationale permettent d'acquérir rapidement les compétences nécessaires pour relever les défis posés par les nouvelles technologies de l'information et de la communication.

Le ministère de la Poste, des Télécommunications et des Technologies de l'Information et de la Communication (MPTIC) sous l'autorité de l'ESATIC est un établissement de renommée dans le domaine des technologies de l'information et de la communication en Afrique. En tant que centre de recherche spécialisé dans la gestion et la régulation des NTIC, elle participe activement à la lutte contre la cybercriminalité en renforçant les compétences des professionnels du secteur. La Côte d'Ivoire est en mesure d'acquérir rapidement les compétences nécessaires pour relever les défis posés par les évolutions constantes des technologies de l'information et de la communication grâce à son corps professoral qualifié et à ses partenariats avec des institutions de renommée internationale.

Discussion

L'analyse de l'influence des nouvelles technologies sur les tendances criminelles et les pratiques d'enquête est essentielle dans un contexte de changement technologique. Les avancées technologiques au fil des décennies ont profondément influencé les schémas criminels et les pratiques d'investigation.

Les résultats de l'étude permettent d'analyser les nouvelles technologies et les tendances criminelles. Ils démontrent qu'en Côte d'Ivoire, les cybercriminels utilisent les nouvelles technologies pour commettre des crimes, notamment à Abidjan, par Phishing, Vishing, Ransomware pour obtenir soit des données personnelles, soit des documents officiels, soit des données des institutions publiques ou des retombées financières frauduleuses, Les services agréés de lutte, tels que la PLCC, l'UIT, la police nationale, la gendarmerie nationale, l'ARTCI et la DITT, révèlent l'importance de la criminalité liée aux nouvelles technologies dans le pays, notamment dans la ville d'Abidjan.

Les écrits de Menn J. (2019) abondent dans ce sens. Les délits économiques tels que la fraude, le vol, l'escroquerie, l'usurpation d'identité, la cyberfraude, le piratage informatique et d'autres infractions d'envergure sont de plus en plus fréquents en raison de l'avènement des nouvelles technologies.

L'étude a également analysé les pratiques d'enquête en lien avec les nouvelles technologies. La loi N° 2013-451 du 19 Juin 2013, visant à combattre la cybercriminalité, autorise les autorités à utiliser des outils numériques avancés pour mener des enquêtes criminelles. Les outils technologiques permettent une collecte et une analyse plus efficace des données, ce qui améliore la résolution des affaires de manière rapide et précise. Parmi ces outils, les caméras de surveillance, les drones et les systèmes de reconnaissance faciale ont grandement facilité l'identification des délinquants et la collecte des preuves plus rapidement et plus efficacement.

Ces observations sont confirmées par les travaux de (Dufresne D., 2021) et Bogaert O. (2021). Ces auteurs ont noté que les nouvelles technologies ont grandement amélioré les techniques d'enquête traditionnelles, notamment en ce qui concerne l'analyse des données

et la collecte de preuve plus précise et plus rapide. Les agences de sécurité ont pu collaborer de manière plus efficace et partager des informations en temps réel, facilitant ainsi la résolution des affaires criminelles grâce à ces innovations.

L'autre résultat de l'étude met en évidence les bénéfices des pratiques d'enquête en lien avec les nouvelles technologies. Les pratiques des autorités policières et des services d'enquête ont été profondément modifiées par l'ère numérique. Les services de télécommunications ont été identifiés par des unités spécialisées dans la lutte contre la cybercriminalité. De nombreuses plaintes ont été traitées par les plateformes spécialisées dans la lutte contre la cybercriminalité. Les outils peuvent également déterminer les zones et les moments à risque, ce qui facilite le renforcement approprié des patrouilles. Les enquêteurs peuvent maintenant utiliser des données numériques provenant de diverses sources pour retracer les déplacements des suspects, recueillir des preuves et reconstituer les scènes de crime. Les techniques numériques ont permis aux enquêteurs de résoudre et d'éviter de nombreuses activités criminelles. De nouveaux outils ont permis aux enquêteurs de disposer d'un arsenal juridique révolutionné.

Les travaux de (Toubiana V., 2021) confirment cette tendance. L'intégration des nouvelles technologies a permis aux organismes chargés des enquêtes de réaliser des avancées significatives en termes d'efficacité opérationnelle, de précision des résultats, de rentabilité, de convivialité et de protection de la vie privée. Ces avancées technologiques ont considérablement amélioré le traitement des affaires, diminué la durée de traitement d'une affaire et augmenté le pourcentage de condamnation des coupables.

Les résultats de l'étude mettent aussi en évidence les limites des nouvelles technologies dans l'enquête de certaines affaires criminelles. En effet, ces lacunes compromettent la fiabilité des éléments de preuve numérique, la sécurité des informations personnelles ou encore la compétence des enquêteurs dans l'utilisation des nouvelles technologies. Les pertes financières demeurent considérables malgré la mise en place de nouvelles méthodes d'enquête en raison de l'évolution de la cybercriminalité. Parfois, les autorités ivoiriennes rencontrent des problèmes d'outils et de savoir-faire pour lutter efficacement contre ce fléau. La mise en place de la coopération

internationale rencontre des obstacles. Le cadre juridique de la cybercriminalité reste lacunaire, ce qui restreint les possibilités d'intervention des autorités. Les enquêteurs laissent donc les criminels bénéficier des lacunes du système.

Cette réalité a été soulignée par (Zuboff S., 2022) qui affirme que l'utilisation de ces nouvelles technologies pose des questions d'ordre éthique et juridique. La collecte de données personnelles à la fin de la surveillance peut affecter la vie privée des individus, tandis que l'utilisation d'une analyse prédictive peut entraîner des discriminations injustes et des formes de criminalité plus sophistiquées grâce aux avancées technologiques.

L'étude s'intéresse aussi aux effets importants du phénomène tant sur l'économie, les entrepreneurs et l'État que sur le social. Cela se traduit par une mauvaise réputation du pays et de ses citoyens à l'étranger et une menace pour la sécurité nationale et individuelle en ce qui concerne la divulgation de la vie privée des personnes.

Cette situation inquiétante est mise en évidence par les travaux de (Bounaamane B et Zined D, (2023), qui soulignent que la délinquance liée aux nouvelles technologies a des conséquences importantes tant sur le plan individuel que communautaire. Les vols de données et les attaques en ligne ont un impact important sur les particuliers ainsi que sur les entreprises et les institutions gouvernementales, causant des pertes financières considérables. La cybercriminalité expose également les individus et la société à des risques de vol d'identité et de cyberharcèlement. La propagation de contenus illégaux sur le Web, comme la pornographie pour enfants ou les propos haineux, peut être préjudiciable à l'ensemble de la population. Les conséquences économiques sont importantes pour les entreprises, les entrepreneurs et l'État, ainsi que sur le plan social, entraînant une détérioration de l'image du pays et de ses citoyens à l'étranger, ainsi que pour la sécurité nationale et individuelle en ce qui concerne l'exposition de la vie privée des individus.

Les stratégies de lutte contre ce phénomène sont également traitées dans les résultats de cette étude. Des sanctions financières ont été prononcées contre les cybercriminels pour tenir compte de ces nouvelles formes de crimes. Des actions concrètes de coopération ont été mises en place pour lutter contre la cybercriminalité. Le groupe IB

MAROC et la Direction de l'Informatique et des Traces Technologiques (DITT) ont conclu une convention pour partager des connaissances et bénéficier d'un soutien stratégique dans le domaine des Technologies de l'Information. Par ailleurs, des policiers ivoiriens ont bénéficié d'une formation intensive en anglais, en particulier en matière de sécurité des technologies de l'information et de la communication, sous l'impulsion des États-Unis. Des établissements de télécommunications et de technologies de l'information et de la communication ont vu le jour dans le but d'offrir une formation de qualité dans le domaine des NTIC.

Les résultats de nos recherches sont comparables à ceux de (Lachaux J-P., 2020), qui soulignent l'importance des investissements des États dans la formation et la perfection des compétences des enquêteurs pour tirer pleinement parti des nouvelles technologies et méthodes d'enquête. Grégoire abonde dans le même sens dans ses recherches, soulignant la nécessité de travailler avec des experts en technologie et en cybercriminalité pour mieux lutter contre ces nouvelles formes de délits. Il met aussi l'accent sur la sensibilisation du public aux bonnes pratiques de sécurité, en particulier en matière de cybersécurité et de confidentialité.

L'article recommande de réaliser des études approfondies sur l'impact des nouvelles technologies sur les tendances criminelles, en mettant l'accent sur des domaines spécifiques tels que la cybercriminalité, la fraude en ligne et le vol d'identité. Il est également recommandé d'analyser les méthodes d'enquête actuelles et de les adapter aux nouvelles technologies, en formant des enquêteurs qui utilisent des outils numériques et en développant des techniques d'investigation spécialisées pour traiter les crimes liés à la technologie. Il est conseillé de collaborer avec des experts en technologie et des organismes de réglementation pour élaborer des politiques et des protocoles efficaces pour lutter contre les crimes numériques.

Ces résultats s'inscrivent dans la théorie de la cybercriminalité en constante évolution de Wall (2024), laquelle met en avant la recrudescence des crimes commis en ligne tels que le piratage informatique, la fraude en ligne et le vol d'identité. Ces actes délictueux sont de plus en plus fréquents et représentent une menace sérieuse pour la sécurité des individus et des organisations. Cette théorie souligne l'importance de comprendre et de combattre ces

crimes numériques afin de protéger les données personnelles et financières des individus, ainsi que de préserver la sécurité des systèmes informatiques et des réseaux. Elle met en lumière la rapide évolution de ce phénomène et les défis qu'il pose aux autorités et aux sociétés en matière d'adaptation aux nouvelles technologies pour contrer les tendances criminelles émergentes.

L'objectif de l'étude a été pleinement atteint et les résultats obtenus viennent confirmer le cadre théorique établi. Cependant, il convient de souligner que notre recherche présente certaines lacunes concernant les données relatives à l'impact des nouvelles technologies sur les tendances criminelles ainsi que sur les méthodes d'enquête. Ces lacunes sont principalement dues à une faiblesse des données empirique sur le phénomène et des problèmes méthodologiques, en termes de collecte et d'analyse des données. En effet, les organismes chargés de lutter contre la criminalité numérique se trouvent confrontés à un manque de données suffisantes, ce qui limite la portée de notre étude et ne permet pas d'approfondir les enquêtes menées dans ce domaine.

Conclusion

L'analyse portant sur l'impact des nouvelles technologies sur les tendances criminelles et les méthodes d'enquête souligne la rapide et complexe évolution du paysage criminel à l'ère numérique. Les progrès technologiques ont indéniablement facilité la commission des infractions, mais ont également offert de nouveaux moyens aux autorités chargées de faire respecter la loi pour les contrer. Les méthodes d'investigation ont démontré que les nouvelles technologies ont un effet bénéfique sur le renforcement des compétences des enquêteurs et la résolution des affaires criminelles, tout en mettant en évidence les failles du système susceptibles d'entraîner des biais dans la collecte de preuves et des violations des droits individuels et de la vie privée. L'étude a également mis en lumière les conséquences des tendances criminelles liées aux nouvelles technologies, telles que les pertes financières, la détérioration de l'image nationale et les atteintes à la sphère privée des individus.

Pour relever ce défi, des mesures législatives ont été instaurées, des renforcements de compétences ainsi que des formations aux nouvelles

technologies ont été initiés, et des écoles professionnelles ont été fondées. De surcroît, il est impératif de développer la coopération avec d'autres États. Les autorités policières et judiciaires doivent constamment s'adapter aux avancées technologiques afin de demeurer efficaces dans la prévention et la résolution des crimes.

En analysant l'impact des nouvelles technologies sur les tendances criminelles et les méthodes d'investigation, cette étude contribue à l'accroissement des connaissances en matière de sécurité publique. Elle offre des informations précieuses sur les tendances émergentes en matière de criminalité et sur les moyens de les combattre de manière efficace. Ces résultats ont des implications pratiques significatives pour les décideurs politiques, les forces de l'ordre et d'autres acteurs engagés dans la prévention et la lutte contre la criminalité.

Références bibliographiques

Bogaert Olivier (2021), *Enquêter avec les nouveaux outils numériques*, Revue française de science politique, pp.123-145.

Boucher David (2014), *Éthique et reconfigurations de l'économie de marché : nouvelles alternatives, nouveaux enjeux, Les nouvelles technologies de surveillance et de contrôle : un défi d'éthique*, Revue internationale d'éthique sociétale et gouvernementale, vol 16, n° 2, pp.23 45.

Bounaamane Bouchar, Zined Drissi (2023), Cybercrime and Cyber Resilience: The Challenges of Digital Security in a Connected World », *International Journal of Accounting, Finance, Auditing, Management and Economics*, vol 3-2, n°4, p.451-469.

Dufresne David (2021), *Dernière sommation : Disparitions et morts suspectes de la rue de la Soif*, Mystères et Enquêtes.

Enyegue Patricia (2024), L'enquête *pénale à l'épreuve de l'internet*. Revue Internationale du Chercheur. Vol 5, n°1, pp.1- 32.

Goodman Marc (2015), *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, The New York Times Book Review.

Gregoire Deal (2019), *Cybercriminalité : Menaces, Enjeux et solutions*, Editions Larcier.

Jean-Meire Caroline (2016), *Les nouvelles technologies et la lutte contre la délinquance : regards croisés France/Royaume Uni, Thèse de doctorat,* Université Panthéon-Sorbonne.

Koffi Koffi Paul (2021), Cybercrime *en Côte d'Ivoire : Enjeux et défis*, Université de Paris 1 Panthéon-Sorbonne École de droit de la Sorbonne.

Lachaux Jean - Phillip (2020), *Le cerveau funambule : Comprendre et apprivoiser son attention grâce aux neurosciences*, Editions Odile Jacob.

Menn Joseph (2019), *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*, The New York Times Book Review.

Rees Manes (2020), *Enquêtes numériques* : *Cybercriminalité, cybermenaces et cyberdéfense*, L'Express.

Stiegler Bernard (2016), *Comment ne pas devenir fou* ? La disruption.

Toubiana Vanessa (2021), *Privacy in the Age of Artificial Intelligence*, Review, pp.213- 301.

Wall David (2024), *Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime*, Criminology, SASS, Durham University, 32 Old Elvet, Durham.

Zetter Kim (2014), *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Wired. Countdown.

Zuboff Shoshane (2022), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, vol 27. n° 4, p. 352.