**CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DEMOCRATIE AINSI QUE DU DEVELOPPEMENT DURABLE**
***REVUE AFRICAINE INTERDISCIPLINAIRE***

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

**28ème année - Numéro 85 - Volume 1 - Octobre-Décembre 2024**

# L'APPORT DE LA CRIMINALISTIQUE EN DROIT JUDICIAIRE CONGOLAIS A L'AUNE DU NUMERIQUE

**Par**

**Héritier BULAMBO WIYALIKA**
*Assistant et Apprenant en D.E.S à la Faculté de Droit de l'Université de Kinshasa*
*Avocat près la Cour d'appel de Kinshasa/Gombe*

**Ferdinand MENDJOLEMBA TOKEMBE**
*Assistant et Doctorant à la Faculté de Droit de l'Université de Kinshasa*
*Avocat près la Cour d'appel de Kinshasa/Matete*

## RESUME

*La criminalistique numérique est un outil indispensable pour faire face à l'évolution de la criminalité en République Démocratique du Congo (RDC). Elle permet de recueillir des preuves fiables et exploitables, de lutter contre l'impunité et de renforcer l'efficacité du système judiciaire. Cependant, son développement nécessite des investissements importants en matière de formation, d'équipement et de législation.*

***Mots-clés :*** *Criminalistique numérique, Droit judiciaire, Cybercriminalité, Preuve numérique, Forensique informatique.*

## ABSTRACT

*Digital forensics is an indispensable tool for dealing with the evolution of crime in the Democratic Republic of Congo (DRC). It makes it possible to gather reliable, usable evidence, combat impunity and enhance the efficiency of the judicial system. However, its development requires significant investment in training, equipment and legislation.*

***Keywords****: Digital forensics, judicial law, Cybercrime, Digital evidence, Computer forensics.*

## INTRODUCTION

La République Démocratique du Congo, comme de nombreux pays en développement, est confrontée à une croissance exponentielle de la criminalité numérique. Cette évolution est étroitement liée à la pénétration croissante des technologies de l'information et de la communication (TIC) dans tous les aspects de la vie sociale, juridique et économique.

En effet, dans sa doctrine, le feu professeur Kasongo Muidinge Maluilo, qui fut l'un de grand enseignant de la criminalistique dans notre pays, affirmait dans un article ce qui suit : « *la lecture des histoires judiciaires nous amène à ce*

*constat général que presque partout dans le monde, le système de justice criminelle ne semble plus répondre aux besoins de la société moderne tant au plan de son fonctionnement, efficacité, la rapidité et qu'à celui de ses objectifs (rééduquer, punir, protéger et des termes en vertu desquelles il fonctionne.* »[1]

Professeur Kasongo fait un constat amer selon lequel « *les paramètres judiciaires indiquent que la machine de répression semble non seulement essoufflée face à l'accroissement sans cesse de la criminalité, mais aussi confinée pratiquement à l'impuissance face à des formes nouvelles de la délinquance* »[2].

Avec comme conséquence qu'elle ne parvient plus à pénétrer dans les eaux profondes et tumultueuses de la criminalité devenue de plus en plus astucieuse et sophistiquée. Cette affirmation faite en 2001 par le professeur Kasongo demeure d'actualité à l'heure actuelle où tous les regards de nos compatriotes et des personnes éprises de justice sont tournés vers l'implantation d'un réel et véritable Etat de droit au travers une bonne administration de la justice.

Notre pays est en pleine mutation numérique. « *L'accès à l'internet et aux technologies de l'information et de la communication (TIC) s'est considérablement démocratisé ces dernières années, entraînant une transformation profonde de la société et de l'économie* »[3]. Cette évolution, bien que positive, a également ouvert de nouvelles portes à la criminalité d'où la nécessité de faire recours à la criminalistique.

Cet article tombe à point nommé, car il passe en revue le concours de la criminalistique sur la découverte de preuves des infractions récemment éditées au regard de nouvelles lois adoptées et promulguées à l'ère de la modernité avec l'internet et la révolution du numérique (réseaux sociaux, réseaux de télécommunications, nouvelles technologies, monnaie virtuelles et électronique, etc.). Il s'agit notamment du code du numérique, de la loi sur le blanchement de capitaux, financement de terrorisme et de la prolifération.

C'est dans ce contexte, que nous voulons réfléchir sur la criminalistique numérique en droit judiciaire congolais, qui se révèle être un outil indispensable pour les autorités judiciaires congolaises, « *pouvant leur permettre de faire face à la complexité des nouvelles formes de crimes et de recueillir des preuves fiables et exploitables devant le juge répressif* »[4].

---

[1] KASONGO MUIDINGE MALUILO, « L'apport de la Criminalistique en droit judiciaire congolais », *in Revue de la Faculté de droit, Université de Kinshasa,* 2ème année, n°2, 2001, p.1.

[2] *Idem.*

[3] P. NTETIKA MBAKATA, « L'Avocat et le numérique : les usages de l'internet aux frontières du secret professionnel » in, *Revue du Barreau de Kinshasa /Gombe*, n°08/2024, p. 33.

[4] H. BULAMBO WIYALIKA, « Le concours de la criminalistique dans la recherche de la preuve et son administration dans un procès pénal », in *Journal of Economics, Finance and Management (JEFM),* ISSN: 2958-7360 Vol. 3, No. 3, May, 2024, p.9.

Cet article a pour objectif d'analyser le cadre théorique et contexte congolais de la criminalistique numérique (I) suivi de l'apport de la criminalistique numérique en droit congolais (II), avant de chuter avec l'analyse de nouvelles formes de criminalité numérique (III) enfin la conclusion.

## I. LE CADRE THEORIQUE ET CONTEXTE CONGOLAIS DE LA CRIMINALISTIQUE NUMERIQUE

Plusieurs facteurs ont contribué à cette transformation rapide de la criminalité numérique en RDC à savoir: la croissance du secteur des télécommunications, (le déploiement de réseaux mobiles et l'augmentation du nombre d'abonnés ont rendu les smartphones accessibles à un plus grand nombre de personnes aujourd'hui en RDC). L'essor des réseaux sociaux (les plateformes comme *Facebook*, *WhatsApp*[5], *tiktok*[6], *Twitter* et *Instagram,*[7] sont devenues des outils de communication incontournables, favorisant les échanges et la diffusion de l'information). Le développement de la criminalité électronique (les transactions en ligne se multiplient, offrant de nouvelles opportunités mais aussi de nouveaux risques), ainsi que la cybercriminalité, le développement du commerce électronique, etc.

La digitalisation de la société a donné naissance à de nouvelles formes de criminalité, souvent transfrontalières et complexes.

Dans les lignes qui suivent, nous allons définir les concepts clés de cet article, en passant en revue les contours sur le cadre théorique de la criminalistique numérique.

### A. Définition de concepts clés

Notre préoccupation est ici de circonscrire, la notion de la criminalistique numérique (1), suivi des étapes de l'enquête numérique (2) avant de développer la question de la cybercriminalité (3), suivi d'un mot sur le forensique informatique (4).

#### *1. La criminalistique numérique*

Le mot criminalistique au sens large, « *c'est l'ensemble des procédés applicables à la recherche et à l'étude matérielle du crime pour aboutir à sa preuve* »[8].

Selon Lionel Prévost, on peut encore définir la Criminalistique comme « *la science de l'enquête criminelle et du procès. Son champ de travail va de la scène de*

---

[5] H. BULAMBO WIYALIKA, *Le concours de la criminalistique dans l'administration de la preuve dans un procès pénal en droit congolais,* Mémoire de DES/DEA, UNIKIN, Faculté de Droit, 2018-2020, p.107.

[6] Application mobile de partage de courte vidéos, photos, de façon simple et instantanée via interface mobile

[7] Réseau social et application gratuite de partage de photo en ligne

[8] P-F. CECCALDI, *La criminalistique,* deuxième édition mise à jour, Paris, PUF, 1969, p.7.

*crime jusqu'au témoignage devant les tribunaux en passant par divers laboratoires*[9]. Essentiellement *multidisciplinaire, elle met à contribution l'expérience et le savoir de plusieurs spécialistes qui recueillent, analysent et interprètent les indices matériels trouvés sur les lieux du délit* »[10]. Dans ce sens, elle joue un rôle extrêmement important dans la conclusion d'une affaire criminelle.

En effet, Mushi Bonane définit la criminalistique en considérant son objet à savoir : « *l'enquête criminelle, avec un accent particulier sur la recherche, la gestion, la protection et l'administration de la preuve tant au niveau pré-juridictionnel qu'au niveau juridictionnel* »[11].

A notre avis, la criminalistique : « *offre aux juristes des techniques variées et indispensables dans l'accomplissement de leur mission par la recherche et la récolte des indices en vue de la constitution des preuves à charge ou à décharge (OMP), bien dire le droit (juge), mieux assurer la défense des intérêts de ses clients (avocat) et mieux orienter les actions (conseiller juridique)* »[12]. « *A l'ère des grandes mutations occasionnées par la révolution technologique* »[13].

A la lumière de ce qui précède, nous pouvons définir la crimininalistique numérique, ou forensique numérique, *comme une branche de la criminalistique qui s'intéresse à la récupération, à l'analyse et à la présentation de preuves numériques en droit positif congolais ainsi que leur administration devant les juges répressifs*. Ces preuves peuvent être retrouvées sur une multitude de supports telles que ordinateurs, smartphones, tablettes, disques durs, clés USB, cartes mémoires, etc.

***a) Les objectifs de la criminalistique numérique***

La criminalistique numérique est une discipline essentielle pour faire face aux défis posés par la criminalité dans notre société numérique. Elle permet de recueillir des preuves fiables et exploitables, et de contribuer à la résolution des affaires pénales devant le juge.

Cette branche nouvelle de la criminalistique revêt les objectifs qui peuvent se résumer comme suit : l'identification et la collecte de de preuves numérique, son analyse, sa conservation et sa présentation devant le juge.

***2. L'enquête numérique et ses étapes***

Du point de vue étymologique, le mot « ***enquête*** » est un substantif qui vient du verbe « *enquérir (s')*»[14]. Ce verbe pronominal vient du latin « *inquirere* » qui

---

[9] L. PREVOST, P. BOULANGER et A. LAUZON, *Eléments de criminalistique appliquée,* Edition Mont-Royal : Modulo, Québec, 1987, p.4.

[10] O. RIBAUX, *Police scientifique le renseignement par la trace*, collection de science forensique, Presses polytechniques et universitaire romandes, Rome, 2014, p. 34.

[11] S. MUSHI BONANE, *Notes de cours de criminalistique*, UNIKIN, Fac de Droit, 2020-2021, p. 5 (inédit).

[12] H. BULAMBO WIYALIKA, *op. cit.,* p. 6.

[13] *Idem.,* p.24.

[14] B-H. du CHAZAUD, *Dictionnaire de synonymes et contraires,* Paris, le Robert, 2000, p. 291.

signifie *rechercher ou chercher à savoir*[15]. Ses synonymes les plus proches sont « *rechercher* », « *s'informer* », « *se renseigner* » ou « *aller aux renseignements* », « *demander* »… Le verbe « *s'enquérir* » trouverait certainement son antonyme dans celui « *se désintéresser de* »[16] et laisserait passer l'idée qu'on ne peut « *aller aux renseignements* » qu'en fin limier, en détective ou en sondeur.

Le mot « enquête » pourra être entendu comme : « *l'ensemble d'activités exercées par des autorités constituées en vue de permettre aux cours et tribunaux de statuer sur la matérialité et l'imputabilité d'un fait pénal* »[17].

L'enquête numérique peut être comprise dans les étapes suivantes : l'acquisition des données numériques, leur analyse, conservation et interprétation et leur présentation devant le juge.

***a) Les outils utilisés en criminalistique numérique***

Les outils utilisés en criminalistique numérique sont nombreux et variés, et évoluent en permanence avec les nouvelles technologies. On peut citer : Les outils d'acquisition de données permettent de copier les données d'un support numérique vers un autre sans les altérer ; Les outils d'analyse permettent d'examiner le contenu des fichiers, de reconstruire des événements, de retrouver des données supprimées, etc. ; Les outils de visualisation permettent de présenter les résultats de manière claire et compréhensible ;

***b) Qu'est-ce que la preuve numérique et ses domaines d'application ?***

La preuve numérique désigne tout élément d'information stocké sous forme numérique pouvant être utilisé comme preuve dans une procédure judiciaire. Il peut s'agir d'un email, d'un document Word, d'une photo numérique, d'une vidéo, d'un fichier audio, d'un enregistrement téléphonique, de données de localisation GPS, d'un historique de navigation internet, etc.

Dans les sociétés évoluées, les systèmes de preuves rationnelles se sont progressivement substitués au système de preuves mystique et divin. L'abolition de la torture et le rejet du rôle primordial de l'aveu en droit pénal ont marqué cette progression.

Ainsi avec « *les progrès scientifiques et le recours à des techniques de laboratoire* »[18], la science pénètre de plus en plus le droit, non pour y remplacer

---

[15] *Le Nouveau Petit Robert de la langue française 2008*, Paris, Le Robert, 2008, p. 879 : « (…) Mesure d'instruction permettant au juge de recevoir des tiers des déclarations de nature à l'éclairer sur les faits litigieux dont ils ont personnellement connaissance (…) » ; Jean DUBOIS, Henri MITTERAND et Albert DAUZAT, *Dictionnaire étymologique*, Paris, Larousse, 2007, p. 275 ; J-M. TASOKI MANZELE, *L'enquête des juridictions pénales internationales*, Thèse de doctorat, UNIKIN, Faculté de Droit, 2011, p.3.

[16] R. BOUSSINOT, *Synonymes, analogies et antonymes,* Paris, éd. Bordas, 2007, p. 354.

[17] Christian de VALKENNER, *Manuel d'enquête pénale*, édition Larcier, 2005, p.11.

[18] *Idem.*

les jugements par des expertises mais pour éclairer les juges par des experts en réduisant au minimum la part, d'impression, d'arbitraire, d'incertitude, de subjectivité et de sentimentalité. La conviction qui emportera sur la décision doit alors se fonder sur la démarche critique d'un examen total des faits.

La criminalistique numérique trouve des applications dans de nombreux domaines permis lesquels on peut retenir : *les enquêtes pénales,* (la cybercriminalité, les infractions sexuelles, le terrorisme, etc.), *les affaires civiles* (les contentieux commerciaux, la propriété intellectuelle, etc).

Dans notre société de plus en plus digitalisée, la preuve numérique joue un rôle de plus en plus important dans les procédures judiciaires. Elle permet d'une part, d'apporter des éléments concrets pour étayer les allégations des parties et d'autre part, d'identifier des auteurs ainsi que les métadonnées contenues dans les fichiers numériques, document ou actes enfin, les preuves numériques peuvent aider à reconstituer la chronologie des événements.

Malgré son importance, la preuve numérique pose plusieurs défis notamment: l'authenticité des preuves avec le risque toute altération de vérité, la fiabilité de preuve parce qu'elle peut être facilement supprimées ou modifiées voire perdues. Il faut qu'elle soit exacte et complète. Son l'interprétation nécessite des compétences spécifiques, la pertinence c'est-à-dire qu'elle doit être susceptible d'apporter une contribution à la résolution du litige ; les systèmes modernes sont de plus en plus complexes, ce qui rend l'analyse des données plus difficile. Enfin son cadre juridique en constante évolution rapide de technologie. Les outils et les techniques utilisés en criminalistique numérique doivent être constamment mis à jour.

### *3. La cybercriminalité*

Dans son mémoire de troisième cycle Kibwe Mulopo, rappelle qu'il y a une absence de consensus moins une controverse de la définition des concepts cyberespace dans laquelle on retrouve *la cybercriminalité et la cyberguerre*[19]. Il soulève le débat intéressant sur la difficulté *d'une admission unanime du terme « cyberguerre » qui découle essentiellement de l'angle d'analyse de la question. L'on ne saurait à vrai dire avoir une définition syncrétique à même de contenir tous les renseignements gravitant autour de cette réalité aux profondeurs imprécises.*

Lozel Kibwe affirme que chaque acteur à sa propre conception de la guerre dans le cyberespace. Dans l'amas littéraire existant, l'on rencontre des termes comme cyberconflictualité, cyberconflit, cyberattaque ou attaque informatique, guerre de l'information. Pour désigner autrement la « guerre » cyberspatiale.

---

[19] L. KIBWE MULOPO, *La République démocratique du Congo face aux défis de la cyberguerre*, Mémoire de DES/DEA, UNIKIN, Faculté de Droit, 2018-2020, p.19.

Malheureusement, même pour ces terminologies, les définitions ne sont pas toujours uniformes et communes.

Cette illustration est faite pour vous démontrer combien, il est difficile de définir la cybercriminalité qui est une menace grandissante dans l'ère numérique. Nous allons tenter de la définir comme *l'ensemble des activités illégales menées à l'aide d'un ordinateur, d'un réseau informatique ou d'un autre appareil connecté à Internet. Ces actes peuvent prendre des formes multiples et variées, allant de la simple fraude en ligne (*Phishing, escroqueries, ventes de produits contrefaits, etc.

### *4. Qu'est-ce que le forensique informatique ?*

Le forensique informatique, ou investigation numérique, est une discipline scientifique qui consiste à examiner et analyser des supports numériques (disques durs, clés USB, smartphones, etc.) afin de recueillir des preuves numériques pouvant être utilisées dans un cadre judiciaire ou pour résoudre des incidents de sécurité informatique.

Dans notre ère numérique, les preuves numériques sont omniprésentes. Que ce soit pour des enquêtes criminelles, des litiges commerciaux ou des incidents de cybersécurité, le forensique informatique joue un rôle crucial en permettant de : identifier l'origine d'une attaque, (en analysant les traces laissées par un attaquant, il est possible de déterminer sa méthode, ses objectifs et parfois même son identité).

Récupérer *des données effacées, (les techniques de forensique permettent de retrouver des fichiers qui ont été supprimés, formatés ou même chiffrés). Etablir une chronologie des événements, (en analysant les métadonnées des fichiers, (date de création, de modification, etc.)*[20]. Il est possible de reconstituer l'ordre dans lequel les événements se sont produits), Enfin fournir des preuves irréfutables, (les preuves numériques, lorsqu'elles sont correctement collectées et analysées, peuvent être utilisées devant un tribunal).

## II. L'APPORT DE LA CRIMINALISTIQUE NUMERIQUE EN DROIT CONGOLAIS

Pour être cohérent, il importe d'analyser l'apport de la criminalistique numérique (A), suivis de méthodes d'analyse et d'interprétation des preuves forensique (B)

### A. Apport de la criminalistique numérique

Il est question de découvrir comment les différents types d'indices numérique identifiés, prélevés et analyser sur des supports informatiques (1),

[20] A. BARICHELLA, « Cybersécurité et protection des données en Europe », in *La guerre cyber*, Biblioveilles, CDEM, octobre 2022. p.12.

Les techniques de collecte et de préservation des preuves numériques : acquisition, clonage et hash (2)

1. ***Les différents types de preuves numériques rencontrés dans les enquêtes : les données sur ordinateurs, smartphones, réseaux sociaux, cloud computing***

Les preuves numériques offrent de nombreuses possibilités pour résoudre des enquêtes, mais elles nécessitent une expertise spécifique pour être collectées, analysées et interprétées correctement.

Pour que les preuves numériques soient recevables devant un tribunal, il est essentiel de maintenir une chaîne de custody ininterrompue. Cela signifie qu'il faut pouvoir retracer le cheminement de la preuve depuis sa collecte jusqu'à sa présentation au tribunal, en garantissant son intégrité et en évitant toute altération.

***a) Données sur ordinateurs***

Les fichiers informatiques eux-mêmes (documents, images, vidéos, etc.) peuvent contenir des informations cruciales. Nous pouvons en trouver sur l'historique de navigation notamment sur les sites web visités, les recherches effectuées, les téléchargements réalisés peuvent révéler les activités en ligne de l'utilisateur.

De petits fichiers qui stockent des informations sur les préférences de l'utilisateur et peuvent être utilisés pour le suivi en ligne qu'on appelle dans le jargon informatique « **Cookies »** on peut également le retrouvé dans les mémoires cachés qui renferment les données temporaires qui peuvent contenir des fragments des pages web, des images ou d'autres contenus récemment consultés.

***b) On peut également en trouver sur des Smartphones***

Les éléments de preuves numériques peuvent être retrouvés, d'une part, dans les Messages, SMS, MMS, messages sur les applications de messagerie instantanée (WhatsApp, Telegram, etc.)[21] et d'autre part, dans les appels téléphoniques, photos et vidéos, données géolocalisation.

***c) Réseaux sociaux***

Avec l'évolution de la technologie, les preuves numériques également à retrouver dans les publications, (les messages, les photos, les vidéos et les commentaires postés sur les réseaux sociaux peuvent être utilisés comme preuve.) ; les messages prives, (les conversations privées peuvent contenir des informations sensibles[22].

---

[21] S. MUSHI BONANE, « La téléphonie cellulaire (GSM), facteur criminogène et booster de la délinquance juvénile en RD-Congo ? », in *Mouvements et enjeux sociaux*, n°112, Janvier-Mars 2020, p.8.

[22] *Idem.*

Nous pouvons les retrouver également dans les métadonnées qui ne sont rien d'autres que les informations associées aux publications (date, heure, emplacement) peuvent fournir des indices importants d'une part, et par contre d'autres preuves peuvent être recueillis autres des amis et contacts qui peuvent révéler les relations sociales avec l'utilisateur.

*d) Cloud computing*

Ces preuves sont à rechercher dans les fichiers stockés dans le cloud (documents, photos, vidéos, etc.) peuvent être récupérés, sont disponibles sur les plateformes cloud qui enregistrent généralement les actions de l'utilisateur, telles que les fichiers téléchargés, modifiés ou supprimés.

***2. Les techniques de collecte et de préservation des preuves numériques : acquisition, clonage et hash***

La collecte et la préservation des preuves numériques sont des étapes cruciales dans le cadre d'une enquête numérique. Ces techniques permettent de sécuriser les données, de garantir leur intégrité et de les rendre admissibles en justice.

*a) Acquisition des preuves numériques*

L'acquisition consiste à extraire les données d'un support numérique (disque dur, clé USB, téléphone, etc.) sans en altérer le contenu original. Les méthodes d'acquisition les plus courantes sont : le support numérique est physiquement déconnecté et connecté à un système d'acquisition, les mémoires vives RAM, nous avons également les preuves numériques sur l'acquisition logique: Seules les données accessibles par le système d'exploitation sont copiées.

**i. Clonage des preuves numériques**

Le clonage consiste à créer une copie identique bit à bit du support numérique original. Cela permet de travailler sur une copie tout en préservant l'intégrité de l'original. Les outils de clonage créent une image disque qui peut être montée comme un disque physique.

**ii. Le hash : une empreinte numérique**

Un hash est une valeur numérique unique générée à partir d'un ensemble de données. Il sert à vérifier l'intégrité des données. Si les données sont modifiées, même légèrement, le hash sera différent.

***Comment fontionner un hash ?***

Une fonction mathématique qui prend en entrée des données de taille variable et produit en sortie une chaîne de caractères de taille fixe. Son utilisation, sert à vérifier l'intégrité et la comparaison de hash d'une copie avec

celui de l'original pour s'assurer qu'aucune modification n'a été apportée. Il permet également de faire la détection de doublons c'est-à-dire identifier des fichiers identiques en comparants leurs hashes et voir identifier de fichiers connus.

**iii. Les bonnes pratiques de collecte et de préservation des données dans une enquête numérique**

Pendent une enquête numérique, il est recommandé de disponibiliser : un document qui retrace toutes les manipulations effectuées sur les preuves, de la saisie à la présentation au tribunal. Il est également recommandé de sécurisé l'environnement, car sans la sécurisation des opérations d'acquisition de clonage la preuve numérique risque la contamination voire son altération, voilà pourquoi, nous recommandons aux enquêteurs d'utiliser des outils forensique certifiés pour garantir la fiabilité des résultats et l'étiquetage de toutes étapes de la procédure, y compris les codages de paramètres utilisées pour la récoltes des résultats.

**B. Méthodes d'analyse et d'interprétation des preuves forensique numérique**

Nous allons aborder les différentes méthodes d'analyse en informatique forensique (1) suivi de la présentation de la preuve numérique recherchée devant le juge (2).

***1. Les différentes méthodes d'analyse en informatique forensique***

L'analyse forensique numérique est un domaine complexe qui requiert une variété de techniques pour extraire et interpréter des données à partir de systèmes informatiques. Les méthodes d'analyse se concentrent généralement sur trois aspects principaux : l'analyse de fichiers (a), l'analyse de réseaux (b) et l'analyse de contenu (c).

Cette analyse forensique numérique est un domaine en constante évolution qui nécessite une combinaison de compétences techniques et méthodologiques. La capacité à comprendre les différentes méthodes d'analyse et à utiliser les outils appropriés est essentielle pour mener à bien une enquête numérique.

***a) Analyse de fichiers***

L'analyse de fichiers consiste à examiner en profondeur les fichiers individuels stockés sur un système. Elle permet d'identifier des fichiers suspects, de reconstruire des événements passés et de découvrir des informations cachées. L'analyse peut se réaliser sur quatre éléments suivants les métadonnées, les contenus informatiques, les attributs ainsi que des fragments de fichiers.

Par analyse des métadonnées, il faut comprendre les différentes informations sur un fichier, telles que la date de création, la date de modification, l'auteur, etc. Ces informations peuvent révéler des indices sur l'historique du fichier. Tandis que l'analyse de son contenu c'est-à-dire du fichier lui-même pourra identifier des mots-clés, des phrases ou des patterns spécifiques.

Par contre, les attributs d'un fichier (lecture seule, caché, système) peuvent fournir des informations sur son utilisation et son origine enfin les fragments de fichiers peuvent être récupérés pour reconstituer des fichiers supprimés ou endommagés.

***b) Analyse de réseaux***

L'analyse de réseaux permet d'examiner le trafic réseau pour identifier les activités suspectes, les communications et les connexions. Cet analyse nous pouvons le réaliser par trois manière suivants : le capture de paquets, l'analyse approfondis des journaux de connexion enfin études des flux de trafic.

Par capture de paquets de données il convient de se mettre en face d'un circulant sur un réseau qui est capturés et analysés pour extraire des informations telles que les adresses IP, les ports, les protocoles utilisés et le contenu des communications.

Par contre, l'analyse des journaux de connexion des serveurs, des routeurs et des pare-feu sont analysés pour identifier les événements importants et les anomalies. Enfin, les flux de trafic sont analysés pour identifier les communications entre différents systèmes et les patterns d'activité.

***c) Analyse de contenu***

L'analyse de contenu consiste à examiner le contenu textuel, les images et les autres types de données telles que les vidéos pour en extraire des informations pertinentes. Les textes sont analysés pour identifier des mots-clés, des phrases, des thèmes et des sentiments tandis que l'étude des images sont analysées pour identifier des objets, des personnes, des lieux et des modifications. Les vidéos eux sont analysées pour identifier des événements, des objets en mouvement et des personnes.

***2. L'interprétation des résultats et leur valorisation juridique en informatique forensique***

L'interprétation des résultats d'une analyse forensique numérique est une étape cruciale. Elle consiste à donner du sens aux données collectées et à les transformer en preuves tangibles et exploitables dans un contexte juridique.

L'interprétation est une étape cruciale qui nécessite des compétences techniques et méthodologiques solides. Une interprétation rigoureuse et objective est essentielle pour garantir la justesse des décisions de justice.

***a) Le rôle de l'expert***

L'expert en informatique forensique, fort de ses connaissances techniques et de sa méthodologie rigoureuse, est chargé d'interpréter les résultats. Il doit *corréler les données*[23] *contextualiser les données*[24], *évaluer leur pertinence*[25] et Rédiger un rapport clair et concis, présentant de manière objective les résultats de l'analyse et les conclusions en découlent.

***b) Les défis de l'interprétation***

L'interprétation des résultats d'une analyse forensique peut s'avérer complexe pour plusieurs raisons notamment les volumes de données, la complexité des systèmes informatiques, l'évolution rapide des technologies ainsi que la subjectivité :

La quantité de données à analyser peut être considérable, ce qui rend la tâche longue et fastidieuse, mais aussi les systèmes informatiques modernes sont de plus en plus complexes, ce qui rend l'analyse plus difficile.

Il n'est secret pour personne que les technologies évoluent rapidement, ce qui nécessite une mise à jour constante des connaissances des experts. Et l'interprétation des données peut parfois être subjective et nécessiter un rapport d'expert.

***c) Valorisation juridique des résultats***

Pour que les résultats d'une analyse forensique soient admissibles en justice, il est essentiel de respecter certaines règles : le respect du droit privé, la présomption d'innocence et la loyauté dans la recherche de la preuve doivent être rigoureusement respectées pour garantir l'intégrité des preuves.

L'analyse doit être menée selon une méthodologie rigoureuse et documentée et le rapport d'expertise doit être clair, concis et compréhensible pour un juge répressif enfin, l'expert doit être reconnu comme compétent dans le domaine de l'informatique forensique.

---

[23] C'est mettre en relation les différents éléments de preuve pour établir des liens de causalité et reconstituer la chronologie des événements

[24] Tandis que contextualiser c'est situer les données dans leur contexte général, en tenant compte des éléments matériels et logiciels utilisés, des habitudes de l'utilisateur et des informations complémentaires disponibles.

[25] Evaluer c'est déterminer si les données sont pertinentes par rapport aux faits à établir et si elles peuvent constituer une preuve.

*d) Les enjeux de l'interprétation*

Une mauvaise interprétation des résultats peut avoir des conséquences graves :

- Des preuves mal interprétées peuvent conduire à la condamnation d'un innocent ;
- Des preuves non reconnues peuvent conduire à l'acquittement d'un coupable ;
- Une expertise mal menée peut remettre en cause la crédibilité de l'ensemble de la procédure judiciaire.

## III. DE NOUVELLES FORMES DE CRIMINALITE NUMERIQUE

Il convient de revenir sur les nouvelles formes de la cybercriminalité (A) suivi des crimes liés aux nouvelles technologies (B) avant de procéder à l'utilisation des TIC pour faciliter d'autres types de crimes à leurs interprétations (C).

### A. La cybercriminalité

Il est ainsi important de faire l'inventaire de quelques crimes cibles de la cybercriminalité notamment la fraude en ligne (1), les attaques informatiques (2) ainsi que la diffusion de contenus illicites (3).

*1. La fraude en ligne : Phishing, escroqueries, ventes de produits contrefaits*

La fraude en ligne est devenue un fléau du monde numérique, prenant de multiples formes et évoluant constamment. Les cybercriminels utilisent des techniques de plus en plus sophistiquées pour tromper les utilisateurs et s'emparer de leurs données personnelles ou financières. Parmi les principaux types de fraudes en ligne, on retrouve le phishing (a), l'escroquerie en ligne (b) et la ventes de produits contrefaits (c).

*a) Le phishing*[26]

Le phishing est sans doute l'une des méthodes les plus courantes. Les fraudeurs envoient des e-mails, SMS ou messages instantanés frauduleux, se faisant passer pour des entreprises de confiance (banques, services en ligne, etc.). Ces messages contiennent généralement des liens vers de faux sites web conçus pour voler vos identifiants de connexion, vos numéros de carte de crédit ou d'autres informations sensibles sur les réseaux Airtel money, Orange money et Mpesa. D'autres font des appels téléphoniques en se faisant passer pour les services clients de ces différents réaux mobiles.

[26] L'hameçonnage numérique, ou phishing en anglais, est une technique de fraude en ligne qui vise à voler des informations personnelles en usurpant l'identité d'une personne ou d'une organisation de confiance.

La fraude informatique est réprimée dans le code du numérique congolais en son article 340 qui dispose : « *Quiconque aura, intentionnellement et sans droit, causé ou cherché à causer un préjudice à autrui avec l'intention de procurer un avantage économique illégal à soi-même ou à un tiers, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante à cent millions de francs congolais : 1. S'il a introduit dans un système informatique, en modifiant, altérant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique ; 2. S'il perturbe le fonctionnement normal d'un système informatique ou des données y contenues* »[27]. Nous avons également la fraude aux cartes bancaires prévue aux articles 353 et 354 du même code du numérique.

***b) Les escroqueries en ligne***

Les escroqueries en ligne prennent des formes très variées, allant des arnaques aux faux cadeaux et aux loteries en passant par les escroqueries romantiques. « *Les cybercriminels exploitent la crédulité des utilisateurs pour les inciter à verser de l'argent ou à partager des informations sensibles* »[28].

D'autres font d'illusion aux utilisateurs pour les proposer des voyages en Europe, en Amérique voir en Asie en le faisant une offre qui semble trop alléchante, avec un travail mieux rémunérer. Il y a de fortes chances qu'il s'agisse d'une arnaque. Les escrocs mettront souvent la pression sur vous pour que vous agissiez rapidement.

***c) La vente et contrefaçon des marques de produits et du nom commercial : une menace pour les consommateurs***

La vente de produits contrefaits est un autre problème majeur en ligne. Les cybercriminels proposent des produits de marque à des prix très attractifs, mais ces produits sont souvent de mauvaise qualité, voire dangereux.

Dans l'actuel code du numérique congolais le législateur prévoit et punie l'infraction de contrefaçon de marque, nom commercial, appellation d'origine, indication géographique, logiciel et matériel de conception préparatoire en son article 376 qui dispose : « *La contrefaçon et/ou le piratage de marque, de nom commercial, d'appellation, de logiciel, des matériels de conception préparatoire et d'indication géographique est punie d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante à cent millions de Francs congolais ou de l'une de ces peines seulement. Constitue la contrefaçon, le fait sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénigrer, de dénaturer une marque, un nom commercial, une appellation d'origine ou une indication géographique*

---

[27] Article 340 du code du numérique

[28] R.B. MANASI N'KUSU KALEBA, « Quel droit pénal pour une lutte efficace contre la délinquance électronique et informatique ? Première partie : contre la délinquance informatique », *in* P. AKELE ADAU (dir.), *Réforme du Code pénal congolais : A la recherche des options fondamentales du Code pénal congolais*, Tome II, Ed. du CEPAS, 2008.

*appartenant à autrui au moyen d'un ou sur un réseau de communication électronique ou un système informatique.* » L'article 377 prévoit à son tour l'infraction « *de la contrefaçon de dessins et modèles* ».[29]

### 2. *Les attaques informatiques*

Les attaques informatiques sont devenues une réalité du monde numérique, mettant en péril les particuliers, les entreprises et les institutions. Ces attaques prennent diverses formes, mais parmi les plus répandues, on retrouve les ransomware (a), le piratage (b) et les intrusions dans les systèmes d'information (c).

***a) Ransomware attack screen*[30] :** Le ransomware est un type de logiciel malveillant qui chiffre les données d'un système informatique, les rendant ainsi inaccessibles. Les cybercriminels exigent ensuite une rançon en échange de la clé de déchiffrement. Les attaques par ransomware peuvent paralyser des entreprises entières et entraîner des pertes financières considérables. Le code du numérique punie toute accès et maintien illégal dans un système informatique dans les articles 332 et 333.

Le ransomware peut se propager par *le biais d'e-mails malveillants ou courrier indésirable ou pourriel ou spam*[31], de téléchargements frauduleux ou d'exploitations de vulnérabilités. *« Une fois à l'intérieur du système, le ransomware identifie les fichiers importants et les chiffre à l'aide d'un algorithme complexe. Un message apparaît à l'écran, informant la victime de l'attaque et demandant le paiement d'une rançon »*[32].

---

[29] Article 377 du code du numérique qui dispose : « *Est puni d'une servitude pénale de trois à cinq ans et d'une amende de cinquante à cent millions de Francs congolais ou de l'une de ces peines seulement celui qui, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de représenter ou de mettre à la disposition du public, un dessin ou un modèle protégé par le droit d'auteur ou un droit voisin au moyen d'un réseau de communication électronique ou un système informatique* ».

[30] En français signifie écran d'attaque par rançon logiciel. C'est possible lorsqu'un ordinateur ou un réseau est infecté par un rançongiciel (ransomware en anglais). L'écran de l'appareil infecté s'affiche généralement avec un message spécifique, appelé « *écran d'attaque par rançon logiciel* ». Ce message est conçu pour intimider la victime et l'inciter à payer une rançon pour récupérer l'accès à ses données.

[31] Article 363 du code du numérique qui dispose ce qui suit : « *Sera puni d'une servitude pénale de deux à cinq ans et d'une amende de dix à cinquante millions de Francs congolais ou d'une de ces peines seulement toute personne qui, intentionnellement et sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime : 1. déclenche la transmission des messages erronés, indésirables ou contraires à la loi, de courrier électronique multiples à partir ou par l'intermédiaire d'un système informatique ; 2. utilise un système informatique ou un réseau de communication électronique protégé pour relayer ou retransmettre des messages de courrier électronique multiples dans le but de tromper ou d'induire en erreur les utilisateurs ou tout fournisseur de service de courrier électronique ou d'accès à l'internet quant à l'origine de ces messages ; 3. falsifie gravement les informations d'en-tête dans des messages de courriers électroniques multiples et déclenche intentionnellement la transmission de ces messages* ».

[32] A. HAKIM, D. ADRIEN et D. SIDNEY, *La protection des réseaux contre les attaques DoS,* Université Paris Descartes, Mai 2009.

***b) Le piratage***[33]

Le piratage consiste à accéder sans autorisation à un système informatique. Les pirates peuvent avoir différents objectifs : *voler des données sensibles, perturber des services en ligne, ou prendre le contrôle de systèmes pour lancer d'autres attaques, espionnage industriel et le sabotage*[34].

En d'autres termes c'est une intrusion dans un système d'information est toute action non autorisée qui permet à un tiers de pénétrer dans un système informatique et d'y accéder, d'y utiliser des ressources, d'en modifier les données ou d'en interrompre le fonctionnement.

C'est ce que le code du numérique congolais réprime à l'article 337 en ces termes : « *Est puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de deux cents millions à deux cent cinquante millions de francs congolais, ou de l'une de ces peines seulement, celui qui, intentionnellement et sans droit, directement ou indirectement, provoque par tout moyen technologique une interruption du fonctionnement normal d'un système informatique. Quiconque, suite à la commission des faits visés à l'alinéa 1er, aura causé un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, … »*[35].

Pour se protéger contre ce piratage, il faut maintenir des logiciels à jours, l'utilisation des mots de passe forts et uniques, être vigilants face aux e-mails et pièces jointes suspectes, formes ses employer à mettre en place des solutions sécurisées.

Il faut retenir que les attaques informatiques sont des menaces omniprésentes. En adoptant les bonnes pratiques de sécurité, vous pouvez réduire considérablement les risques.

***c) Les intrusions dans les systèmes d'information***

C'est tout accès non autorisé à un système informatique par un tiers. Cela peut concerner une large variété d'appareils connectés tels que : l'ordinateur, téléphone serveur, réseaux. Soit pour y supprimer de manière des données dans un système informatique. Telle que prévue et punie par l'article 336 du code qui dispose : « *Celui qui, intentionnellement et sans droit, directement ou indirectement endommage, efface, détériore, altère ou supprime des données, sera puni d'une peine de servitude pénale de six mois à cinq ans et d'une amende de cinquante millions à cent millions de Francs congolais, ou de l'une de ces peines seulement. Si l'infraction visée à l'alinéa 1 est commise avec une intention frauduleuse ou dans le but de nuire, la peine de servitude pénale est de deux à cinq ans et d'une amende de*

[33] C'est le fait de s'introduire illégalement dans un système informatique

[34] A. NGUMBI AMURI, « Quel droit pénal pour une lutte efficace contre la délinquance électronique et informatique ? Seconde partie », in P. AKELE ADAU (dir.), *op. cit.*, p. 11.

[35] Article 337 alinéa 1et 2 du code du numérique.

*cinquante millions à cent millions de Francs congolais, ou l'une de ces peines seulement ».*

Soit dans le but d'y interrompre de manière frauduleuse dans un système informatique ou porter atteinte à l'intégrité du système informatique. Ce comportement est aussi prévue et puni par l'article 337 alinéa 1 du code du numérique qui dispose : « *Est puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de deux cents millions à deux cent cinquante millions de francs congolais, ou de l'une de ces peines seulement, celui qui, intentionnellement et sans droit, directement ou indirectement, provoque par tout moyen technologique une interruption du fonctionnement normal d'un système informatique* ».

***3. La diffusion de contenus illicites***

La diffusion de contenus illicites en ligne, tels que la pédopornographie constitue une menace grave pour la société. Ces contenus non seulement portent atteinte à la dignité humaine, mais ils peuvent également alimenter la violence et la radicalisation.

**a) La Pédopornographie ou la pornographie infantile**

La pédopornographie par le biais d'un système informatique ou d'un réseau de communication électronique est la production, la distribution, la possession ou la diffusion d'images à caractère sexuel d'enfants. Ce crime est universellement condamné et sévèrement réprimé dans la plupart des pays.

En droit congolais l'article 357 du CN qui dispose : « *Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de rendre disponible, de vendre, de se procurer ou de procurer à autrui, de posséder tout matériel pornographique mettant en scène un enfant par le biais d'un système informatique ou d'un réseau de communication électronique, est puni de cinq à quinze ans de servitude pénale principale et d'une amende de deux mille à un million de Francs congolais.* » et renchérie par les articles 174m du code pénal congolais, 179 alinéa 3 et 180 de la loi portant protection de l'enfant.

Cette infraction à des conséquences graves car les victimes de pédopornographie souffrent de traumatismes psychologiques durables. La diffusion de ces images contribue à pérenniser un marché criminel lucratif et à alimenter des réseaux de pédophiles. Pour lutter contre cette criminalité il est essentiel de signaler tout contenu pédopornographique aux autorités compétentes et aux plateformes en ligne. Il est également important de dispose des moteurs de recherche et les réseaux sociaux mettent en œuvre des systèmes de filtrage pour détecter et supprimer ce type de contenu.

La diffusion de contenus illicites en ligne est un problème complexe qui nécessite une réponse globale et coordonnée. La lutte contre ce fléau est un enjeu de société majeur qui concerne chacun d'entre nous.

**B. Les crimes liés aux nouvelles technologies**

Dans ce sous point nous allons nous limiter à l'analyser quelques infractions récurrentes notamment le harcèlement en ligne (1), la diffamation en ligne (2), et la violation de la vie privée (3).

***1. Le harcèlement en ligne***

Le harcèlement en ligne, ou cyberharcèlement, est devenu un fléau de notre société numérique. Il se manifeste de multiples façons et peut avoir des conséquences dévastatrices sur les victimes.

Le cyberharcèlement *désigne tout comportement agressif, répété et intentionnel exercé par une ou plusieurs personnes, à l'aide d'outils numériques, visant à porter atteinte à la dignité ou à l'intégrité psychologique d'une autre personne*[36].

Le cyberharcèlement est prévu dans le code du numérique en son article 359 comme suit : « *Quiconque aura harcelé, par le biais d'un système informatique ou d'un réseau de communication électronique, une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais, ou de l'une de ces deux peines seulement* »[37]. Le cyberharcèlement peut prendre plusieurs formes **:** les insultes et menaces, la diffusions de rumeurs, le harcèlement *sexuel*[38]*, le chantage* [39] etc.

***2. La diffamation en ligne***

La diffamation en ligne est une forme particulière de cyberharcèlement qui consiste à porter atteinte à l'honneur ou à la réputation d'une personne en diffusant de fausses informations à son sujet. *Les caractéristiques de la diffamation :* les faits diffusés doivent être faux pour qu'il y ait diffamation ; L'auteur de la diffamation doit avoir l'intention de porter atteinte à la réputation de la victime et l'existence de la publicité ; Que Faire en cas de cyberharcèlement et ou de diffamation?

Si vous êtes victime de cyberharcèlement et ou diffamation en ligne, il est important de réagir rapidement en conservant les éléments des preuves en faisant (les Screenshots, captures d'écran, etc.). Vous pouvez également bloquez l'harceleur sur les réseaux sociaux et signalez ses comptes. Vous pouvez également vous confiez à un proche, à un ami ou à un avocat enfin de

[36] J.Y. CIMALA CIBAKA, *Op.cit.,* p.150.
[37] Article 359 du code du numérique congolais
[38] Article 358 qui dispose : « *Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement haineux, tribal et hostile aux bonnes mœurs et aux valeurs patriotiques* ». Et enrichi par l'article 174D du code pénal congolais livre II.
[39] Article 174 W du Code pénal congolais livre II.

Portez plainte auprès des autorités compétentes conformément à l'article 360 du code congolais du numérique qui réprime ce comportement à son article 360 du CN.

***3. La violation de la vie privée***

La violation de la vie privée « *est devenue une préoccupation majeure dans notre société hyperconnectée. Avec la prolifération des technologies numériques, nos données personnelles sont de plus en plus exposées à des risques d'intrusion et d'exploitation illicites* »[40]. Parmi les principales formes de violation de la vie privée, on retrouve l'espionnage et la collecte illicite de données personnelles.

***a) L'espionnage en ligne***

L'espionnage est une atteinte à intimité personnelle qui consiste à recueillir des informations confidentielles sur une personne ou une organisation sans leur consentement, en utilisant des moyens illicites. Les motivations peuvent être diverses : espionnage industriel, rivalité personnelle, ou encore à des fins de chantage. Les méthodes utilisées sont nombreuses et variées, il peut s'agir de : *surveillance physique*[41], *cyberespionnage*[42] ou *de l'ingénierie sociale.*[43]

***b) La Collecte Illicite de données personnelles***

La collecte illicite de données personnelles désigne toute action visant à recueillir, traiter ou utiliser des données à caractère personnel sans le consentement de la personne concernée ou en violation des lois et réglementations en vigueur. La violation de la vie privée est un problème complexe qui nécessite une approche multidimensionnelle. La sensibilisation du public, le renforcement de la législation et le développement de technologies de sécurité sont autant d'éléments essentiels pour lutter contre ce fléau.

Les données personnelles peuvent être collectées de différentes manières : sur les réseaux sociaux, sur les sites web et les applications mobiles Les conséquences de la collecte illicite de données personnelles peuvent être graves telles que l'usurpation d'identité, chantage ou des publications ciblée intrusive.

Alors que faire pour se Protéger ? Nous suggérons à nos lecteurs les astuces suivent : sécuriser vos comptes en ligne par un mot de passe unique forts secret d'une part et d'autre part d'etre vigilant. Sur les réseaux sociaux, utiliser également les *VPN*[44].

---

[40] H. BULAMBO WIYALIKA, *Op.cit.*
[41] Installation de dispositifs d'écoute, de caméras cachées, suivi à distance.
[42] Piratage de comptes informatiques, interception de communications électroniques.
[43] C'est la manipulation psychologique pour obtenir des informations confidentielles.
[44] Le VPN est un réseau privé virtuel permet de chiffrer les données et de masquer votre adresse IP.

## C. L'utilisation des TIC pour faciliter des types de crimes

Les Technologies de l'Information et de la Communication (TIC) ont révolutionné notre mode de vie, mais elles offrent également de nouvelles opportunités aux criminels. En effet, les TIC sont de plus en plus utilisés pour faciliter la commission d'une multitude d'infractions, allant de la fraude à l'identité au trafic d'êtres humains, en passant par le blanchiment d'argent.

### *1. Le blanchiment d'argent ou de capitaux et les cryptomonnaies un mariage dangereux*

Nous avons tout à fait raison de souligner le lien entre le blanchiment d'argent et les cryptomonnaies. Ces dernières années, les cryptomonnaies ont été de plus en plus utilisées par les criminels pour dissimuler l'origine illégale de leurs fonds.

Le code du numérique congolais punie toute personne qui fera obstruction à l'enquête criminelle de blanchement par les moyens de cryptomonnaie à son article 345 qui dispose ce qui suit : « *Est puni de cinq à dix ans de servitude pénale et d'une amende de cinquante à cent millions de Francs congolais, ou de l'une de ces peines seulement, quiconque par un moyen de cryptologie, aura fait obstacle au déroulement des enquêtes au sens du Code de procédure pénale et de la présente ordonnance-loi ou refusé de fournir des informations ou documents y afférents* »[45].

Tandis que les *articles 4 point 1 et 124 de la loi n°22/068 du 27 décembre 2022*[46], prévoit et punie ce qu'il faut entendre par le blanchement d'argent ou de capitaux, comme suit : « *c'est le fait dans le but de dissimuler ou de déguiser l'origine illicite des biens au préjudice de l'Etat congolais commis un acte (ou un fait) de blanchement de capitaux soit en convertissant, transférant ou manipulant ces biens tout en sachant que lesdits biens proviennent d'une activités criminelle ou d'une participation à une activité criminelle.*

Pourquoi les cryptomonnaies sont-elles attrayantes pour les blanchisseurs d'argent ?

Les transactions en cryptomonnaies sont souvent pseudonymes, ce qui rend difficile de retracer l'identité des utilisateurs et de suivre le flux d'argent. Les transactions en cryptomonnaies sont généralement très rapides, ce qui permet de déplacer de grandes sommes d'argent rapidement et à travers les frontières.

Les cryptomonnaies peuvent être divisées en très petites unités, ce qui facilite le fractionnement de sommes importantes en de plus petites transactions, rendant ainsi le suivi plus difficile. Les plateformes d'échange de

[45] Article 345 du code du numérique.

[46] Lire utilement la loi n°22/068 du 27 décembre 2022 portant lutte contre le blanchement de capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive, JORDC, 64eme année, numéro spécial, Kinshasa, 11 janvier 2023.

cryptomonnaies sont nombreuses et faciles d'accès, ce qui facilite l'entrée dans le monde des cryptomonnaies. Comment les blanchisseurs d'argent utilisent-ils les cryptomonnaies ? Nous avons les *layering*[47], *les tumblers*[48] *et les mixers*.[49] Avec comme les risques Erosion de la confiance dans les cryptomonnaies, financement du terrorisme et la création d'instabilité des marchés financiers.

### 2. *Le trafic d'êtres humains et des organes est possible sur les réseaux sociaux à l'ère du numérique*

Le saviez –vous que c'est possible que les trafics des êtres humains et la ventes des organes puissent s'opèrent sur les réseaux sociaux? Les réseaux sociaux jouent un rôle non négligeable dans le trafic d'êtres humains. Ces plateformes, initialement conçues pour connecter les individus, sont malheureusement détournées par des trafiquants pour recruter et exploiter leurs victimes et vendre les organes tels que les cœurs et les reins. Comment les réseaux sociaux facilitent-ils le trafic d'êtres humains et la vente d'organe ?

Les trafiquants utilisent les réseaux sociaux pour identifier et cibler leurs victimes potentielles, souvent des jeunes vulnérables ou en situation de précarité. Ils peuvent créer de faux profils, publier des offres d'emploi alléchantes ou simuler des relations amoureuses pour gagner la confiance de leurs victimes d'une part et d'autre part la manipulation c'est-à-dire les trafiquants utilisent les réseaux sociaux pour manipuler psychologiquement leurs victimes, les isoler de leur entourage et les amener à croire en de fausses promesses.

[47] C'est une opération qui consiste à mélangés les fonds illégaux à d'autres fonds légaux à travers une série de transactions complexes pour en brouiller les traces.

[48] Un service en en ligne permet de mélanger les bitcoins de manière à rendre le suivi des transactions impossible.

[49] Ces outils permettent de mélanger les bitcoins de plusieurs utilisateurs, rendant ainsi difficile d'identifier l'origine des fonds.

## CONCLUSION

La criminalistique numérique est un outil indispensable pour faire face à l'évolution de la criminalité en RDC. Elle permet de recueillir des preuves fiables et exploitables, de lutter contre l'impunité et de renforcer l'efficacité du système judiciaire. Cependant, son développement nécessite des investissements importants en matière de formation, d'équipement et de législation. Car La formation des magistrats et des avocats à la compréhension des enjeux liés à la preuve numérique est une nécessité absolue pour garantir l'efficacité et la justice dans un monde de plus en plus digitalisé. Cette formation doit être continue et adaptée aux évolutions technologiques afin de permettre aux juristes de relever les défis posés par la preuve numérique.

La transformation numérique en RDC offre de nombreuses opportunités, mais elle pose également de nouveaux défis en matière de sécurité. Pour en tirer pleinement parti, il est nécessaire de mettre en place un cadre juridique adapté, de renforcer les capacités des acteurs concernés et de sensibiliser le grand public. Il est essentiel de sensibiliser les citoyens aux risques liés à l'utilisation d'Internet et de les former aux bonnes pratiques de sécurité.

Organiser des formations régulières pour les magistrats, les policiers et les avocats sur les techniques de la criminalistique numérique et sur le droit de la preuve numérique.

Créer des laboratoires de criminalistique numérique c'est-à-dire équiper les laboratoires existants et en créer de nouveaux dans les principales villes du pays. Réviser la législation congolaise pour prendre en compte les spécificités de la preuve numérique et garantir une protection adéquate des droits des individus.

## BIBLIOGRAPHIE


- Décret du 30 janvier 1940 Portant Code pénal congolais, tel que modifié et complété à ce jour ;
- Loi n°22/068 du 27 décembre 2022 portant lutte contre le blanchement de capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive, JORDC, 64ème année, numéro spécial, Kinshasa, le 11 janvier 2023 ;
- Ordonnance-loi n°23/010 du 13 mars 2023 portant code du Numérique, année, numéro spécial du 11 avril 2023 ;
- BARICHELLA A., « Cybersécurité et protection des données en Europe », in *La guerre cyber*, Biblioveilles, CDEM, octobre 2022 ;
- BULAMBO WIYALIKA H., *Le concours de la criminalistique dans l'administration de la preuve dans un procès pénal en droit congolais,* Mémoire de DEA, UNIKIN, Faculté de Droit, 2018-2020 ;
- BULAMBO WIYALIKA H., « Le concours de la criminalistique dans la recherche de la preuve et son administration dans un procès pénal », *in, Journal of Economics, Finance and Management (JEFM),* ISSN: 2958-7360 Vol. 3, No. 3, May, 2024 ;
- CECCALDI P-F, *La criminalistique,* deuxième édition mise à jour, Paris, PUF, 1969 ;
- CHRISTIAN de VALKENNER, *Manuel d'enquête pénale*, édition Larcier, 2005 ;
- Du CHAZAUD B-H., *Dictionnaire de synonymes et contraires,* Paris, le Robert, 2000 ;
- DUBOIS J., Henri MITTERAND et Albert DAUZAT, *Dictionnaire étymologique*, Paris, Larousse, 2007 ;
- HAKIM A., D. ADRIEN et D. SIDNEY, *La protection des réseaux contre les attaques DoS,* Université Paris Descartes, mai 2009 ;
- KASONGO MUIDINGE MALUILO, « L'apport de la Criminalistique en droit judiciaire congolais », *in Revue de la faculté de droit, Université de Kinshasa,* 2ème année, n°2, 2001 ;
- KIBWE MULOPO L., *La République démocratique du Congo face aux défis de la cyberguerre*, Mémoire de DEA, UNIKIN, FAC de Droit, 2018-2020 ;
- MANASI N'KUSU-KALEBA R.B., « Quel droit pénal pour une lutte efficace contre la délinquance électronique et informatique ? Première partie : contre la délinquance informatique », *in P. AKELE ADAU (dir.), Réforme du Code pénal congolais : A la recherche des options fondamentales du Code pénal congolais*, Tome II, Ed. du CEPAS, 2008 ;
- MUSHI BONANE S., « La téléphonie cellulaire (GSM), facteur criminogène et booster de la délinquance juvénile en RD-Congo ? », *in Mouvements et enjeux sociaux*, n°112, Janvier-Mars 2020 ;

- MUSHI BONANE S., *Notes de cours de criminalistique*, UNIKIN, Fac de Droit, 2020-2021 ;
- NGUMBI AMURI A., « Quel droit pénal pour une lutte efficace contre la délinquance électronique et informatique ? Seconde partie », in *P. AKELE ADAU (dir.), Réforme du Code pénal congolais : A la recherche des options fondamentales du Code pénal congolais,* Tome II, Ed, du CEPAS, 2008 ;
- NTETIKA MBAKATA P., « L'Avocat et le numérique : les usages de l'internet aux frontières du secret professionnel » in, *Revue du Barreau de Kinshasa /Gombe*, n°08/2024 ;
- RIBAUX Ol., *Police scientifique le renseignement par la trace*, collection de science forensique, Presses polytechniques et universitaire romandes, Rome, 2014 ;
- TASOKI MANZELE J-M., *L'enquête des juridictions pénales internationales*, Thèse de doctorat, UNIKIN, Faculté de Droit, 2011.