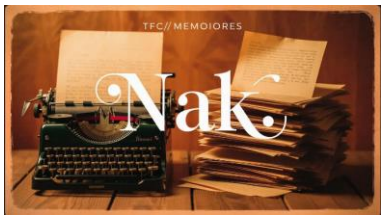

PUBLICATIONS

TFC & Mémoires

LA MISE EN ŒUVRE DU CODE DU NUMÉRIQUE EN MATIÈRE DE CYBERCRIMINALITÉ EN RDC : DÉFIS ET PERSPECTIVES

Ruth Mindana Sona
(*Tél: +243829043052*)

Citer cette version:
Ruth Mindana Sona, L*a mise en œuvre du code du numérique en matière de cybercriminalité en RDC : défis et perspectives*, Mémoire sous dir. Pr. K. Ndukuma, UPC, Kinshasa, 2023-2024. (N°2024-NAK-04M-DR-D-UPC)
https://www.kodjondukuma.com/2024-NAK-04M-DR-D-UPC_memoire_mindana.php

Submitted on 06 April 2025

Les vues et positons exprimées, dans le présent Mémoire ou TFC, sont celles de l'auteur et ne reflètent pas la position de l'Université ni ne doivent être considérées comme telle. Les ouvrages, articles, citations, et autres exemples mentionnés dans l'œuvre sont à titre de références et d'informations scientifiques

Cette publication est destinée au dépôt et à la diffusion des documents scientifiques de niveau mémoires et TFC, publiés ou non, émanant des établissements d'enseignement et de recherche UCC, UPC, UPN, en RD Congo sous la direction de recherche du Professeur Kodjo Ndukuma Adjayi.

En envoyant son œuvre, l'auteur a consenti à être publié sans frais d'exposition à payer et revendique le droit de paternité de son œuvre vis-à-vis du public pour tout référencement.

Le site web ne commercialisant pas le contenu de l'œuvre, les vues sur le contenu n'emportent aucune rétribution quelconque pour l'auteur à qui la vitrine d'exposition de son œuvre est offerte gratuitement, pour tout contact personnel, au monde sous l'icône du directeur de recherche.
L'auteur conserve le droit de demander la suppression de son œuvre du site web à tout moment.

UNIVERSITE PROTESTANTE AU CONGO

FACULTE DE DROIT

Département de Droit Privé et Judiciaire

B.P: 4745
KINSHASA/LINGWALA

LA MISE EN ŒUVRE DU CODE DU NUMÉRIQUE EN MATIÈRE DE CYBERCRIMINALITÉ EN RDC : DÉFIS ET PERSPECTIVES

Par

Ruth MINDANA SONA

Graduée en Droit

Mémoire de fin d'études présenté et défendu en vue de l'obtention du grade de Licencié en Droit.

Directeur : Kodjo NDUKUMA ADJAYI

Professeur Full

Année Académique : 2023 - 2024

EPIGRAPHE

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques et nucléaires. »

Colin Rose
Auteur et Chercheur,
Il a prononcé ce discours lors de la
Conférence du G8 sur la sécurité et
la confiance dans le cyberespace
à Paris le 15 mai 2000

DEDICACE

A mes parents, Josué MINDANA MUKOKO et Bienvenue LESWA MANDER, je dédie ce travail car vous avez battu un grand travail.

A mon petit frère Blessing MINDANA, puisse ceci être un modèle d'encouragement pour ton parcours.

À mes oncles et tantes, Richard MINDANA, Aimé MUBWISA, Sylvie LESWA, Aimée MINDANA, Gerry et Nico LESWA, Caroline, Méline et Gertrude MINDANA pour votre amour, vos sacrifices et peines.

À mes cousins et cousines Carmel, Danny, Divine, Nida, Georges, Jordini, Pistis, Promedi, Emile à toute ma famille trouvez ici un signe de fierté et un exemple à suivre.

À mes amis et connaissances, Keren, Ketsia, Rachel, Nadege, Suzane, Mystère, Gad, Sady, Emmanuel, Prisca, Jem, Yannick MAPAMBA.

À tous les membres du groupe de la distinction.

MINDANA SONA Ruth

REMERCIEMENTS

À l'Eternel Dieu Tout-Puissant, soit l'honneur, la gloire et l'adoration à perpétuité, car sans Lui, nous ne serons pas aujourd'hui à la fin de ce second cycle de notre étude universitaire.

Nos remerciements aux Autorités Académiques de l'Université Protestante au Congo, UPC en sigle et en particulier ceux de la Faculté de Droit au Département de Droit Privé Judiciaire pour avoir fait de nous ce que nous sommes aujourd'hui.

Nos remerciements à Monsieur Francis VANGU son aide dans l'élaboration de ce travail.

MINDANA SONA Ruth

PRINCIPAUX SIGLES, ACRONYMES ET ABREVIATIONS

ANCY	: Agence Nationale de la Cybersécurité
BCN	: Bureau Central National
CC	: Cybercriminalité
CI	: Crime informatique
CTC	: Commission Technique pour la Cybersécurité
DTNTIC/PNC	: Direction des Télécoms et des Nouvelles Technologies de l'Information et de Communication de la Police Nationale Congolaise
GPS	: Global Poitioning System
Hacking	: Piratage informatique
IMEI	: International Mobile Equipement Identity
INTERPOL	: Organisation internationale de police criminelle (pour la coopération Internationale)
Malware	: Logiciels malveillants
NTIC	: Nouvelles Technologies de l'information et de la communication
ONUDC	: Office des Nations Unies contre la drogue et le crime (pour les aspects Internationaux)
PDP	: Protection des données personnelles
Phishing	: Usurpation d'identité
PNC	: Police Nationale Congolaise
RDC	: République Démocratique du Congo
SI	: Système d'information
SSI	: Sécurité des systèmes d'information
TGI	: Tribunal de Grande Instance
TIC	: Technologies de l'information et de la communication

INTRODUCTION

La partie introductive de notre travail comprend six principaux points, à savoir : la problématique (I), les hypothèses (II), les méthodes et techniques de recherche (III), le choix et l'intérêt du sujet (IV), la délimitation du travail (V), ainsi que le plan sommaire (VI)

I. PROBLEMATIQUE

La cybercriminalité est en constante développement grâce à l'action accélérée de la digitalisation et la popularisation de l'internet.[1] Cette évolution s'explique par plusieurs autres facteurs notamment par l'augmentation de la connectivité, la sophistication des technologies, la démonstration des moyens techniques et outils numériques ainsi que la mondialisation des échanges commerciaux.

La police nationale congolaise démontre aussi les statistiques des cas de Cybercriminalité perpétrés entre janvier 2017 et septembre 2019. Au cours de cette période au moins 1882 cas de Cybercriminalité répartis en 17 catégories ont été enregistrés : 258 cas d'usurpation d'identité et escroquerie , 78 cas de chantage à la Webcam et Sextorsion , 143 cas de Fraude sur compte mobile ou bancaire , 60 cas de vente frauduleuse sur Internet , 450 cas de pédopornographie , 95 cas de diffamation et insultes en ligne , 153 cas de menace de mort par appel téléphonique ou via internet , 17 cas d'effacement de site web etc.[2]

La criminalité commit sur le réseau fait plusieurs victimes et parmi eux figurent l'État, les entreprises et les individus. La cybercriminalité se définit comme une notion large qui regroupe toutes les infractions commises sur ou au moyen d'un système informatique connecté sur le réseau.[3] La loi n°23/010 portant code du numérique la définit comme l'ensemble des infractions pénales spécifiques liées aux

---

[1] K. NDUKUMA ADJAYI, *Résumé écrit des séances de cours de droit du numérique*, Université protestante au Congo, année académique 2021-2022, p. 43.

[2] T. KALONJI , « La cybercriminalité en RDC en chiffres » [en ligne], in [https://tresorkalonji.pro/2018/09/la-cybercriminalite-en-rdc-en-chiffres.html], (consulté le 20 juillet 2024).

[3] Article 4.25, Loi n°20/017 du 20 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

technologies de l'information et de la communication dont la commission est facilitée ou liée à l'utilisation des technologies.[4]

La cybercriminalité ne fait pas allusion à une seule infraction, elle regroupe plusieurs autres comportements qui sont de trois types : les infractions de droit commun pour lesquelles l'internet est le moyen de commission telle que l'escroquerie, l'injure publique, l'offense envers le chef de l'État ; Les infractions informatiques au sens strict pour lesquelles l'informatique est la cible ou l'objet par exemple l'accès illicite aux bases de données, la falsification informatique ; Les infractions de diffusion en ligne, celles dont la condition d'existence est la divulgation d'information liées à la vie intime ou à la sphère privée sur le support électronique grand public telle que la revanche pornographique.[5]

La cybercriminalité est la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires. C'est un véritable tsunami[6] informatique au regard des dégâts et pertes qu'elle occasionne.[7]

La cybercriminalité fait objet de la répression en droit congolais, car la loi du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication prévoit plusieurs incriminations liées aux comportements cybercriminels. Ces incriminations prennent en charge les infractions dont notamment la pornographie infantile, le racisme, la xénophobie, etc.[8]

De même l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique est venue renforcer cette répression en prévoyant plusieurs mécanismes qui concernent tant le droit pénal de forme que droit pénal de fond. Elle réprime entre autre les atteintes contre les personnes à l'exemple de l'envoi de messages non sollicités, la tromperie, l'usurpation d'identité et autres. Mais également les atteintes

---

[4] Article 2.2, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, JO RDC, numéro spécial, 64e année, 11 avril 2023.

[5] K. NDUKUMA ADJAYI, « RDC, cybercriminalité, faire du vieux avec du neuf pour un renouveau sans révolution », *in ZooEco*, 25 mai 2020, disponible sur : [https://zoom-eco.net/a-la-une/rdc-cybercriminalite-faire-du-vieux-avec-du-neuf-pour-un-renouveau-sans-revolution-kodjo-ndukuma/] (Consulté le 5 juin 2023)

[6] Tsunami : « terme japonais désignant une série des vagues gigantesque générée par le déplacement rapide de grands volumes d'eau en raison d'évènements sismiques, d'éruptions volcaniques, de glissement de terrain, d'impacts météorites et d'autres perturbations. » (Voir la définition de tsunami dans le glossaire disponible sur www.seismecanada.gc.ca)

[7] M. CHAWKI, *Essai sur la notion de cybercriminalité*, IEHEI, Paris, 2006, p. 2.

[8] Articles 181 et 193, Loi du 25 novembre 2020, Préc.

contre les biens ou même les atteintes contre l'État entre autre la fraude aux cartes bancaires, le cyberespionnage, etc.[9]

La cybercriminalité profite de la distance physique entre auteurs et victimes, rendant d'autant plus complexe le travail des magistrats et des enquêteurs dans la recherche de preuve et l'identification de présumés auteurs.[10]

La cybercriminalité en RDC demeure une difficulté majeure dans l'administration de la preuve informatique, de l'indentification de la personne derrière ses traces informatiques et la territorialité.[11]

Le code du numérique prend en charge ces défis dans le cas des infractions commises sur internet par la personne physique ou morale. Et cela, sur le territoire ou hors du territoire de la RDC, à condition que ces faits soient reprimable par la législation congolaise.[12] De ce fait, les règles de compétence et de procédure applicables sont celles prévues par la loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétence des juridictions de l'ordre judiciaire et le Code de procédure pénale.[13]

La cybercriminalité est une réalité dans la société congolaise. Dans un jugement de 2018 du Tribunal de paix de Kinshasa/Gombe, le député Gecoco fut condamné à 18 mois de Servitude Pénale, sur pied de l'article 1 de l'ordonnance-loi du 16 décembre 1963 réprimant l'offense envers le Chef de l'État pour des contenus outrageants trouvés dans son téléphone.[14]

Dans un autre jugement de 2020 du même tribunal, un Communicateur d'un Parti politique Henry Maggie fut également condamné à la même peine pour des propos offensants à l'égard du Chef de l'État contenus dans une vidéo enregistrée et publiée sur les réseaux sociaux numériques.[15]

En novembre 2019, l'artiste musicien Héritier Watanabe avait fait l'objet d'un mandat d'amener du Procureur près le TGI de Kinshasa/Gombe à la suite de la

---

[9] Article 330-381, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[10] F. DESCHAMPS et C. LAMBILOT, *Cybercriminalité état des lieux*, Anthémis, Bruxelles, 2016, p. 6.

[11] K. NDUKUMA ADJAYI , B. LOSEKE RAMAZANI et al. , *Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité*, Harmattan, Paris, 2021 , p. 2.

[12] Article 329, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[13] Article 328, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[14] K. NDUKUMA ADJAYI, B. LOSEKE RAMAZANI et AL. , *Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité, Op. Cit*., p.343.

[15] *Ibidem.*

publication sur les réseaux sociaux numériques des vidéos faisant état d'une scène de sextape entre lui et sa compagne Naomie. Les deux partenaires avaient été arrêtés pour atteinte à la pudeur et outrages aux bonnes mœurs.[16]

L'accroissement de ce nouveau phénomène de criminalité, nous conduit à réfléchir aux préoccupations suivantes :

- Quelles sont les solutions données par le code du numérique face aux difficultés d'administration de la preuve, de l'identification de cybercriminels et de difficulté de la territorialité ?
- Quelles sont les défis et les perspectives de la mise en œuvre du code du numérique en ce qui concerne la cybercriminalité ?

Telles sont les questions fondamentales qui constituent la problématique de notre étude.

II. HYPOTHESES DE TRAVAIL

L'utilisation de nouvelles technologies de l'information et de la communication permet de maintenir la compétitivité et de développer de nouvelles opportunités.[17] L'objectif avoué est de faire du numérique congolais un levier d'intégration, de bonne gouvernance, de croissance économique et du progrès social.[18]

Le Code du numérique dans ses dispositions fixe les règles applicables à la cybersecurité et aux modalités de lutte contre la cybercriminalité.[19] Il dispose aussi les moyens permettant d'assurer la protection et l'intégrité des systèmes informatiques, ainsi que des données numériques.[20]

En ce qui concerne le défi de la territorialité, le code du numérique établit la compétence des juridictions congolaises. Lorsque l'infraction est commise sur internet sur le territoire congolais ou dès lors que le contenu illicite est accessible depuis la République Démocratique du Congo. Si la personne physique ou morale se rend coupable sur le territoire congolais comme complice d'une infraction commise à

---

[16] K. NDUKUMA ADJAYI, B. LOSEKE RAMAZANI et al. , Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité, *Op. Cit.*, p. 342.

[17] Présidence RDC, *Stratégie nationale de cybersécurité de la République Démocratique du Congo*, Kinshasa, Juillet 2022, p. 15.

[18] *Idem,* p. 6.

[19] Article 271, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[20] Article 272, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

l'étranger à condition que celle-ci soit punissable à la fois par la loi congolaise et par la loi étrangère. Et enfin lorsque l'infraction est commise par des Congolais hors du territoire de la République Démocratique du Congo et que les faits sont punis par la législation du pays où ils ont été commis.[21]

Le Code du numérique pose les modalités d'utilisation de la cryptologie en vue de la collecte des preuves électroniques de toute infraction.[22] Ce code met aussi en place une Agence Nationale de Cybersécurité chargée de la sécurité des systèmes informatiques en République Démocratique du Congo.[23]

Le code du numérique pose des principes tels que la participation criminelle et de la tentative punissable, la récidive et des circonstances aggravantes ; de peines et des sanctions contre les infractions les cybercriminels. Ces sanctions sont la servitude pénale, l'amende, la confiscation spéciale.[24] Mais aussi les règles relatives à constatation des infractions à la législation du numérique, à la perquisition des données stockées dans un système informatique ; et à l'interception des données et poursuites.

En ce qui concerne les perspectives, les approches en matière de la cybersécurité varient d'un pays à l'autre. Pour y parvenir il faut renforcer la législation en la matière, sensibiliser le public et les entreprises, promouvoir les structures nationales de la cybersécurité et créer un service informatique spécialisé en la matière.

Tous ceux-ci dans le but de réprimer ces actes criminels nés de l'utilisation des nouvelles technologies et de l'intérêt.

III. METHODES ET TECHNIQUES DE TRAVAIL

La réalisation d'un travail scientifique exige une démarche afin d'obtenir les résultats escomptés. Les méthodes sont utiles avant toute réflexion et elles organisent les techniques qui sont concrètes en vue d'atteindre un but.

Il convient de présenter les méthodes et les techniques que nous avons utilisées tout au long de notre travail :

---

[21]Articles 328 et 329, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[22]Article 272, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[23]Article 274, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[24] Article 310, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

A. METHODES

La méthode est une manière de dire, d'agir ou de faire une chose en suivant certains principes et un certain ordre pour parvenir à un but. C'est aussi l'ensemble des règles pour conduire raisonnablement et logiquement nos pensées.[25]

Il existe tant de méthodes exploitables mais dans le cadre de ce travail, nous avons analysé deux méthodes. Il s'agit de la méthode exégétique et la méthode analytique.

La méthode exégétique est utilisée dans la compréhension des textes par la recherche de l'intention du législateur. Elle consiste à expliquer la volonté du législateur à l'origine de la norme. Cette méthode nous permet de comprendre l'intention du législateur congolais portée dans l'élaboration de textes liés à la cybercriminalité tels que l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique et la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'informatique et de la communication.

La méthode analytique est une méthode de recherche qui se concentre sur l'analyse des données et des informations pour comprendre et expliquer des phénomènes.

Dans le cadre de ce travail, cette méthode nous permet de comprendre les enjeux de la cybercriminalité en RDC et solutions que le code numérique apporte à ces fléaux.[26]

B. TECHNIQUES

Les techniques représentent les étapes d'orientations limitées, liées à des éléments pratiques, concrets, adaptés à un but défini.[27] Elles sont un ensemble des procédés spécifiques qui président à l'agencement et à la réalisation de la méthode choisie par l'auteur d'un sujet d'étude pour sa réalisation.

---

[25] K. NDUKUMA ADJAYI et J. DOBO KUMA, *Guide méthodologique de référence pour recherches et rédaction des écrits universitaires en sciences sociales et juridiques*, Harmattan, Paris, 2023, p. 57.

[26] COMPILATIO, « Mener une recherche académique efficace : 9 méthodes de recherche à connaitre. », [en ligne] disponible [https://www.compilatio.net/blog/methode-recherche-academique#analytical] (Consulté le 22 juillet 2024)

[27] K. NDUKUMA ADJAYI et J. DOBO KUMA, *Guide méthodologique de référence pour recherches et rédaction des écrits universitaires en sciences sociales et juridiques*, *Op.cit.*, p. 63.

Dans le cadre de ce présent travail, nous recourons à la technique documentaire et la technique d'observation.

La technique documentaire nous permet de consulter les bibliothèques afin de recueillir le maximum d'informations disponibles contenues dans des ouvrages, des articles, de revues ainsi que l'internet sur le sujet sous examen.

La technique d'observation, les réseaux sociaux étant devenus des plateformes incontournables pour la communication et le partage d'informations attirent les cybercriminels. On y observe plusieurs délits tels que l'atteinte à la vie privée, l'arnaque, l'usurpation d'identité et autres.

IV. CHOIX DU SUJET ET INTERET

La cybercriminalité est un sujet qui fait l'actualité au sein de la société congolaise vu le nombre de fraudes informatiques, des violations de données personnelles, de piratage, d'usurpation d'identité, d'escroquerie sur internet etc. Elle suscite un intérêt croissant au sein de la société civile, des professionnels du droit et des autorités publiques.

Notre étude présente un double intérêt tant sur le plan théorique que sur le plan pratique.

Sur le plan théorique, ce sujet nous permet d'analyser les évolutions du droit pénal à la cybercriminalité. Il permet également de réfléchir aux concepts de cyberespace, de données personnelles et de cybersécurité.

Sur le plan pratique, elle nous permet de sensibiliser le public sur la question de la cybercriminalité afin de proposer des solutions et de se protéger contre ce phénomène. Il permet également de contribuer à l'amélioration du cadre juridique de la lutte contre la cybercriminalité en République démocratique du Congo.

V. DELIMITATION DU SUJET

Un sujet ne peut pas embrasser tout le droit en même temps d'où la nécessité d'une délimitation. Notre travail connait une délimitation triptyque à savoir : sur le plan spatial, sur le plan temporel et sur le plan matériel.

Sur le plan spatial, notre travail couvre tout l'espace géographique de la République démocratique du Congo.

Sur le plan temporel, notre étude débute à partir de la date d'entrée en vigueur du code du numérique en RDC le 13 mars 2023 tout en prenant en compte la loi du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication. Cela nous permet d'évaluer l'évolution de la cybercriminalité et l'efficacité des mesures mises en place depuis l'adoption de cette nouvelle législation.

Sur le plan matériel, notre présente étude sur la cybercriminalité mobilise plusieurs branches du droit telles que la procédure pénale, le droit pénal général et le droit pénal spécial afin de lutter contre ce phénomène.

VI. PLAN SOMMAIRE

Notre travail se structure en deux chapitres, en plus de l'introduction et de la conclusion. Le premier chapitre est relatif au développement du phénomène cybercriminel, le deuxième au cadre de répression de la cybercriminalité.

CHAPITRE I. LE DÉVELOPPEMENT DU PHÉNOMÈNE CYBERCRIMINEL

Aujourd'hui, on entend parler des pirates informatiques et de leurs crimes partout dans le monde. Mais s'est-on posé la question de savoir s'ils existent au Congo ? Comment opèrent-ils ? Sont-ils structurés ? Malheureusement, les pirates informatiques existent bel et bien en RDC. Ils sont arrivés par vagues, d'abord de l'Inde, puis du Maghreb. C'était pour la plupart d'anciens étudiants congolais revenus au pays qui s'essayaient à l'escroquerie pour gagner leur vie.[28]

En janvier 2021, le site de la Société Nationale d'Électricité (SNEL) a été la cible d'une cyberattaque, le rendant inaccessible jusqu'à ce jour. Cet acte a été attribué à des Congolais mécontents des interruptions intempestives de l'électricité. Les auteurs de cette cyberattaque promettaient de passer à un niveau supérieur en piratant également les turbines et les centrales électriques.[29] Chose qui a suscitée des multiples questionnements au tour de la cybersécurité, non seulement au sein de la population, mais aussi dans le chef des autorités Congolaises.

Dans le souci de répondre dans un cadre répressif en vue de prévenir ou d'atténuer ce fléau, nous allons exposer dans ce chapitre les dangers liés à la cybercriminalité, notamment son caractère transfrontière, l'identification du cyberdélinquant ainsi que la volatilité des preuves. Il traite également les principes posés par la loi contre les actes cybercriminels.

Nous développons ici deux sections dont la première, consacrée aux défis de la cybercriminalité (section 1) et la seconde, à la protection pénale des systèmes informatiques (section 2).

Section 1. Les défis de la cybercriminalité

La particularité de la cybercriminalité demeure intrinsèquement dans son caractère de déterritorialité. Le plus souvent, les auteurs des infractions informatiques sont en dehors du territoire de la victime ciblée.

En ce qui concerne les questions liées aux défis de la cybercriminalité, il est approprié que nous abordions les défis liés au caractère transfrontière de la

[28] TRESOR KALONJI, « Les pirates informatiques existent-ils en RDC ? », [en ligne] in [https://habarirdc.net] (Consulté le 05 octobre 2024).

[29] N. DJUMA SOSTHENE, « Augmentation des cyberattaques en RDC : Quelle réglementation pour lutter contre ce fléau ? », *In Droit Numérique*, Août 2024, n°2, p. 2.

Cybercriminalité en premier paragraphe **(§1)** et en second paragraphe **(§2)**, les défis liés à l'identification des délinquants et la volatilité des preuves.

§1. Les défis liés au caractère transfrontière de la cybercriminalité

La révolution numérique fait partie des processus de changement dont la dynamique est d'ordre universel. Cette révolution a affectée profondément nos habitudes, particulièrement par la fréquentation du cyberespace.[30]

La cybercriminalité intervient dans un cadre de déterritorialité tandis que le droit d'un État est territorial. De ce fait, dans ce paragraphe **(§1)** nous allons analyser le principe de la territorialité à l'épreuve de la cybercriminalité **(A)** afin de comprendre les caractères de la cybercriminalité**(B)**.

A. Le principe de la territorialité à l'épreuve de la cybercriminalité

Aux termes du principe de l'application de la loi pénale dans l'espace, il est question de déterminer la loi applicable lorsqu'une personne, auteur d'une infraction se trouve lors des poursuites dans un pays différent du lieu du crime.[31]

Le principe de la territorialité ou la *lex loci delicti* est la règle selon laquelle, la loi pénale d'un pays s'applique à toutes les infractions commises sur le territoire du pays, quelle que soit la nationalité du coupable.[32] Mais, l'internet est un media véritablement universel, les aspects géographiques tels que l'emplacement où l'information est physiquement stockée, revêtent une importance mineure.

Le droit pénal congolais traite le fond et la forme des infractions ainsi que leurs sanctions. Les juridictions reprisent dans la loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire ont l'habileté de poursuivre les actes cybercriminels. L'article 67 alinéa 1 de cette loi organique dispose qu' : *«en matière répressive, le Ministère Public recherche les infractions aux actes législatifs et réglementaires qui sont commises sur le territoire de la République »*.[33]

---

[30] K. NDUKUMA ADJAYI, *Résumé écrit des séances de cours de droit du numérique, Op.Cit*., 41.

[31] R. NYABIRUNGU, S. BOKOLOMBE, ET AL, *Droit pénal général congolais*, Éditions Droit et Société, Kinshasa, 2020, p. 57.

[32] K. NDUKUMA ADJAYI et J. DOBO KUMA, *Guide méthodologique de référence pour recherches et rédaction des écrits universitaires en sciences sociales et juridiques, Op.cit.*, p.330.

[33] Article 67 al.1, Loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire.

Par territoire congolais, il faut entendre l'espace sur lequel s'exerce la souveraineté de la RDC qui est régi par ses lois. Il s'agit du sol, du sous-sol, des eaux et des forêts, de l'espace aérien.[34]

La loi n°23/010 portant code du numérique consacre le même droit tel que les règles de compétence et des procédures applicables en matière des infractions à la législation numérique.[35] Ce principe présente plusieurs avantages liés à l'intérêt social, à une meilleure justice, au respect du principe de légalité et à l'exercice de la souveraineté par l'État.[36]

Au sujet de l'intérêt social, il est important que l'infraction soit jugée le plus près possible du lieu de la commission, car elle trouble l'ordre social et celui-ci doit être apaisé. Pour une meilleure justice, le juge local connaît sa loi nationale et pourra donc en faire une bonne application alors que le recours au droit étranger compromettrait sérieusement une saine justice.[37]

Par ailleurs, la procédure est facilitée lorsqu'elle a lieu sur le territoire de l'infraction. Les enquêtes peuvent être facilement conduites, avec des indices mieux recueillis et les auditions des témoins, possible et peu coûteuses. Le principe de la territorialité prône le respect de la légalité car le délinquant est sans ignorer la loi pénale du pays où il a posé son acte. Il n'est pas exclu qu'on lui applique la loi pénale qu'il pouvait effectivement ignorer.[38] Ceci permet à l'État d'exercer sa souveraineté sur son territoire, le maintien de l'ordre et de la sécurité à l'intérieur de ses frontières. Mais parfois les Etats n'ont pas toujours le moyen d'assurer le respect des règles à l'intérieur de leurs frontières.[39]

1. Les suppléments au principe de la territorialité

Le principe de la territorialité ne suffit pas à lui seul de poursuivre toutes les infractions, d'où le complément d'autres principes s'applique.

---

[34] Article 9, Constitution du 18 février 2006 telle que modifiée par la loi n° 11/002 du 20 janvier 2011 portant révision de certains articles de la constitution, in JO RDC, 52 ème année, n° spécial du 5 février 2011 .

[35] Article 328-329, Ordonnance-loi n° 23/010 du 13 mars 2023 préc.

[36] R. NYABIRUNGU, S. BOKOLOMBE, et al. *Droit pénal général congolais, op.cit.,* p. 59.

[37] *Idem,* p. 60.

[38] *Ibidem.*

[39] D. DANET et A. CATTARUZZA, « *La cyberdefense : quel territoire, quel droit ? »,* Economica, Paris, 2013, p.77.

a. La compétence personnelle et la compétence réelle

La compétence personnelle ou le principe de la personnalité est fondée non sur un titre territorial, mais sur un lien d'allégeance de l'auteur de l'infraction ou de la victime. La loi pénale s'attache ici aux personnes peu importe l'endroit où elles se trouvent.[40] La compétence personnelle peut être active ou passive. Elle est active lorsqu'elle découle de la nationalité, du lieu de domiciliation ou de la résidence de l'auteur de l'infraction à l'étranger.[41]

C'est ainsi que la loi pénale s'applique aux infractions qui se commentent sur le territoire national dans le but d'assurer la protection des citoyens hors du territoire. Le délinquant peut préférer la juridiction de l'État où il est ressortissant tout simplement parce qu'elle lui est plus familière que la juridiction étrangère et, en estimant que la loi nationale et le juge national sont mieux adaptés pour sa cause.[42]

La compétence personnelle est passive lorsque la loi pénale suit les ressortissants de l'État où elle est en vigueur et s'applique à toutes les infractions dont ils sont victimes. Ce principe va de l'idée que l'État doit protéger ses citoyens où qu'ils se trouvent et de connaître les infractions dont ils sont victimes.[43] Cependant, ce principe n'est pas à l'abri des critiques. Tout d'abord le juge de la nationalité de la victime peut être partial. Ce qui ne garantit pas une justice équitable.

La compétence réelle autrement appelée principe de la réalité, consiste pour un État de confier à ses tribunaux, la poursuite des atteintes portées à l'étranger à ses intérêts supérieurs.[44] Ce principe apparaît à la lecture des alinéas 4 et 5 de l'article 3 du code pénal congolais. L'alinéa 4, « *le juge congolais est compétent pour les infractions commises à l'étranger attentatoires à la sûreté de l'État et à la foi publique* ». Et l'alinéa 5 fait comprendre que : « *ces atteintes citées sont poursuivables par les juridictions Congolaises quelle que soit la nationalité du coupable et quel que soit l'endroit où il se trouve*».[45]

Le droit congolais prévoit aussi la compétence universelle pour la prise en charge des infractions d'une certaine gravité commise à l'étranger.

---

[40] D. DANET et A. CATTARUZZA, *La cyberdefense : quel territoire, quel droit ?, Op.Cit.,* p.61.

[41] A. HUET, R. KOERING -JOULIN, *Droit pénal international*, PUF, Paris, 1994, p. 230.

[42] *Idem*, p. 231.

[43] R. NYABIRUNGU, S. BOKOLOMBE, et AL, *Droit pénal général congolais, Op.Cit.*, p. 62.

[44] A. HUET, R. KOERING -JOULIN, *Droit pénal international, Op.Cit.*, p. 233.

[45] Article 3 alinéas 4 et 5, Décret du 30 janvier 1940 portant code pénal congolais tel modifié à ce jour, in J.O RDC, 45ème numéro spécial, Kinshasa, 30 novembre 2004

b. Le principe de l'universalité

La compétence universelle de la loi pénale donne au juge du lieu d'arrestation le pouvoir de juger toutes les infractions, quel que soit le lieu de leur commission et sans égard à la nationalité du délinquant ou de la victime.[46]

Ce principe de l'universalité trouve sa place en RDC dans l'article 3 alinéa 1 du code pénal qui dispose : *«Toute personne qui, hors du territoire de la République Démocratique du Congo, s'est rendue coupable d'une infraction pour laquelle la loi Congolaise prévoit une peine de servitude pénale de plus de deux mois, peut être poursuivie et jugée en République Démocratique du Congo, sauf application des dispositions légales sur l'extradition»*.[47]

En ce sens, les cours et tribunaux congolais peuvent juger toute personne, peu importe sa nationalité ou celle de la victime rendue coupable à l'étranger d'une infraction de certaine gravité au regard du droit congolais. A condition que ces infractions soient prévues par la loi congolaise et ensuite punies d'une peine supérieure à deux mois.[48]

2. La maitrise et le contrôle du cyberespace

Le cyberespace est un espace virtuel fait des connexions d'ordinateurs accessibles par médias et périphériques interposés.[49] Cet espace immatériel est une nouvelle forme de territoire que les Etats doivent maitriser et contrôler pour le bien de leurs nations ainsi que leurs populations, en raison des acteurs multiples qui peuvent y exercer diverses activités.

Selon l'article 9 de la constitution de la RDC, « *l'Etat exerce une souveraineté permanente notamment sur le sol, le sous-sol, les eaux et les forêts, ainsi que l'espace aérien*. »[50] L'Etat possède le droit de police et de surveillance dans la couche d'air qui surplombe son territoire en dehors de l'espace extra-atmosphérique.

---

[46] D. VANDERMEERSCH, « La compétence universelle », *in* A. CASSESE, M. DELMAS-MARTY, *Juridictions nationales et crimes internationaux*, P.U.F., Paris, 2002, p. 889.

[47] Article 3, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[48] K. NDUKUMA ADJAYI , B. LOSEKE RAMAZANI et al. , Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité ,Op.Cit., p.331.

[49] *Ibidem*.

[50] Article 9, Constitution du 18 février 2006, préc.

Le cyberespace est en juxtaposition avec d'autres espèces d'espace notamment la terre, l'air, la mer et l'espace-atmosphérique. Il s'oppose à l'espace conventionnel du fait qu'il affranchit toute localisation physique ou géographique.[51]

Cependant le cyberespace reste un concept difficile à cerner en raison de la nature dématérialisée des actes qui y sont commis. Contrairement aux actes blâmables dans le monde physique, où les lieux et les acteurs sont généralement bien définis, la cybercriminalité se déploie dans un espace numérique sans frontières géographiques précises.[52] Nous comprenons ici que les activités en ligne peuvent se dérouler n'importe où, sans lien avec un lieu physique précis. A l'exemple du commerce en ligne, qui, peut être géré depuis n'importe quel endroit du monde.

Le système juridique dans lequel une défense fonctionne dépend souvent de deux choses : qui vous attaque et pourquoi. Malheureusement, cela n'est pas le cas lorsque vous êtes attaqué dans le cyberespace.[53]

Plusieurs pays à travers le monde sont confrontés aux cybermenaces. La République démocratique du Congo, à l'instar de nombreux autres pays africains, subit fréquemment des cyberattaques dans le système informatique de l'administration. Face à ces menaces numériques croissantes, une réponse juridique renforcée s'impose pour maintenir l'ordre dans l'usage des outils informatiques et déterminer la responsabilité des auteurs qui se livrent à des actes de cyberattaque.[54]

B. Les caractères de la Cybercriminalité

La cybercriminalité est devenue une préoccupation majeure de nos jours en raison de la forte dépendance de la société moderne aux technologies de l'information et de la communication. Cette forme de criminalité implique l'utilisation illégale de l'informatique et de l'internet pour commettre des actes malveillants.[55] Ce

---

[51] G. PEREC, *Espèces d'espace*, Galilée Ed, Paris, essai 1974, p. 14

[52] [https://www.interpol.intl/fr/infractions/cybercriminalité/reponse-aux-cybermenaces] (Consulté le 11 aout 2024).

[53] B. SCHNEIER, « Les cyberconflits et la sécurité nationale », *in un.org*, 2017, disponible sur : [https://www.un.org/fr/chronicle/article/les-cyberconflits-et-la-securite-nationale] (Consulté le 03 août 2024).

[54] N. DJUMA SOSTHENE, « Augmentation des cyberattaques en RDC : Quelle réglementation pour lutter contre ce fléau ? », *in Droit-Numérique.cd* - Dossier N° 2 – Août 2024, p.1.

[55] R. CHARBONNIER, « Comprendre la cybercriminalité : focus sur cette menace moderne», *in Guardia.School*, 12 juin 2024, disponible sur : [https://guardia.school/boite-a-outils/quest-ce-que-la-cybercriminalite.html#:~:text=La%20cybercriminalit%C3%A9%20est%20devenue%20une,pour%20commettre%20des%20actes%20malveillants.] (Consulté le 15 Août 2024)

qui nous conduit à parler de leur caractère transfrontière (1), ainsi que leur caractère organisationnel(2).

1. La criminalité transfrontière et mondialisée

Le cyberdélinquant opère sous couvert d'anonymat, c'est-à-dire sous une fausse identité, afin de franchir les frontières et de porter atteinte à des victimes dans le monde entier. Les cyberdélinquants profitent de la faiblesse de la législation des États en matière de cybercriminalité pour opérer.[56]

La particularité de la criminalité commise sur les réseaux numériques est qu'elle a pour cible un espace désormais sans frontière et mondialisée.[57] Elle représente les traits d'une délinquance marquée essentiellement par l'immatérialité de son objet, l'internationalité de ses implications, l'anonymat de ses acteurs, l'évolution très rapide des techniques et des stratégies. Les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles-mêmes sont des données régies par le droit national. La cybercriminalité a donc un caractère international et pose des défis aux systèmes de justice pénale en place.[58]

Le spamming fait souvent partie du mode opératoire des cyberdélinquants. Définit comme l'envoi massif de courriers électroniques non sollicités à des personnes ciblées. Le spam est devenu une véritable pandémie pour les internautes du fait que leurs boîtes aux lettres sont envahies par des messages publicitaires non sollicités.[59] Par le Phishing ou hameçonnage qui est l'information consistant à envoyer un e-mail non sollicité à une personne dans le but d'obtenir ses coordonnées confidentielles.[60] Ensuite par le cheval de Troie qui est un logiciel permettant d'entrer les programmes malveillant dans la machine visée.[61]

---

[56] . NDUKUMA ADJAYI, B. LOSEKE RAMAZANI et AL., « *Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité* », *op.cit.*, p. 334.

[57] M. QUEMENER et Y. CHARPENEL, *Cybercriminalité, droit pénal appliqué*, Economica, 2010, p. 14.

[58] F. SKAF, « Cybercriminalité : une réalité protéiforme mal définie », *in Revue internationale de criminologie et de police technique et scientifique* 1/20, Paris, p. 2.

[59] E. FILIOL et R. PHILIP, *Cybercriminalité : enquête sur les mafias qui envahissent le Web*, Dunad, Paris, 2006, p. 80.

[60] K. NDUKUMA ADJAYI, B. LOSEKE RAMAZANI et AL. , « *Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité* », op.cit., p. 313.

[61] *Idem*, p.315.

Parfois même par des logiciels espions, des virus et des vers informatiques dans le but de recueillir des informations personnelles et d'introduire de programme informatique capable d'infecter la machine de l'utilisateur recherché.[62]

2. Une criminalité organisée

Divers actes de cybercriminalité requièrent un haut niveau d´organisation et de spécialisation. Le terme criminalité organisée est un ancien concept d'origine policière qui a été utilisé à partir des années 1920 le plus souvent dans des rapports de police. La cybercriminalité est considérée comme une criminalité organisée dans le sens où les cybercriminels avec la révolution de l'internet font de plus en plus partie de réseaux très organisés.[63]

La quasi-totalité des groupes cybercriminels utilisent des technologies en réseau pour mener à bien leurs activités criminelles. La nature même de l'organisation des cybercrimes varie en fonction du niveau de technologie numérique, du mode opératoire et des groupes de victimes visés. Dans le rapport de l'Office des Nations Unies Contre la Drogue et le Crime intitulé « *La criminalité transnationale organisée et son impact sur le secteur privé : les bataillons cachés* », les auteurs ont analysé les effets du crime organisé sur six secteurs suivants : Services financiers, technologie, biens de consommation et vente au détail, construction et immobilier, transport et logistique, et ressources naturelles. Leurs conclusions ont révélé quelques formes d'activités criminelles organisées qui affectent matériellement différents secteurs pour faciliter leurs crimes notamment par le blanchiment d'argent, le détournement d'actifs, la fraude, l'extorsion et la cybercriminalité.[64]

§2. Les défis liés à l'identification des cyberdélinquants et la volatilité des preuves

L'identification précise et rapide des cyberdélinquants, ainsi que la préservation des preuves constituent des défis important dans la démarche d'une enquête judiciaire efficace. Ainsi, ce paragraphe comporte deux points qui exposent l'identification du cyberdélinquant (A), et aussi la volatilité des preuves (B).

---

[62] Idem, 316.

[63] K. NDUKUMA ADJAYI, B. LOSEKE RAMAZANI et AL., « *Droit du commerce électronique: enjeux civils, consuméristes, cybercriminels, d'extranéité et de territorialité* », op.cit. , p. 335.

[64] [https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html] (Consulté le 1er Octobre 2024).

A. L'identification du cyberdélinquant

La description complète d´un cyberdélinquant peut contenir plusieurs éléments tels que : l'âge, le sexe, les antécédents socio-économiques, la nationalité et la motivation.[65] Sur ce, nous examinons les profils des auteurs des cyberdélits(1), en mettant l'accent sur les délinquants typiques, les niveaux de l´organisation criminelle, et aussi les techniques d'identification(2) selon les recommandations du code du numérique.

1. Les profils des cyberdélinquants

Les cyberdélinquants ont des profils et de motivations variées. Certaines attaques représentent souvent un moyen pour tester l'efficacité des systèmes de sécurité informatique afin de le rendre plus performants et sécurisés. Mais d'autres ont réussi à développer des techniques d'attaques rendant ainsi le cyberespace, un gigantesque territoire de crime organisé. Nous analysons alors ici deux principaux profils des acteurs malveillants du cyberespace.

a. Le hacker

C'est un anglicisme fréquemment utilisé dans le monde de l'économie digitale et la sécurité numérique et qui signifie « *pirate informatique*». Ce mot évoque l'image de quelqu'un ayant de mauvaises intentions envers les individus, les sites Web et les systèmes d'information des entreprises. La théorie la plus répandue est qu'ils cherchent des moyens de recueillir des données des entreprises et de détruire ou de modifier les informations des clients.[66]

Ce type de cybercriminel se regroupe en trois grandes familles qui se classent en fonction de la capacité à agir et des intérêts pécuniaires à poursuivre. Cependant, nous soulignons que tous les hackers ne sont pas de cybercriminel, mais une grande partie d'entre eux s'adonnent à des pratiques criminelles. On distingue ainsi :

- Les hackers « *white hat* » : sont ceux qui utilisent leurs capacités pour attaquer une entreprise, mais seulement de façon hypothétique. Son véritable objectif est

[65] Département des affaires économiques et sociales des Nations Unies, Division de statistique, 2003. Manuel pour l´élaboration d´un système de statistiques de la justice pénale ST/ESA/STATSER.F/89.

[66] [https://www.techtarget.com/searchsecurity/definition/white-hat] (Consulté le 1er octobre 2024).

de découvrir les failles du système de sécurité afin de proposer une solution optimale en vue de protéger la cible contre les pirates dangereux.[67]

- Les hackers « *black hat* » : Ceux-ci effectuent des violations informatiques illégales. Ayant l'accès non autorisé à un système, exécutant des modifications illicites d'un contenu, la diffusion de logiciels malveillants ou, la manipulation de données confidentielles. Ce type de pirate n'a que ses propres intérêts à cœur et utilise ses compétences d'une manière nocive.[68]
- Enfin, il y a les hackers « *grey hat* » : des pirates qui utilisent leurs compétences pour s'introduire dans les systèmes et les réseaux sans autorisation (tout comme les « black hat »). Mais au lieu de faire des ravages criminels, ils peuvent signaler leur découverte au propriétaire de la cible et proposer de réparer la vulnérabilité pour une somme sodique.[69]

b. Le crasher[70]

Le crasher est un cybercriminel qui se démarque plus de l'hacker classique par sa vision de voir les choses dont il veut opérer une attaque informatique. Il est avant tout un informaticien et possède aussi de bonnes connaissances en sécurité informatique. Le Crasher comme le nom l'indique n'a qu'un seul but, c'est détruire tout ce qui passe devant lui. En effet, le crasher ne se préoccupe pas trop souvent des contenues qu'il est à même de découvrir lorsqu'il entre dans un système informatique. Pour lui, l'ambition n'est pas nécessairement de trouver un gain ou un avantage, mais de se venger ou de faire payer à la victime en effaçant les données, quelle que soit sa valeur ou la sensibilité.

2. Les techniques d'identification

L'identification des cyberdélinquants est un enjeu majeur actuellement, marqué par une multiplication des cyberattaques. Ces cybercrimes sont souvent de nature transfrontalière et perpétré sous couvert d'anonymat. Malgré ces difficultés, plusieurs techniques sont utilisées pour tenter pour à identifier les cyberdélinquants.

---

[67] [https://www.kaspersky.fr/resource-center/definitions/white-hat-hackers] (Consulté le 1er octobre 2024).

[68] [https://www.cyber-securite.fr/hacker-definition-et-tout-savoir/] (Consulté le 1er octobre 2024).

[69] [https://www.malwarebytes.com/fr/cybersecurity/basics/hacker] (Consulté le 1er octobre 2024).

[70][https://www.legavox.fr/blog/laqueendupalais/lutte-contre-cybercriminalite-republique-democratique-32980.htm.] (Consulté le 2 octobre 2024).

a. Les données d'identification matérielles et personnelles

Dans le cadre d'une enquête sur la cybercriminalité, le procureur peut solliciter le concours des opérateurs et fournisseurs de communications électroniques afin de procéder à l'identification d'un utilisateur de ses services. En vue d'obtenir par exemple, les informations relatives à une ligne téléphonique, une adresse de courrier électronique, « une adresse IP »[71], un code « *IMEI* »[72] d'un téléphone, l'adresse « *MAC* »[73] d'un ordinateur, et cela conformément à l'article 15 du code du numérique qui dispose ce qui suit: « *Sont soumis au régime d'autorisation, les opérateurs et, ou fournisseurs de services numériques construisant des centres de données; les fournisseurs des services numériques de confiance qualifiée; les fournisseurs des services numériques essentiels; les fournisseurs des services d'hébergement d'applications, y compris celles financières; les plateformes numériques et les fournisseurs en position dominante œuvrant en République Démocratique du Congo ».*[74]

b. Les données de trafic et de localisation

Les données de trafic et de localisation aussi appelées données de connexion ou métadonnées sont un ensemble de données techniques liées à l'utilisation d'un terminal numérique connecté à un réseau de communication électronique ou à un fournisseur d'accès à internet.[75]

Les données de trafic permettent de renseigner sur l'utilisation technique du support numérique connecté à un réseau. Il s'agit notamment des factures détaillées, de l'annuaire téléphonique, des appareils utilisés, de l'historique d'envoi et de la réception des courriels, la liste des adresses IP. Les données de localisation quant

---

[71] L'Internet Protocol Address, abrégée en « adresse IP » ou tout simplement « IP », constitue la base du réseau Internet. Voir: https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quune-adresse-ip/.

[72] International Mobile Equipment Identity. L'IMEI est un numéro permettant d'identifier de manière unique les terminaux d'un téléphone mobile. Toute personne peut l'obtenir en composant le code : « *#06# » sur le clavier de son téléphone portable. Voir: https://www.futura-sciences.com/conso/questions-reponses/guides-telecoms-quest-ce-numero-imei-trouver-18358/.

[73] L'adresse MAC, également appelée adresse physique ou Media Access Control désigne une séquence composée de lettres et de chiffres codés sur 6 octets ou 48 bits. Elle fonctionne comme un numéro de série. Deux cartes réseau fabriquées le même jour de même marque auront par exemple une adresse MAC différente. L'adresse MAC permet d'identifier avec certitude une carte réseau. Cette adresse est généralement présentée au format hexadécimal avec les octets séparés par un double point, exemple:00:37:6C:E2:EB:62. Voir : https://www.jedha.co/formation-cybersecurite/adresse-mac.

[74] Article 15, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[75] [https://www.hal.science/hal-0740874] (Consulté le 20 Septembre 2024).

à elles, correspondent aux zones d'émission et de réception d'une communication. C'est un registre des appels ayant transité par une antenne relais. En informatique, on parle d'événements réseaux.[76]

Le juge cependant est compétent pour demander l'isolement de certaines données d'appel, par exemple, les différents numéros de téléphone composés ou reçus par un téléphone, leur durée, le moment de la prise de contact, etc. Il peut également par ce biais localiser le signal émis par un appareil en fonctionnement sans qu'une communication « ne soit émise ou reçue et ainsi, géolocaliser une personne.[77]

B. La volatilité des preuves

L'application du droit pénal en matière de cybercriminalité est rendue souvent complexe en raison de la volatilité des sites et des informations sur l'internet. C'est pour cette raison que les preuves doivent être saisies le plus rapidement possible pour éviter la nature volatile de la cybercriminalité. Les preuves numériques sont immatérielles et difficilement saisissables.

Les preuves numériques peuvent être constituées par de connexion coordonnées GPS, enregistrement de transaction, messages postés sur les réseaux sociaux.[78] Il est impossible d'assurer la totale sécurité car les informations sur internet passent par différentes infrastructures. La sécurité implique l'authentification, l'intégrité, la preuve.[79]La preuve en matière pénale vise à démontrer l'existence d'un fait au cours d'un procès. Elle est un élément capital en ce qu'elle a pour objectif de convaincre le juge. La preuve électronique est définie comme *« tout élément qui existe sous forme électronique, transitoire ou non*».[80]

La criminalistique numérique dispose cependant de nombreuses techniques lui permettant de récupérer ces informations. Par exemple à la réalisation de copies, d'informations stockées et effacées, au blocage de l'écriture empêchant la modification de l'information originale, ou encore au hachage cryptographique des

---

[76] M. AUDIBERT, « L'accès aux données de traffic et de localization dans le cadre d'une enquête judiciaire», [en ligne], in [https://www.lexbase.fr/article-juridique/87159156-focuslaccesauxdonneesdetraficetdelocalisationdanslecadreduneenquetejudiciaire#:~:text=Les%20donn%C3%A9es%20de%20trafic%20et%20de%20localisation%20aussi%20appel%C3%A9es%20donn%C3%A9es,fournisseur%20d'acc%C3%A8s%20%C3%A0%20internet.] (Consulté le 22 Septembre 2024).

[77] C. FORGET, « Revue du droit des technologies de l'information », - N° 66-67/2017, Bruxelle, p.40.

[78] H. MATSOUPOULOU, « Modalité de la preuve et transformations dans le recueil et l'administration de la preuve », *Archives de politique criminelle*, 2004, 1(n°26).

[79] K. NDUKUMA ADJAYI, *Liminaires du cours de droit du numérique*, Deuxième licence, UPC, 2018-2019, p. 48.

[80] DESCHAMPS et LAMBILOT, *Cybercriminalité: état des lieux*, *op.cit*., p. 74.

fichiers ou des signatures numériques.[81]Les dispositifs de cryptage de données permettent de coder les données avec des systèmes de chiffrement.

Section 2. La protection pénale des systèmes informatiques

La protection pénale du système informatique est devenue un enjeu crucial dans la société numérique. Les avancées technologiques ont considérablement modifié le mode de vie, rendant les systèmes informatiques indispensables au quotidien. C'est ainsi ces systèmes sont devenus des cibles privilégiées pour les cybercriminels. Cette section relève donc les principes généraux applicables à la cybercriminalité (§1) et les règles de procédure et de compétence (§2).

§1. Les principes généraux applicables à la Cybercriminalité

La loi pose quelques principes qui doivent guider la démarche de l'autorité judiciaire dans sa mission tels que le principe de la responsabilité pénale et des peines point (A) et les principes à la participation criminelle, à la tentative punissable, à la récidive et aux circonstances aggravantes point (B).

A. Le principe de la responsabilité pénale et des peines

Le principe de la responsabilité pénale est le fondement général de droit universellement admis en droit pénal interne qu'international, et cela en cas de violation d'une norme à laquelle sont attachées des sanctions. Nous allons voir premièrement le principe de la responsabilité pénale (1) et les peines (2)

1. Le principe de la responsabilité pénale

La responsabilité pénale est entendue comme l'obligation de répondre des infractions commises, c’est-à-dire, des comportements prohibés par la loi et passibles selon leur gravité d'une peine. Pour qu'il y ait responsabilité pénale, il faut donc l'existence de deux éléments dont la culpabilité et l'imputabilité.[82]

Il est de principe que les personnes morales ne peuvent déclinquer. Ce sujet suscite une grande controverse opposant les tenants de la thèse de la responsabilité pénale des personnes morales aux tenants des thèses de l'irresponsabilité pénale des personnes morales.

---

[81] *Idem,* p. 75.

[82] NYABIRUNGU MWENE SONGA, *« Traite de droit pénal général congolais »*, Deuxième édition, Editions Universitaires, Africaines, Collection Droit et Société, Kinshasa, 2007, p. 280.

Pour les tenants de la thèse de l'irresponsabilité pénale de la personne morale, l'accomplissement de l'infraction requiert une volonté coupable. Les êtres moraux, étant des fictions, ne peuvent déclinquer car elles sont dénuées de la capacité de vouloir.[83] Et les peines établies par la loi pour les personnes physiques sont de peines privatives et restrictives. Les appliquer à des personnes morales impliquent inévitablement la sanction des êtres physiques ce qui est contraire au principe de la personnalité des peines. D'après lequel la peine ne peut atteindre que celui qui a personnellement accompli l'acte délictueux.[84]

Par ailleurs, réfutant toute théorie de l'irresponsabilité pénale des êtres moraux, les partisans de la théorie en faveur de la responsabilité pénale des êtres moraux pensent que la délinquance des personnes morales, et plus généralement de tous les groupements pourvus d'une possibilité d'expression collective.[85]

Les personnes morales ne sont plus des êtres fictifs, mais qu'elles constituent une réalité juridique, qu'elles ont une volonté collective propre, distincte de celle de leurs membres et qu'elles engagent leur responsabilité civile.[86] Cette volonté est libérée à travers son assemblée générale, son conseil d'administration et son comité de gestion. Il existe une série de peines parfaitement adaptées à la nature de la personne morale. C'est le cas de l'amende, la dissolution ou la fermeture et la confiscation.

En droit congolais, Il est de principe que seules les personnes physiques peuvent déclinquer. La responsabilité des personnes morales est toujours discutée.[87] Les personnes morales sont irresponsables pour les infractions de droit commun, que pour les crimes contre la paix et la sécurité de l'humanité. En cas des faits infractionnels de leur part seuls les dirigeants, personnes physiques pourront répondre pénalement.[88]

De ce fait certaines lois fixent la responsabilité de personnes morales. Le code du numérique prévoit que pour l'Etat, les provinces, les entités territoriales décentralisées, les autorités administratives indépendantes et les établissements publics

---

[83] B. WANE BAMENE, *Cours de Droit Pénal Général*, 2013-2014, UPC, Kinshasa, p. 129.
[84] B. BOULOC, *Droit Pénal Général*, 25ème édition, Dalloz, Paris, 2007, N°327, p. 291.
[85] G. NGBANDA TE BOYIKOTE TENGE, *Manuel de Droit Pénal Général*, Editions CRIGED, Kinshasa, 2007, p. 131.
[86] B. BOULOC, *Droit Pénal Général*, *op.cit.*, p. 328.
[87] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, *op.cit.*, p. 159.
[88] *Idem*, p. 171.

n'engagent pas leurs responsabilités pénales. Ainsi ceux qui peuvent engager leur responsabilité individuelle, les agents de l'Etat ou fonctionnaires publics œuvrant pour l'Etat, les provinces, les entités territoriales décentralisées, les autorités administratives indépendantes et les établissements publics à condition que ces infractions commises dans l'exercice de leurs fonctions, soient reprimables par la présente ordonnance-loi.[89]

Le code du numérique prévoit également la responsabilité pénale des personnes morales de droit privé. Les personnes morales de droit privé, ce qui veut dire les dirigeants des personnes morales de droit privé engagent leur responsabilité lorsqu'elles commettent les infractions pour leur compte par l'un de leurs représentants dans les circonstances de l'exercice de leurs fonctions.[90]

2. Les peines

Dans le but de maintenir l'ordre social, l'Etat recourt à l'application des peines qui sont régit par le principe de la légalité des peines. La peine est définie comme un mal infligé à titre de punition par le juge au coupable d'une infraction. Elle se diffère d'une simple mesure administrative de la police, d'une réparation civile et elle peut avoir une fonction de vengeance, de prévention individuelle, éliminatrice ou même réparatrice.[91]

En droit pénal ordinaire les peines sont portées par les dispositions de l'article 5 du code pénal congolais qui dispose : *les peines applicables aux infractions sont : la mort, les travaux forcés, la servitude pénale, l'amende, la confiscation spéciale, l'obligation de s'éloigner de certains lieux ou d'une certaines région, la résidence imposée dans un lieu déterminée, la mise à la disposition de la surveillance du gouvernement.*[92]

Bien que la peine soit inséparable de l'idée de souffrance, la sanction pénale est censée remplir plusieurs fonctions dont la fonction rétributive ; celle qui vise à faire payer le délinquant pour le mal infligé à la société par son acte criminel et la fonction préventive ; celle qui concerne d'une part la prévention individuelle et d'autre part la prévention générale.[93]

---

[89] Article 308, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[90] Article 309, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[91] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, *op.cit.* , p. 237.

[92] Article 5, Décret du *30* Janvier 1940 portant code Pénal Congolais tel que modifié à ce jour, in J.O 45ème numéro Spécial 30 Novembre 2004.

[93] NYABIRUNGU MWENE SONGA, *Droit pénal général congolais, op.cit.,* p.295.

Pour les infractions relatives à la cybercriminalité, les peines applicables sont la servitude pénale, l'amende et la confiscation spéciale. Pour les personnes morales, la peine peut être une amende dont le montant maximum vaut 5 fois plus que celui prévu pour les personnes physiques. La dissolution pour les infractions portant atteinte à la sécurité et sûreté de l'Etat, l'interdiction définitive ou pour une durée de deux à cinq ans d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales. La fermeture définitive ou pour une durée de deux à cinq ans d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés, l'exclusion définitive des marchés publics pour une durée de deux à cinq ans et la confiscation de l'outil qui a servi à commettre l'infraction.[94]

B. Les principes relatifs à la participation criminelle, à la tentative punissable, à la récidive et aux circonstances aggravantes

Le phénomène criminel s'adapte continuellement dans la vie sociale, les délinquants ressentent le besoin d'organiser leurs activités au sein des collectivités. Cela leur permet de gagner du terrain en formant une collectivité puissante. Pour comprendre comment contrarier leurs actes, nous allons aborder sur la participation criminelle (1) et les cas de récidivité aux circonstances aggravantes (2).

1. La participation criminelle et la tentative punissable

En droit congolais, la participation criminelle trouve son siège dans le code pénal congolais dans ses articles 21 à 23. En réalité, la commission d'une infraction est souvent l'œuvre de plusieurs personnes. Et pour que la participation criminelle soit retenue à titre de complicité, il faut qu'il ait l'existence d'une infraction principale, un acte de participation et l'élément moral ou intention criminelle.[95]

On ne peut parler de la participation criminelle dans le chef de celui qui vient au secours de son prochain injustement agressé. Il en est de même de celui qui apporte son aide à un individu qui se suicide.[96]

La tentative punissable est une activité complexe parfois longue qui conduit le délinquant à poser des actes par les moyens matériels et humains permettant à la réalisation d'une infraction. Cette institution a été imaginée pour faire face à la

---

[94] Article 311, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[95] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, *op.cit.*, p. 174.

[96] G. STEFANI, G. LEVASSEUR et B. BOULOC, *Droit pénal général*, 11e éd., Dalloz, Paris, 1980 et 13e éd., 1987, p. 257.

situation créée par l'agent dont l'activité criminelle avancée voir même achevée, mais qui n'a pas conduit au résultat escompté.[97]

Il y a tentative punissable lorsque la résolution de commettre l'infraction a été manifestée par des actes extérieurs, qui forment un commencement d'exécution de cette infraction et qui n'ont été suspendus ou qui n'ont manqué leur effet que par des circonstances indépendantes de la volonté de l'auteur. Elle est punie de la même peine que l'infraction consommée.[98] De cette définition légale ressort deux formes de la tentative punissable :

- Celle qui manque son effet parce qu'elle a été interrompue par une cause extérieure. Il s'agit d'une infraction tentée, cette infraction existe lorsque l'exécution des actes matériels consommant l'infraction est interrompue par suite des circonstances indépendantes de la volonté de l'auteur.[99]
- Ensuite celle qui manque son effet alors que tous les actes d'exécution ont été commis. L'infraction impossible peut être définie comme étant celle dont le résultat recherché par l'auteur n'a pu être atteint soit par manque d'objet, soit par inefficacité des moyens utilisés.[100]

Le code pénal qualifie de complice, celui qui donne des instructions pour la commission de l'examen, les armes, des instruments ou tout autre moyen, aide le criminel en connaissance de sa conduite.[101] Toute participation ou tentative violation contre les prescrits de les infractions réprimés par le code du numérique sont punissable conformément au code pénal congolais.[102] Les complices d'une infraction sont punis d'une peine qui ne dépassant pas la moitié de la peine de l'auteur de l'infraction. Et lorsque cette peine est la mort ou la servitude pénale à perpétuité, la peine applicable au complice est là servitude pénale de dix à vingt ans.[103]

2. La récidive et les circonstances aggravantes

La réitération de l'infraction est une circonstance qui justifie l'aggravation de la peine. Selon les théoriciens de l'école classique, si la première condamnation n'a pas réussi à corriger le délinquant, ce qu'il en résulte qu'elle n'était pas efficace. Pour

---

[97] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, op.cit., p.136.
[98] Article 4, Décret du 30 Janvier 1940, préc.
[99] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, *op.cit.*, p.137.
[100] *Idem*, p.145.
[101] Article 22, Décret du 30 Janvier 1940, préc.
[102] Article 315, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[103] Article 23, Décret du 30 Janvier 1940, préc.

le positiviste, la récidive ne devrait pas être plus sévèrement punie, il faut préconiser les mesures de sûreté.[104]

La loi congolaise ne définit pas la récidive. La définition est l'œuvre de la doctrine qui enseigne qu'il s'agit de la rechute dans l'infraction selon les conditions légalement déterminées et après une ou plusieurs condamnations coulées en force de la chose jugée.[105] Elle constitue un problème pénal du fait que les sanctions prises à l'égard du délinquant n'ont pas été efficaces.

La réitération de l'infraction est une circonstance qui justifie l'aggravation de la peine. Le code du numérique prévoit que lorsque les infractions commises dans les Cinq ans qui suivent le prononcé de la condamnation devenue irrévocable ou les infractions commises par un membre d'une organisation criminelle, une bande organisée ; la peine prévue par la loi est doublée, le maximum de la servitude pénale ne pouvant dépasser vingt ans.[106]

Et si ces infractions porte atteinte à la sûreté de l'Etat, des données informatiques et, ou aux systèmes informatiques liés à des infrastructures et applications stratégiques ou sensibles, la peine prononcée est la servitude pénale à perpétuité et une amende d'un milliard à vingt milliards de Francs congolais. [107]

§2. Les règles de procédure et de compétence des juridictions

Le bon déroulement de toute activité judiciaire repose sur un ensemble des normes précises. Par ce paragraphe, nous allons analyser deux points essentiels dont le premier touche les règles de procédure des juridictions (A), ensuite les règles de compétences des juridictions (B).

A. Les règles de procédure

Les règles fixées par la loi et la jurisprudence ont pour objectif de garantir un procès équitable pour toutes les parties. A propos des règles des procédures des juridictions, nous parlons de la constatation des infractions (1) et de l'interception des données numériques (2).

---

[104] R. NYABIRUNGU MWENESONGA, S. BOKOLOMBE et R-B MANISA, Droit pénal général congolais, *op.cit.*, p. 262.
[105] *Idem,* p. 261.
[106] Article 316, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[107] Article 317, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

1. La constatation des infractions et la perquisition des données stockées dans un système informatique

La constatation des infractions cybercriminelles s'effectue par les officiers de la police judiciaire à compétence restreinte ou à compétence générale. Ces derniers ont l'obligation d'informer le fait infractionnel à l'officier du ministère public compétent.[108] Ces faits sont constatés dans des procès-verbaux établis conformément au code de procédure pénale.[109]

Sur le territoire national, l'officier du Ministère Public a l'habilité d'opérer une perquisition ou accéder à un système informatique, lorsque les données que contient ce système est important pour une enquête. Et si ces données sont situées à l'extérieur du territoire congolais, l'officier du Ministère Public les obtient par voie de commission rogatoire internationale.[110] Et lorsque la saisie de ces supports par l'officier du Ministère Public ne parait pas souhaitable, ils sont copiés sur des supports de stockage informatique pouvant être saisis et placés sous scellés.[111]

2. L'interception des données numériques

L'officier du ministère public peut prescrire l'interception des données numériques telles que : l'enregistrement et la transcription de correspondances, lorsque les nécessités de l'information l'exigent. L'interception est autorisée par décision du Procureur General près la Cour d'Appel, saisi par réquisition du Magistrat poursuivant, le Bâtonner national informé ou le Bâtonnier selon le cas.[112]

L'Agence Nationale de Cybersécurité autorise aussi les interceptions de correspondances émises par la voie des communications électroniques ainsi que la conservation et la protection de l'intégrité.[113] Toutes ces opérations engagées par l'Agence Nationale de Cybersécurité sont faites dans le but:

- du maintien de la souveraineté nationale, de l'intégrité du territoire ou de la défense nationale;
- de la préservation des intérêts majeurs de la politique étrangère de la République Démocratique du Congo;

[108] Article 318, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[109] Article 319, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[110] Article 320, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[111] Article 321, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[112] Article 322, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[113] Article 323, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

- de la sauvegarde des intérêts économiques, industriels et scientifiques majeurs de la République Démocratique du Congo ;
- de la prévention du terrorisme, des violences collectives de nature à porter gravement atteinte à l'ordre public ou de la criminalité et de la délinquance organisées. [114]

B. Les règles de compétence

La commission d'une infraction trouble l'ordre social établi par l'Etat, et nécessite l'intervention des autorités judiciaires en vue de rétablir la paix dans la société au moyens des organes répressifs. Le législateur pose les règles des poursuites ainsi que l'extinction de l'action publique (1) et met en place les juridictions compétentes à la législation numérique (2).

1. Les poursuites et l'extinction de l'action publique

A ce niveau de notre réflexion, il est question d'exposer d'une manière générale les poursuites, ainsi que l'extinction de l'action publique dans le domaine de la cybercriminalité.

a. Les poursuites

Le code numérique prévoit dans son article 325 que « *Les infractions à la législation du numérique que sont poursuivies conformément au Code de procédure pénale et prouvées par toute voie de droit* ». L'action publique a pour but la répression de l'infraction ayant porté atteinte à l'ordre social et pour objet l'application d'une peine ou une mesure de sûreté au délinquant. C'est ainsi exercer l'action publique, c'est saisir les tribunaux répressifs en vue de faire punir le coupable.[115]

La plénitude de l'exercice de l'action publique appartient au procureur général près la cour d'appel. Le procureur général exerce les fonctions du ministère public près toutes les juridictions établies dans le ressort de cours d'appel.[116] Le Ministère Public a le droit et le devoir d'exercer des poursuites, chaque fois qu'une infraction est portée à sa connaissance sauf dans certains cas. Son pouvoir se trouve parfois paralysé, soit limité pour diverses raisons notamment: La qualité de l'inculpé,

---

[114] Article 324, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[115] L. LUZOLO BAMBI, S. MAKAYA KIELA, *Eléments de procédure pénale manuel d'enseignement*, 1ère édition, centre de recherche sur la justice, justice transitionnelle et justice pénale internationale (CRJT), Kinshasa, 2020, p. 28.

[116] *Idem*, p.29.

les poursuites conditionnées (exemple l'adultère, grivèlerie, les infractions commises à l'étranger passible d'une peine d'emprisonnement d'au moins 5 ans, les infractions de droit d'auteur etc.) ainsi que l'autorité du Ministère de la justice sur les magistrats du parquet.[117]

b. L'extinction de l'action publique

L'extinction de l'action publique constitue un obstacle permanent empêchant de saisir définitivement les juridictions compétentes. L'action publique peut s'éteindre par le décès du délinquant, l'amnistie, le retrait de la plainte, la dépénalisation etc.[118]

La prescription est un droit accordé par la loi à l''auteur d'une infraction de ne pas être poursuivi depuis la perpétration du fait après l'écoulement d'un certain laps de temps déterminé par la loi.[119] L'action publique peut s'éteindre aussi lorsqu'elle n'est pas exercée pendant un certain délai c'est à dire elle s'éteint par l'effet de la prescription.

Le code du numérique dispose que l'action publique en répression des infractions à la législation du numérique se prescrit conformément au Code de Procédure Pénale congolais. Les délais de prescription commencent à courir du jour de la commission du fait infractionnel ou, s'il a été dissimulé, du jour de sa découverte ou de sa révélation.[120] L'idée de la prescription est d'éviter le dépérissement de la preuve parce que plus le temps passe, plus il est difficile de trouver les preuves et de rétablir l'ordre lésé.

2. Les juridictions compétentes à la législation numérique

Les règles de compétence et de procédure applicables aux infractions à la législation du numérique sont celles prévues respectivement par la loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétence des juridictions de l'ordre judiciaire et le Code de procédure pénale.[121]

---

[117] *Idem,* pp. 30 à 37.

[118] *Idem,* p. 38.

[119] G. MINEUR, *Commentaire du code pénal congolais*, 2ème éd.58 p. 96) (Voir R. Merle et A. VITU : traité de droit criminel Tome II 2ème éd. n°842.).

[120] Article 327, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[121] Article 328, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

Le tribunal de commerce est compétent pour toutes les infractions à la législation numérique portent atteinte à la législation économique et commerciale quel que soit le taux de la servitude pénale ou la hauteur de l'amende. Les juridictions prévues par la loi organique n°13/011-B du 11 avril 2013 précitée sont compétentes lorsque :

- L'infraction a été commise sur internet sur le territoire de la République Démocratique du Congo lorsque le contenu illicite est accessible depuis la République Démocratique du Congo;
- La personne physique ou morale s'est rendue coupable, sur le territoire de la République Démocratique du Congo, comme complice d'une infraction commise à l'étranger si l'infraction est punie à la fois par la loi congolaise et par la loi étrangère ;
- L'infraction a été commise par des Congolais hors du territoire de la République Démocratique du Congo et que les faits sont punts par la législation du pays où ils ont été commis.[122]

[122] Article 329, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

CHAPITRE II. LE CADRE DE RÉPRESSION DE LA CYBERCRIMINALITÉ

La cybercriminalité est une délinquance qui correspond, non seulement aux infractions strictement informatique, mais qui vise aussi l'ensemble du champ pénal. En allant des escroqueries, aux fraudes, en passant par l'usurpation d'identité, la pornographie enfantine, etc. Ainsi que tout acte malveillant s'opérant dans le cyberespace.

Dans le présent chapitre, il est question d'examiner minutieusement le cadre juridique de la lutte contre la cybercriminalité, en analysant les enjeux des qualifications légales (section 1) et aussi les organes répressifs de cybersécurité (section 2).

Section 1. Les enjeux des qualifications légales de la cybercriminalité

Le cyberespace apparaît comme une zone dangereuse où rodent les entités agressives et mystérieuses. Il est autant une menace pour les usagers que pour les systèmes informatiques. Ce qui justifie la commission de plusieurs actes criminels attentifs non seulement aux personnes physiques mais également aux équipements informatiques.

Cette section aborde alors l'étude des infractions de droit commun (§1), ainsi que les atteintes aux systèmes informatiques et les infractions liées à l'utilisation des données à caractère personnel (§2).

§1. Les infractions de droit commun

Le décret du 30 janvier 1940 portant code pénal congolais reste applicable à plusieurs comportements cybercriminels. Le code pénal congolais incrimine certains comportements manifestés lors de l'utilisation des nouvelles technologies de l'information et de la communication.

La cybercriminalité n'est pas faite que d'incriminations nouvelles. Le code pénal congolais reste efficace pour les infractions classiques qui trouvent particulièrement la facilité de commission grâce aux NTIC.

Il existe toute une catégorie des infractions en droit commun mais dans ce paragraphe, nous allons voir les infractions telles que la pornographie enfantine et

l'outrage aux bonnes mœurs (A) ainsi que l'injure publique et l'escroquerie sur internet (B).

A. La pornographie et l'outrage aux bonnes mœurs

L'internet a accru de façon exponentielle permettant d'accéder à des contenus sexuellement explicites mettant ainsi la pornographie à la portée de tout le monde, y compris les enfants et les adolescents.[123]

a. La pornographie enfantine

Les contenus à caractère sexuel sont parmi les premiers contenus commercialisés sur internet. On entend par pornographie enfantine toute représentation, par quelque moyen que ce soit d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées ; ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles.[124] Voici donc deux d'éléments constitutifs de ce délit:

- Eléments matériels : Les éléments matériels de cette infraction facilité par les TIC consiste par le fait « *de produire, de distribuer, de diffuser, de vendre, de se procurer...tout matériel mettant en scène un enfant* »[125]
- Elément moral : C'est l'intention qu'a l'agent sur l'enfant à des fins sexuelles.

Une servitude pénale est prévue dans l'article sus-évoqué, d'une peine de cinq à quinze ans principales et d'une amende de deux cents mille à un million des Francs congolais.[126]

b. L'outrage aux bonnes mœurs

L'outrage aux bonnes mœurs trouve son siège à l'article 175 Al 1 du décret du 30 janvier 1940 portant code portant code pénal congolais qui prévoit ce qui suit : « *Quiconque aura exposé, vendu ou distribué des chansons, pamphlets ou autres écrits, imprimés ou non, des figures, images, emblèmes ou autres objets contraires aux bonnes mœurs, sera condamné à une servitude pénale de huit jours à un an et à une amende de vingt-cinq à mille zaïres ou à l'une de ces peines seulement* ». L'outrage

---

[123] JANET ZACHARIAS, *La pornographie – un enjeu de santé publique, IA, B. Sc.Inf.*, 7 février 2017, p. 1.
[124] Article 179 alinéa 2, Loi n°09/001 du 10 janvier 2009 portant protection de l'enfant.
[125] Article 357, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[126] *Idem*, ordonnance loi n◦23/010 du 13 mars 2023, préc.

aux bonnes mœurs consiste à l'exposition ou publication sur internet des images obscènes et ou immorales.[127]

Cette infraction existe lorsque dans le chef de l'agent l'on parvient à prouver le caractère contraire aux bonnes mœurs. Le législateur tient à protéger ici des mœurs de la personne humaine.[128] L'infraction d'outrage aux bonnes mœurs peut se réaliser par divers faits notamment :

- L'élément matériel : premièrement l'outrage aux bonnes mœurs peut se commettre par écrit ou objet quelconque. Il peut s'agir des affiches, photographies, gravures, peintures, films pornographiques.[129] Deuxièmement les outrages par la parole car la loi punit quiconque aura chanté, lu, récité, fait entendre ou proféré des obscénités dans des réunions ou lieux publics devant plusieurs personnes et de manière à être entendu de ces personnes.[130]
- L'élément moral de l'outrage aux bonnes mœurs : consiste du fait que l'agent doit agir avec une intention coupable c'est-à-dire par désir ou la volonté d'outrager les mœurs et cela peu importe le mobile.[131]

De ce fait, l'exposition ou la publication sur internet des images obscènes ou immorales peut être sanctionnée d'une peine de servitude pénale de huit jours à un an et une amende équivalente de vingt-cinq mille Zaïres sur base de l'article 175 du code pénal.

B. L'injure publique et l'escroquerie sur internet

L'avènement du numérique a considérablement modifié les contours de la vie sociale. Il y a des ces infractions qui étaient traditionnellement associée à des propos diffamatoires, tenus en face-à-face ou dans des publications imprimées. Aujourd'hui, ces infractions se sont étendues à l'espace virtuel. En RDC. Le droit a dû s'adapté à cette nouvelle réalité.

1. L'injure publique

---

[127] K. NDUKUMA ADJAYI, A. DIANGIENPA MVETE, B. LOSEKA RAMAZANI et al., *Droit du commerce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité et déterritorialité*, Harmattan, Paris, p.342

[128] B. WANE BAMEME, *Cours de droit pénal spécial*, Kinshasa, 2022, p. 254.

[129] *Idem*, p. 255.

[130] Article 175 alinéas 4, Décret du 30 Janvier 1940, préc.

[131] B. WANE BAMEME, *Cours de droit pénal spécial*, *op.cit.*, p. 256.

L'injure publique est le fait d'offenser une personne par des expressions blessantes, outrageantes, par mépris ou invectives. La loi condamne quiconque aura publiquement injurié une personne d'une servitude pénale de huit jours à deux mois et d'une amende n'excédant pas l'équivalent de cinq cents zaïres.[132] Elle ne peut exister que si elle est perpétrée « publiquement » contre les particuliers et proférée à l'encontre d'un être humain.[133]

Le code pénal congolais ne donne pas la définition de la publicité, il faut comprendre par l'injure un acte posé en présence de plusieurs personnes. En ce qui concerne ses éléments constitutifs l'injure publique comprends :

- L'élément matériel : le fait d'avoir tenu des propos par parole ou par chanson, couché des écrits, affiché des images constitue son élément matériel. L'infraction de l'injure publique se réalise donc par déclaration verbale, gestuelle ou écrit et non par une quelconque agression physique.
- L'élément moral : le fait d'injurier une personne suppose que l'agent a conscience de son acte de nature à offenser ou à blesser une personne.[134]

2. L'escroquerie sur internet

L'internet a facilité le passage des escrocs. Issue de la compréhension de l'article 98 du code pénal congolais, l'escroquerie est « *le fait de se faire remettre volontairement une chose appartenant à autrui, soit en faisant usage d'un faux nom ou d'une fausse qualité soit en employant des manœuvres frauduleuses*».[135]

C'est un mécanisme par lequel une personne obtient frauduleusement la remise d'une, à l'aide d'une tromperie. L'infraction de l'escroquerie requiert les conditions préalables ci-après :

- La chose, objet de la remise, telle que précisée à l'article 98 code pénal congolais les procédés frauduleux doivent avoir pour objet la remise de la chose. Il peut s'agir des fonds, meubles, obligations, chose corporelle, matérielle, etc.
- L'appartenance de la chose à autrui, pour que l'infraction de l'escroquerie soit retenue, il s'impose d'apporter la preuve de l'appartement de la chose à autrui ;

---

[132] Article 75, Code pénal congolais, préc.
[133] B. WANE BAMEME, *Cours de droit pénal spécial, Op.Cit.*, p.166.
[134] B. WANE BAMEME, *Cours de droit pénal spécial, Op.Cit.*, p.167.
[135] *Idem*, p.283.

- L'emploi de moyen frauduleux, qui généralement peuvent être un mensonge, de l'usage de faux noms, l'usage d'une fausse qualité ou des manœuvres frauduleuses, ou encore une tromperie en vue d'obtenir la chose.[136]

Pour ce qui est de ses éléments constitutifs, nous retenons :

- L'élément légal : l'escroquerie se réalise matériellement par le fait de se faire remettre ou délivrer la chose d'autrui. Il faut que l'agent se soit fait remettre la chose convoitée d'où il n'y a pas d'escroquerie en cas d'abstention, d'omission ou d'inaction.
- L'élément moral : l'escroquerie n'est pas une infraction par imprudence, la mauvaise foi doit exister. L'agent agit premièrement avec une intention coupable de fraude c'est-à-dire avec volonté et conscience de s'approprier d'une chose appartenant à autrui. Et deuxièmement l'agent doit avoir agi en recherchant le résultat du dol spécial.[137]

De ce fait, l'article 98 précité punit d'une servitude pénale de trois mois à cinq ans et d'une amende dont le montant ne dépasse pas deux mille zaïres l'auteur de cette infraction.

§2. Les atteintes aux systèmes informatiques et les infractions liées à l'utilisation des données à caractère personnel

Dans cette sphère, la cybercriminalité recouvre un éventail d'inconduites dont l'existence est entièrement dépendante de celle des réseaux. Cette typologie vise les atteintes aux systèmes informatiques (A) et les infractions liées à l'utilisation des données à caractère personnel (B).

A. Les atteintes aux systèmes informatiques

Les plus grandes menaces du monde numérique actuel restent les atteintes aux systèmes informatiques. Que ce soit pour les entreprises ou les individus, tout le monde est susceptible d'être victime.

1. La Fraude informatique

[136] *Idem,* p.286.
[137] *Idem*, p. 289.

La fraude informatique est le fait de se procurer par soi-même ou pour autrui un avantage quelconque de manière frauduleuse dans tout ou une partie d'un système informatique.[138] La fraude informatique est différente de l'escroquerie en ce qu'elle résulte de manipulation illicites de données sur une machine alors que l'escroquerie porte essentiellement atteinte à la confiance de tiers. [139]

La fraude informatique est l'un des délits les plus courants sur internet car elle peut être automatisée et réalisée avec des logiciels permettant au fraudeur de cacher son identité. Cette infraction est punie d'une servitude pénale cinq à dix ans et d'une amende de cinquante à cent millions de Francs congolais. Dans le chef de toute personne modifie, altère ou efface des données qui sont stockées, traitées ou transmises par un système informatique. Ou bien s'il perturbe le fonctionnement normal d'un système informatique.[140]

2. L'accès et le maintien illégal au système informatique

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système automatisée de données est une infraction prévue par l'article à l'article 332 à 333 du code du numérique. Elle vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données «*STAD*».[141]

L' infraction de l'accès et le maintien illégal du système informatique a pour vocation de sanctionner les cyberdélinquants qui cherchent à prendre connaissance d'informations, confidentielles ou non, figurant dans des système de données dont l'accès ou la présence leur est interdit.[142] Elle requiert pour sa qualification des éléments strictement constitutifs dont l'élément matériel et intentionnel.

- L'élément matériel Cette infraction pose la condition préalable pour être retenue dans le chef du délinquant, la pénétration obligatoire du STAD. Sous cette condition le législateur retient à titre d'actes matériels, l'instruction ou

[138] K. NDUKUMA ADJAYI, DIANGIENPA MVETE, LOSEKA RAMAZANI et al et al. *Droit du commerce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité et déterritorialité, op.cit.,* p. 326.
[139] F. DECHAMPS et C. LAMBILOT, *Cybercriminalité état des lieux,* Athemis, Bruxelles, 2016, p. 31.
[140] Article 340, Ordonnance loi n◦23/010 du 13 mars 2023, préc.
[141] E. MATIGNON, *La Cybercriminalité : Focus dans le monde des télécoms*, Mémoire, Université Paris 1 Panthéon -Sorbonne, sous-direction de William GILLES, Paris, 25 juin 2012, p. 13.
[142] *Idem*, p.14.

l'acte de se maintenir dans une partie ou dans tout le système informatique.[143] Par accès il faut entendre, la connexion directe ou indirecte dans l'intégralité ou dans une partie quelconque d'un système informatique via un réseau télécommunication électronique.[144] Le maintien résultats de plusieurs situations juridiques notamment celle où la personne ayant une autorisation d'accès à une partie du système en profite pour accéder et s'y maintenir sans autorisation. C'est aussi le fait pour une personne d'entrer dans le système par erreur ou par hasard qui s'y maintient sachant qu'elle n'a pas le droit.[145]

- L'élément intentionnel : Il est nécessaire de démontrer le caractère intentionnel de l'intrusion illégale. L'accès peut résulter d'une erreur par le simple fait de se maintenir dans le système informatique ceci pourra constituer d'une fraude. L'auteur de l'acte doit agir volontairement en connaissance de cause pénétrer ou maintenir dans un système informatique sans autorisation.[146] Le code du numérique condamne premièrement toute personne accède ou se maintient intentionnellement et sans droit dans l'ensemble ou partie d'un système informatique d'une peine de servitude pénale de trois à cinq ans et d'une amende de cinquante millions a cent millions de francs Congolais avec une intention frauduleuse. Deuxièmement celui qui agit avec intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès légal à un système informatique d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinquante millions à cent millions de francs congolais.[147]

B. Les infractions liées à l'utilisation des données à caractère personnel

À l'ère des avancées des technologies de l'information et de la communication (NTIC), la cybercriminalité connait elle aussi une progression notable. Le numérique nous a facilité l'accès aux données, elle a rendu notre vie privée ainsi que notre sécurité plus vulnérable, et nos données personnelles encore plus exposées, ce qui peut engendrer un usage parfois abusif et qui peuvent être bafouées en pratique. Le cyberespace, est devenue le domaine privilégié de la délinquance, de ce fait, la

---

[143] M. BODELET MARCEL, D*roit pénal congolais face aux nouvelles technologies de l'information et de la communication*, Travail de fin de cycle, Université protestante au Congo, sous-direction du Professeur K. NDUKUMA ADJAYI, Kinshasa, 2022-2023, p. 33.

[144] Article 2 point 1, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[145] M. BODELET MARCEL, *Droit pénal congolais face aux nouvelles technologies de l'information et de la communication, op.cit.*, p.34

[146] *Ibidem*

[147] Article 332, Ordonnance loi n°23/010 du 13 mars 2023, préc.

protection pénale des données à caractère personnel s'inscrit dans le cadre de la lutte contre la cybercriminalité multiforme et amène donc à envisager la protection des données personnelles dans plusieurs domaines.

1. L'envoi de messages non sollicités

Tout message électronique non sollicite envoyé sur base de la collecte de données à caractère personnel doit contenir un lien pouvant permettre au bénéficiaire de se désabonner. Le non-respect de cette disposition expose le contrevenant à une amende de cinq cent mille à deux millions de francs congolais.[148]

2. L'usurpation d'identité

L'usurpation d'identité numérique consiste à s'emparer frauduleusement d'éléments permettant de déterminer à la fois l'unicité et l'authenticité d'une personne.[149] Ce phénomène s'est multiplié au cours de ces dernières années grâce à l'utilisation des réseaux informatiques deux façons. D'une part, dans le but de se faire passer pour quelqu'un d'autre et d'autre part dans le but illégal de rechercher de profit économique.[150]

C'est ainsi que la loi punit quiconque qui s'approprie d'une chose appartenant à autrui dans le but de s'approprier une chose appartenant à autrui, s'est fait remettre ou délivrer des fonds, meubles, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses dans le but de le persuader.[151]

L'auteur de cet acte est puni d'une servitude pénale de trois mois à cinq ans et d'une amende dont le montant ne dépasse pas deux mille zaïres. Le code de la famille condamne également l'usurpation volontaire et continue du nom d'un tiers d'une peine de sept jours à trois mois de servitude pénale et de 50 à 100 Zaïres d'amende.[152]

La répression spécifique de l'usurpation d'identité sur internet semble importante pour sanctionner l'usage frauduleux de l'identité d'une personne. C'est ainsi

---

[148] Article 348, Ordonnance loi n°23/010 du 13 mars 2023, préc.

[149] K. NDUKUMA ADJAYI et al, *Droit du commerce électronique : enjeux civils, consuméristes, cybercriminel, d'extranéité et de territorialité, op.cit*., p. 343.

[150] M. QUEMENER et J. FERRY, *Cybercriminalité : Défi mondiale*, 2ème Ed, Economica, Paris, p. 117.

[151] Article 98, Décret du 30 janvier 1940 portant code pénale.

[152] Article 69, Loi n◦16/008 du 15 juillet 2016, modifiant et complétant la loi n°87/010 du 1er aout 1987 portant Code de la famille.

le code du numérique sanctionne quiconque qui usurpe par hameçonnage, phishing ou tout autre moyen, intentionnellement et sans droit par le biais d'un système informatique, l'identité d'autrui.[153]

Cette infraction se caractérise par deux éléments strictement constitutifs. D'une part, un élément matériel, qui réside dans le fait pour un cyberdélinquant d'usurper l'identité d'un tiers par les biais d'un système informatique.[154] Et d'autre part, un élément intentionnel caractérisé par l'intention de troubler la tranquillité, porter atteinte à l'honneur ou à la considération d'un individu. L'auteur doit être sanctionné d'une servitude pénale d'un an à cinq ans et d'une amende de vingt millions à cent millions de Francs congolais.

Section 2. Les Organes répressif de cybersécurité

Face aux cyberdélits, des nombreux pays, y compris la RDC, ont mis sur pied des organes répressifs spécialisés dans la lutte contre la cybercriinalité. Ces structures ont pour missions de prévenir, d'enquêter et de poursuivre les auteurs d'actes illégaux commis dans le cyberespace. Pour ce faire, nous abordons deux paragraphes dont le premier décrit l'agence nationale de cybersécurité et les organes policiers de repression de la cybercriminalité (§1), et le second présente les faiblesses de la legislation congolaise face aux aspects de la cybercriminalité (§2).

§1. L'agence nationale de cybersecurité (ANCY) et les organes policiers de répression de la cybercriminalité

Pour remédier au fléau de la cybercriminalité en RDC, l'Etat Congolais a mis en place une agence nationale de la cybersécurité (ANCY), aussi au niveau de la Police Nationale Congolaise, une direction consacrée aux Telecoms et NTIC. Dans un cadre répressif, nous allons exploiter les différentes missions et attributions de ces organes en vue de comprendre leur apport dans la lutte contre la cybercriminalité.

A. L'Agence Nationale de cybersécurité (ANCY)

L'Agence Nationale de cybersécurité est l'autorité nationale en charge de la cybersécurité et de la sécurité des systèmes informatiques en RDC.[155] L'ANCY est

[153] Article 351, Ordonnance loi n◦23/010 du 13 mars 2023, préc.

[154] MATIGNON E., *La Cybercriminalité : un focus dans le monde des télécoms*, Mémoire, sous-direction de William GILLES, Université Paris 1 Panthéon -Sorbonne, Paris, 2011-2012

[155] Article 274, Ordonnance loi n°23/010 du 13 mars 2023, préc.

un organisme public doté de la personnalité juridique et elle relève de l'autorité du Président de la République.[156]

1. Le fonctionnement de l'ANCY

Elle collabore de manière transversale notamment avec les Ministres ayant dans leurs attributions l'intérieur et la sécurité, la justice, la défense, les droits humains, la poste et les télécommunications, le numérique ainsi que la recherche scientifique et l'innovation technologique.[157]

Elle a pour fonction d'assure la régulation en matière de cybersecurité, la conformité et l'audit des systèmes informatiques ainsi que des réseaux de communication électronique, l'homologation des prestataires de services et produits de cybersécurité. L'ANCY reçoit des informations de la part de l'exploitant d'un système informatique de toutes les attaques, intrusion et pénétrations susceptibles d'entraver le fonctionnement d'un autre système informatique en vue de prendre les mesures nécessaires pour y faire face.[158]

Elle oriente la stratégie nationale de cybersécurité et propose la politique de sécurité des systèmes informatiques de l'État. Et apporte son expertise et son assistance technique aux administrations ainsi qu'aux entreprises tant publiques que privées dans le but de renforcer les infrastructures critiques et essentielles et des opérateurs d'importance Vitale.[159]

2. Les missions de l'ANCY[160]

L'Agence nationale de la cybersécurité est chargée, en coordination avec les différentes structures impliquées dans le domaine, de la supervision de la sécurité des systèmes d'information et de communication des structures publiques et privées de l'espace cybernétique national.

Elle a pour mission notamment de piloter, coordonner et suivre la mise en œuvre de la Stratégie Nationale de cybersécurité.

L'ANCY met en place des mesures de prévention, de protection et de défense des données. Mais aussi des infrastructures critiques et essentielles ainsi que

[156] Article 275, Ordonnance loi n°23/010 du 13 mars 2023, préc.
[157] Présidence, Stratégie nationale de cybersécurité de la RDC, la commission technique pour la cybersécurité (CTC), Kinshasa, 2022, p.25.
[158] Article 276, ordonnance loi n°23/010 du 13 mars 2023, préc.
[159] Article 277, ordonnance loi n°23/010 du 13 mars 2023, préc.
[160] Article 278, ordonnance loi n°23/010 du 13 mars 2023, préc.

celles des réseaux de communications électroniques face aux risques de cybermenaces en République Démocratique du Congo.

Elle s'occupe également de la gestion des risques au niveau national, ainsi que des mesures de cyber-résilience dans la gestion des cyber-incidents. L'ANCY établi la conformité des procédures de cybersécurité pour les organismes et institutions publiques. Dans le but de garantir le mécanisme d'inclusion nationale des différentes parties prenantes à la mise en œuvre de la stratégie nationale de la Cybersécurité.

Pour l'identification des cybercriminels, l'ANCY travaille en collaboration avec les Ministères et les régulateurs sectoriels, les organismes à importance vitale et les services essentiels, et s'assurer de leur mise à jour. Permettant ainsi de suivre les indicateurs de performances en matière de Cybersécurité et sécurité des systèmes informatiques. Elle est l'organe chargée d'établir et de maintenir les bases de données des cyber-vulnérabilités et de participer au développement de la confiance numérique.

L'ANCY se charge de l'audit et la veille technologique des systèmes informatiques et des réseaux de communications électroniques en République Démocratique du Congo. De même, l'ANCY certifie les produits et services de cybersécurité et de cryptologie en République Démocratique du Congo. Elle accompagne et collabore dans la lutte contre la cybercriminalité avec d'autres organismes et institutions publiques. Participe à la sensibilisation et à la formation ainsi qu'aux investigations en matière de cybersécurité.

Tout en pilotant la gestion du fonds souverain, elle contribue à l'application des accords, traités et conventions relatifs à la cybersécurité et à la lutte contre la cybercriminalité ratifiés par la RDC.

Afin de veiller à l'exécution des dispositions légales et réglementaires relatives à la sécurité des systèmes informatiques et des réseaux de communication électronique, l'ANCY centralise les demandes d'assistance à la suite des incidents de sécurité sur les systèmes informatiques et les réseaux de communication électronique.

B. Les organismes policiers de répression de la cybercriminalité

La cybercriminalité, un fléau du monde moderne, nécessite une réponse coordonnée et spécialisée. De nombreux organismes policiers à travers le monde se sont dotés de structures dédiées à la lutte contre ces nouvelles formes de délinquance. Ce paragraphe est consacré à l'étude de l'organisation internationale de police l'Interpol (1) et la Direction des Télécoms et des Nouvelles Technologies de l'Information et de Communication de la police nationale congolaise (2).

1. L'interpol

L'Interpol, est une organisation internationale de police criminelle (OIPC) créée le 7 septembre 1923 dans le but de promouvoir la coopération policière internationale. Elle est composée de 196 pays membres, son siège se situe à Lyon (France) depuis 1986. Etant une organisation mondiale, elle permet aux autorités de police de collaborer directement avec leurs homologues, y compris entre des pays n'entretenant pas de relations diplomatiques.[161]

L'objectif est de limiter l'impact mondial de la cybercriminalité et de protéger les populations. L'Interpol coordonne et assiste aussi ses 196 pays membres dans le cadre d'activités visant à prévenir et détecter la cybercriminalité, ainsi qu'à enquêter à ce sujet.[162]

a. L'organisation de l'Interpol

L'Interpol est organisé en trois instances dont le secrétariat général, le bureau central national (BCN) et l'Assemblée générale. Le Secrétariat général est chargé de coordonner les activités quotidiennes d'INTERPOL dans le but de lutter contre les multiples facettes de la criminalité. Il est assuré par des personnes civiles et des policiers qui opèrent depuis le siège de l'Interpol.[163]

Le BCN est installé dans chaque Etat membre et sert de point de contact central pour le Secrétariat général et les autres BCN. Il est dirigé par les agents de la police nationale et se trouve au sein des directions générales de la police nationale. Les BCN sont chargés de mettre à jour les bases de données criminelles de l'Interpol et collaborent ensemble et avec les polices nationales dans les enquêtes, les opérations et des arrestations transnationales.[164]

---

[161] J. KYDENLU BATIONO, *La coopération policière pour la lutte contre la cybercriminalité au sein de l'UEMOA : bilan et perspectives*, Mémoire online, Université Libre du Burkina, 2023.

[162] Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique perspectives du bureau pour les opérations de lutte contre la cybercriminalité en Afrique - 3ème édition, p. 3.

[163] [https://www.memoireonline.com/01/24/14482/m_La-cooperation-policiere-pour-la-lutte-contre-la-cybercriminalite-au-sein-de-l-UEMOA-bilan-et-pe25.html] (Consulté le 23 septembre 2024).

[164] J. KYDENLU BATIONO, *La coopération policière pour la lutte contre la cybercriminalité au sein de l'UEMOA*, *op.cit.*, p. 4.

L'Assemblée générale est l'instance dirigeante qui réunit, chaque année, l'ensemble des pays membres pour les prises de décisions. Elle est l'instance suprême de l'Interpol et chaque pays membre dispose d'une voix de poids égal.[165]

b. Les missions de l'Interpol

Le rôle principal d'Interpol est de permettre aux différents services de police d'échanger et d'accéder aux informations sur les infractions et les criminels en leur apportant un appui technique et opérationnel. Il dispose d'un système de communication commun à tous membres et de toute une gamme de bases de données d'information de police de services spécialisés relatifs à l'analyse de l'information sur la cybercriminalité informatique.[166] Il apparaît comme un instrument privilégié pour l'échange d'informations entre enquêteurs concernant la cybercriminalité.

L'Interpol appuie aussi les services de police dans le cadre des enquêtes policières principalement en matière criminalistique, d'analyse et de soutien à la localisation de fugitifs dans le monde entier. De plus, l'Interpol forme des experts qui soutiennent les initiatives nationales en matière de lutte contre le terrorisme, la cybercriminalité et la criminalité organisée. Ces agents spécialisés ont de multiples tâches auprès des pays membres, telles que dans le domaine de l'appui aux enquêtes, des opérations sur le terrain, de formation.[167]

Les activités de l'Interpol sont politiquement neutres et menées dans le respect de la législation en vigueur au sein des différents Etats.

2. La Direction des Télécoms et des Nouvelles Technologies de l'Information et de Communication de la police nationale Congolaise DTNTIC

La Police Nationale Congolais en sigle PNC dans le cadre de sa réforme dispose d'une nouvelle direction de lutte contre la cybercriminalité, en sigle DTNTIC PNC. Elle a été instituée par le décret n°13/017 du 6 juin 2013 déterminant l'organisation et le fonctionnement du commissariat général de la police nationale congolaise.

a. L'Organisation de la DTNTIC PNC

[165] Article 10, Statut de l'Organisation Internationale de la Police Criminelle - INTERPOL

[166] M. QUEMENER et J. FERRY, *Cybersecurité : Défi mondial, op.cit.*, p. 236.

[167] J. KYDENLU BATIONO, *La coopération policière pour la lutte contre la cybercriminalité au sein de l'UEMOA : bilan et perspectives, op.cit.*, p. 45.

Il est organisé au sein de cette direction un bureau d'études et planification ; un bureau nouvelles technologies de l'information et de la communication et enquêtes ; un bureau liaison. Il dispose, en outre, d'un secrétariat.[168]

Dans la lutte contre la Cybercriminalité, les du ministère public et les officiers de la police judiciaire collabore avec les agents de l'autorité de régulation et de l'administration des télécommunications et des technologies de l'information et de la communication, sont chargés de la recherche, de la constatation des infractions commises dans ce secteur. Ils sont appelés à :

- Effectuer des contrôles et constater sur procès-verbal les infractions commises en matière des télécommunications et technologie de l'information et de la communication ;
- Procéder à des perquisitions ainsi qu'à la saisie ayant servi à la commission des faits délictueux (sur réquisition du procureur de la République 84 Article 168 de la loi de 2020 sur les télécoms et les NTIC).

b. Mission de la DTNTIC PNC

DTNTIC PNC pour mission d'organiser la lutte contre les infractions affectant les données informatiques, les systèmes internet et les infrastructures nationales vitales. Elle contribue aussi à la lutte contre la cybercriminalité de ce fait il est chargé de superviser, coordonner et effectuer au plan opérationnel, à l'échelon national et international. Les investigations de police judiciaire de même surveiller les activités criminelles et interpeller des suspects, sur base des informations à caractère judiciaire mises à sa disposition.[169]

Elle propose des normes en matière de prévention et répression de la cybercriminalité ainsi que la gestion en outre, la documentation et les statistiques de la criminalité liée aux NTIC et procède aux analyses de tendances en matière de cyberattaque.

Nature: cybercrimes sur monitoring DTNTIC PNC sur plainte: Janvier 2017 - Septembre 2018	**Nombre de plaintes**	**%**
Arnaque à l'inscription sur internet	10	0,6
Arnaque à l'héritage	240	14,5

[168] Article 45, Loi Organique n° 11/013 du 11 août 2011 Portant Organisation et fonctionnement de la Police Nationale Congolaise, JO RDC, 25 juin 2013, n° spécial.

[169] Article 2, Loi organique n° 11/013 du 11 août 2011, préc.

Vente frauduleuse sur internet	60	3,61
Pédopornographie	450	27,1
Diffamation et insultes en ligne	93	5,6
Fausses conférences	43	2,59
Vol de vehicules par contact téléphonique	25	1,51
Usurpation d'identité et escroquerie	258	15,5
Chantage à la webcam/sextorsion	78	4,7
Fraude sur compte mobile ou bancaire	143	8,61
Fraude à la SIMBOX	2	0,12
Fourniture clandestine de l'internet	40	2,41
Détournement de numéros de téléphone mobile	20	1,2
Arnaque à l'emploi	198	11,9
Total	**1660**	**100**

Statistiques de 1.660 cybercrimes. Source : DTNTIC/PNC

§2. Les faiblesses et les perspectives de la législation congolaise face aux aspects de la cybercriminalité

A. Les faiblesses de la législation Congolaise face aux aspects de la cybercriminalité

La promulgation de l'ordonnance-loi n°23/010 portant sur le Code du numérique le 13 mars 2023, marque une étape importante dans le développement du secteur numérique en RDC. Le code du numérique a été vanté par les autorités congolaises, du fait qu'il vient combler les lacunes juridiques que connaissait le pays dans le secteur du numérique.[170]

Le code du numérique pose des règles qui garantissent les libertés individuelles réprimant par la même occasion des faits de cybercriminalité et consacre les obligations de cybersécurité aux opérateurs du secteur. Les innovations apportées par ce dispositif législatif incluent la réglementation des plateformes numériques, la dématérialisation des éléments de preuve tels que l'écrit électronique et la preuve électronique y compris la signature électronique. L''identification électronique basée sur les données des personnes physiques ou morales, l'obligation de stockage et d'hébergement des données en RDC pour assurer la souveraineté numérique du pays. Ainsi que la sécurisation du système informatique contre les cyberattaques.

[170] [https://paradigmhq.org/la-protection-des-droits-numeriques-a-laube-du-nouveau-code-du-numerique-en-republique-democratique-du-congo/?lang=fr]

Le code du numérique met en place des services publics spécialisés sur les questions du numérique notamment, l'autorité de régulation du Numérique ; l'autorité nationale de Certification Electronique ; l'Agence Nationale de cybersécurite et le Conseil National du Numérique.[171] Toutefois, cette avancée normative se heurte à plusieurs difficultés ou faiblesse qui risquent d'affecter l'application effective de ce nouveau code du numérique. Ces faiblesses sont notamment :

- Manque de matériel informatique adéquat et de personnel qualifié y affecté contre la cybercriminalité ;
- Absence de laboratoire d'informatique légal ;
- Manque de sensibilisation dans toutes les branches de la population (gouvernement, citoyens, entreprises et autres organisations) ;
- La majorité des services ou organes de répression de la cybercriminalité placés par le code du numérique ne sont pas encore opérationnels.

B. Les perspectives

La répression des infractions contre la législation numérique exige une expertise, une logistique et des compétences, ainsi que l'infrastructure numérique appropriée. Il est vrai que notre pays a connu du retard dans la gestion du domaine numérique, mais cela ne peut pas nous maintenir sur place.

Il y a donc nécessité d'édicter toutes les mesures d'application indispensables et mettre en place les institutions prévues par le code. Ensuite, il faudra renforcer les capacités, outiller et équiper les acteurs commis à l'application de ce code.

Outre la vulgarisation du code et la sensibilisation, il est indiqué, par ailleurs, la mise en place d'un laboratoire moderne traitant tous les problèmes sur la cybercriminalité à l'exemple de la France qui dispose d'un Procureur numérique.

La formation des autorités judiciaires à l'utilisation de nouveaux outils numériques en vue d'assurer la performance de l'informatique légale. Cette démarche consiste en l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution judiciaire par réquisition, ordonnance ou jugement.

[171] Article 5, Ordonnance-loi n°23/010, préc.

La République Démocratique du Congo, à l'instar de nombreux pays africains, se trouve à un tournant décisif de son développement numérique. La ratification de la convention de Budapest sur la cybercriminalité et de celle de Malabo sur la cybersécurité constituerait un enjeu majeur pour sécuriser son espace et accompagner sa transformation digitale. Permettant ainsi à la RDC de s'aligner sur les normes internationales en matière de cybersécurité.

La République Démocratique du Congo devra mettre en place, dès l'école primaire, une sensibilisation à la sécurité de l'information et aux comportements responsables dans le cyberespace. En suite encourager la création d'un Institut National et la promotion des Instituts privés en cybersécurité. Pour ce faire, nous proposons un projet de programme radio-télévisé sur la cybersécurité.

CONCLUSION

En République Démocratique du Congo, comme dans plusieurs pays du monde, le fléau de la cybercriminalité ne cesse de s'accroitre. Plusieurs cas ont été enregistrés. Le cyberharcèlement sur les réseaux sociaux, les fuites des données notamment les sextapes, le piratage des sites à l'exemple du cas de Société Nationale de L'électricité (SNEL). Pour y remédier, le législateur Congolais a mis en place la loi portant code du numérique dans la lutte contre la cybercriminalité.

Les perspectives d'avenir pour la mise en œuvre du code du numérique en RDC sont à la fois prometteuses et pleines de défis. Ce nouveau cadre juridique, ambitieux et novateur, vise à réguler un secteur en pleine expansion et à accompagner le développement numérique du pays. Elle nécessite des moyens humains et financiers importants.

Il faudra former les acteurs concernés, adapter les infrastructures et mettre en place des mécanismes de contrôle et de sanction. Le secteur numérique évolue rapidement. Il sera donc nécessaire d'adapter régulièrement le code du numérique pour qu'il reste pertinent et efficace. Le cyberespace n'a pas de limite territoriale, d'où l'intérêt de trouver le juste équilibre entre la régulation nécessaire pour protéger les citoyens et les entreprises.

En ce qui concerne les avancées à promouvoir dans le domaine juridique pour mieux prévenir les cyberattaques et renforcer le contrôle d'un État sur son cyberespace.

Au niveau national, il faudra une adaptation aux nouvelles menaces. Les lois doivent évoluer en permanence pour suivre le rythme des nouvelles technologies et des nouvelles formes de cyberattaques. Définir clairement les responsabilités des acteurs publics et privés en matière de cybersécurité, notamment en cas d'incident. Et renforcer les sanctions pour décourager les cybercriminels.

Des mesures incitatives peuvent encourager les entreprises à investir dans la recherche de nouvelles solutions de cybersécurité. En vue de protéger les innovations en matière de cybersécurité pour favoriser la concurrence et l'émergence de nouvelles technologies.

Dans le but de garantir un certain niveau de qualité et de fiabilité du cyberespace et peuvent également aider les entreprises et les particuliers à choisir des solutions de sécurité adaptées.

Il est grand temps de vulgariser la promotion de la culture de la cybersécurité, en sensibilisant le grand public aux risques liés à la cybercriminalité et aux bonnes pratiques à adopter.

Au niveau international, il est raisonnable de renforcer la coopération entre les États, permettant ainsi, de partager des informations sur les menaces, les vulnérabilités et les meilleures pratiques. Ensuite, la coopération judiciaire essentiellement pour traquer et poursuivre les cybercriminels qui agissent à l'échelle internationale. La création de mécanismes de résolution des conflits pourra aider à gérer les incidents de sécurité informatique et à éviter l'escalade.

Le code du numérique apporte une clarification juridique indispensable dans un domaine en constante évolution. Ainsi, le droit a un rôle essentiel à jouer dans la lutte contre la cybercriminalité. En évoluant en permanence et en s'adaptant aux nouvelles menaces et contribuer à créer un environnement numérique plus sûr et plus fiable.

BIBLIOGRAPHIE

I. TEXTE CONSTITUTIONNEL

- Constitution de la République Démocratique du Congo modifiée et complétée par la loi n°11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006, *in JORDC*, numéro spécial, 05 février 2011.

II. LÉGISLATION CONGOLAISE

1) Textes législatifs

- Loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire.
- Loi n°20/017 du 20 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.
- Loi n°09/001 du 10 janvier 2009 portant protection de l'enfant.
- Loi n◦16/008 du 15 juillet 2016, modifiant et complétant la loi n°87/010 du 1er aout 1987 portant Code de la famille.
- Loi organique n° 11/013 du 11 août 2011 portant organisation et fonctionnement de la Police Nationale Congolaise, JO RDC, n° spécial, 25 juin 2013.
- Code pénal.

2) Textes réglementaires

- Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, *in JO RDC*, numéro spécial, 64e année, 11 avril 2023.
- Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, *in JORDC*, 45ème Année, Numéro Spécial, 30 novembre 2004.

III. LÉGISLATIONS INTERNATIONALES ET ÉTRANGÈRES

- Statut de l'organisation internationale de police criminelle – INTERPOL.

IV. OUVRAGES

1) Ouvrages généraux

1. BOULOC B., *Droit Pénal Général*, 25ème édition, Dalloz, Paris, 2007.
1. CHAWKI M., *Essai sur la notion de cybercriminalité*, IEHEI, Paris, 2006.
2. DANET D. et CATTARUZZA A., *La cyberdefense : quel territoire, quel droit ?*, Economica, Paris, 2013.
3. DECHAMPS F. et LAMBILOT C., *Cybercriminalité état des lieux*, Athemis, Bruxelles, 2016.
4. DESCHAMPS F. et LAMBILOT C., *Cybercriminalité état des lieux*, Anthémis, Bruxelles, 2016.
5. FILIOL E. et PHILIP R., *Cybercriminalité : enquête sur les mafias qui envahissent le Web*, Dunad, Paris, 2006, p.80
2. HUET A., KOERING -JOULIN R., *Droit pénal international*, PUF, Paris, 1994.
6. NDUKUMA ADJAYI K., DIANGIENPA MVETE, LOSEKA RAMAZANI et al., *Droit du commerce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité et déterritorialité*, Harmattan, Paris.
3. NDUKUMA ADJAYI K., *Guide méthodologique de référence pour recherches et rédaction des écrits universitaires en sciences sociales et juridiques*, Harmattan, Paris, 2023.
4. NGBANDA TE BOYIKOTE TENGE G., *Manuel de Droit Pénal Général*, Editions CRIGED, Kinshasa, 2007.
5. NYABIRUNGU MWENE SONGA, *Traite de droit pénal général, congolais*, Deuxième édition, Editions Universitaires, Africaines, Collection Droit et Société, Kinshasa, 2007.

2) Ouvrages spécifiques

1. PEREC G., *Espèces d'espace*, Galilée Ed. Essai, Paris, 1974.
2. QUEMENER M. et CHARPENEL Y., *Cybercriminalité, droit pénal appliqué*, Economica, 2010.

3) Ouvrage collectif

1. LUZOLO BAMBI L., MAKAYA KIELA S., *Eléments de procédure pénale manuel d'enseignement*, 1ère édition, centre de recherche sur la justice, justice transitionnelle et justice pénale internationale (CRJT), Kinshasa, 2020.

2. NYABIRUNGU MWEVE SONGA R., BOKOLOMBE BATULI S., et MANASI N'KUSU KALEBA, *Droit pénal général congolais*, éditions Droit et Société, Kinshasa, 2020.
3. Stefani G., Levasseur G. et Bouloc B., *Droit pénal général*, 11e éd., Dalloz, 1980 et 13e éd., Paris, 1987.

V. NOTES DE COURS

1. NDUKUMA ADJAYI K., *Liminaires du cours de droit du numérique*, Deuxième licence, UPC, 2018-2019.
2. NDUKUMA ADJAYI K., *Résumé écrit des séances de cours de droit du numérique*, Université protestante au Congo, année académique 2021-2022.
3. WANE BAMEME B., *Cours de droit pénal spécial*, Kinshasa, 2022.
4. WANE BAMENE B., *Cours de Droit Pénal Général*, 2013-2014.

VI. MÉMOIRES ET TFC

1. BODELET MARCEL M., D*roit pénal congolais face aux nouvelles technologies de l'information et de la communication*, Travail de fin de cycle, Université protestante au Congo, sous-direction du Professeur K. NDUKUMA ADJAYI, Kinshasa, 2022-2023.
2. KYDENLU BATIONO J., *La coopération policière pour la lutte contre la cybercriminalité au sein de l'UEMOA : bilan et perspectives*, Mémoire online, Université Libre du Burkina, 2023.
3. MATIGNON E., *La Cybercriminalité : un focus dans le monde des télécoms*, Mémoire, sous-direction de William GILLES, Université Paris 1 Panthéon - Sorbonne, Paris, 2011-2012

VII. ARTICLES

1. DJUMA SOSTHENE N., « Augmentation des cyberattaques en RDC : Quelle réglementation pour lutter contre ce fléau ? », *In Droit Numérique*, Août 2024, n°2, p. 2.
2. FORGET C., « Revue du droit des technologies de l'information », - N° 66-67/2017, Bruxelle, p.40.
3. JANET ZACHARIAS, « La pornographie – un enjeu de santé publique », *IA, B. Sc.Inf.*, 7 février 2017, p.1.

4. MATSOUPOULOU H., « Modalité de la preuve et transformations dans le recueil et l'administration de la preuve », *Archives de politique criminelle*, 2004, 1(n°26).
5. VANDERMEERSCH D., « La compétence universelle », *in* A. CASSESE, M. DELMAS-MARTY, *Juridictions nationales et crimes internationaux*, P.U.F., Paris, 2002, p. 889.

VIII. RESSOURCES EN LIGNE

1) Articles accessibles sur Internet

1. AUDIBERT M., « L'accès aux données de traffic et de localization dans le cadre d'une enquête judiciaire», [en ligne], in [https://www.lexbase.fr/article-juridique/87159156-focuslaccesauxdonneesdetraficetdelocalisationdanslecadreduneenquetejudiciaire#:~:text=Les%20donn%C3%A9es%20de%20trafic%20et%20de%20localisation%20aussi%20appel%C3%A9es%20donn%C3%A9es,fournisseur%20d'acc%C3%A8s%20%C3%A0%20internet.] (Consulté le 22 Septembre 2024).
2. CHARBONNIER R., « Comprendre la cybercriminalité : focus sur cette menace moderne», *in Guardia.School*, 12 juin 2024, disponible sur : [https://guardia.school/boite-a-outils/quest-ce-que-la-cybercriminalite.html#:~:text=La%20cybercriminalit%C3%A9%20est%20devenue%20une,pour%20commettre%20des%20actes%20malveillants.] (Consulté le 15 Aout 2024)
3. COMPILATIO, « Mener une recherche académique efficace : 9 méthodes de recherche à connaitre. », [en ligne] disponible [https://www.compilatio.net/blog/methode-recherche-academique#analytical] (Consulté le 22 juillet 2024)
4. KALONJI T., « La cybercriminalité en RDC en chiffres » [en ligne], in [https://tresorkalonji.pro/2018/09/la-cybercriminalite-en-rdc-en-chiffres.html], (consulté le 20 juillet 2024).
5. L'Internet Protocol Address, abrégée en « adresse IP » ou tout simplement « IP », constitue la base du réseau Internet.
   Voir: https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quune-adresse-ip/.
6. NDUKUMA ADJAYI K., « RDC, cybercriminalité, faire du vieux avec du neuf pour un renouveau sans révolution », *in ZooEco*, 25 mai 2020, disponible sur :

[https://zoom-eco.net/a-la-une/rdc-cybercriminalite-faire-du-vieux-avec-du-neuf-pour-un-renouveau-sans-revolution-kodjo-ndukuma/] (Consulté le 5 juin 2023)

7. SCHNEIER B., « Les cyberconflits et la sécurité nationale », *in un.org*, 2017, disponible sur : [https://www.un.org/fr/chronicle/article/les-cyberconflits-et-la-securite-nationale] (Consulté le 03 aout 2024]
8. TRESOR KALONJI, « Les pirates informatiques existent-ils en RDC ? », [en ligne] in [https://habarirdc.net/pirates-informatiques-existent-congo/] (Consulté le 05 octobre 2024).

2) Pages Web et liens HTML

1. [https://paradigmhq.org/la-protection-des-droits-numeriques-a-laube-du-nouveau-code-du-numerique-en-republique-democratique-du-congo/?lang=fr]
2. [https://www.cyber-securite.fr/hacker-definition-et-tout-savoir/] (Consulté le 1er octobre 2024)
3. [https://www.futura-sciences.com/conso/questions-reponses/guides-telecoms-quest-ce-numero-imei-trouver-18358/].
4. [https://www.hal.science/hal-0740874] (Consulté le 20 Septembre 2024).
5. [https://www.interpol.intl/fr/infractions/cybercriminalité/reponse-aux-cybermenaces] (Consulté le 11 aout 2024)
6. [https://www.kaspersky.fr/resource-center/definitions/white-hat-hackers] (Consulté le 1er octobre 2024)
7. [https://www.legavox.fr/blog/laqueendupalais/lutte-contre-cybercriminalite-republique-democratique-32980.htm.] (Consulté le 2 octobre 2024)
8. [https://www.malwarebytes.com/fr/cybersecurity/basics/hacker] (Consulté le 1er octobre 2024)
9. [https://www.memoireonline.com/01/24/14482/m_La-cooperation-policiere-pour-la-lutte-contre-la-cybercriminalite-au-sein-de-l-UEMOA-bilan-et-pe25.html] (Consulté le 23 septembre 2024)
10. [https://www.seismecanada.gc.ca]
11. [https://www.techtarget.com/searchsecurity/definition/white-hat] (Consulté le 1er octobre 2024)
12. [https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html] (Consulté le 1er Octobre 2024)
13. https://www.jedha.co/formation-cybersecurite/adresse-mac.

IX. AUTRES DOCUMENTS

1. Département des affaires économiques et sociales des Nations Unies, Division de statistique, 2003. Manuel pour l´élaboration d´un système de statistiques de la justice pénale ST/ESA/STATSER.F/89.
2. Présidence RDC, *Stratégie nationale de cybersécurité de la République Démocratique du Congo*, Kinshasa, Juillet 2022, p. 15.
3. Présidence, Stratégie nationale de cybersécurité de la RDC, la commission technique pour la cybersécurité (CTC), Kinshasa, 2022, p.25.
4. Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique perspectives du bureau pour les opérations de lutte contre la cybercriminalité en Afrique - 3ème édition, p. 3

TABLE DES MATIÈRES