Lutte contre la cybercriminalité environnementale : évolution du cadre juridique international et congolais

Cléo MASHINI MWATHA

Citer :
C. MASHINI MWATHA, « Lutte contre la cybercriminalité environnementale : évolution du cadre juridique international et congolais », in RJCE, vol. Vol. 3, n° 1/2025, Juin 2025, pp. 13-24.

ISSN 3005-706X (imprimé)
ISSN 3005-7078 (numérique)
Dépôt légal : ZR 3.02310-57531

LUTTE CONTRE LA CYBERCRIMINALITÉ ENVIRONNEMENTALE : ÉVOLUTION DU CADRE JURIDIQUE INTERNATIONAL ET CONGOLAIS

Cléo MASHINI MWATHA
Professeur de droit public
à l'Université Pédagogique Nationale (UPN)
Directeur du CRIDE et de JURISTRALE
Avocat au Barreau de Kinshasa-Gombe

Résumé
La cybercriminalité environnementale, qui exploite les outils numériques pour nuire à l'environnement, représente un défi planétaire majeur. Cet article propose une analyse approfondie de l'évolution du cadre juridique, tant au niveau international que national en République Démocratique du Congo, face à cette menace grandissante. Il examine les atouts et les lacunes des instruments juridiques actuels, souligne les obstacles inhérents à l'application de la loi dans un environnement numérique, et suggère des pistes novatrices pour intensifier la lutte contre cette forme de criminalité.

Mots-clés : cybercriminalité environnementale, criminalité environnementale, cyberattaque, droit international, droit du numérique, espèces protégées, commerce illégal, piratage, *fake news*, cryptominage.

Abstract
Environmental cybercrime, which exploits digital tools to harm the environment, represents a major global challenge. This article provides an in-depth analysis of the evolution of the legal framework, both internationally and nationally in the Democratic Republic of Congo, in response to this growing threat. It examines the strengths and weaknesses of current legal instruments, highlights the obstacles inherent in enforcing the law in a digital environment, and suggests innovative ways to step up the fight against this form of crime.

Keywords: *environmental cybercrime, environmental crime, cyberattack, international law, digital law, protected species, illegal trade, piracy, fake news, cryptomining.*

Introduction

L'année 2023 a marqué un jalon significatif, avec plus de 67% de la population mondiale, soit 5,4 milliards de personnes, ayant accès à l'Internet[1], témoignant d'une connectivité sans précédent qui façonne désormais nos modes de vie, de la communication aux transactions commerciales, en passant par la recherche et l'innovation. Cependant, cette omniprésence numérique expose également une large majorité de l'humanité aux périls insidieux de la cybercriminalité. L'absence de résilience face à la fracture numérique accentue d'ailleurs la vulnérabilité de ceux qui se trouvent en marge de cette révolution technologique une fois en ligne[2].

Si l'avènement de l'ère numérique a indubitablement révolutionné nos quotidiens et ouvert des perspectives inédites en matière de développement, il a simultanément engendré l'émergence de nouvelles formes de criminalité, menaçant gravement notre environnement. La cybercriminalité environnementale, en tirant parti des outils numériques, s'attaque de front à la biodiversité, aux

[1] UIT, Communiqué de presse du 12 septembre 2023, accessible sur : https://www.itu.int/fr/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx, consulté le 1er juin 2025.
[2] Nations unies, *La Convention contre la cybercriminalité, pour un monde numérique et physique plus sûr*, accessible sur : https://news.un.org/fr/story/2024/12/1151706, consulté le 28/05/2025.

écosystèmes et aux ressources naturelles, engendrant des conséquences souvent dévastatrices. Elle se positionne comme l'une des formes de criminalité transnationale affichant la progression la plus rapide au sein des pays membres d'INTERPOL. La croissance fulgurante d'Internet et de l'informatique, bien qu'ayant catalysé un développement économique et social notable, a paradoxalement accru les risques et les vulnérabilités, ouvrant la voie à de nouvelles activités criminelles[3].

La République Démocratique du Congo (RDC), dotée d'une biodiversité d'une richesse inestimable, n'est pas épargnée par ce fléau. Confrontée à une exploitation illégale de ses ressources naturelles, facilitée par les technologies émergentes, la RDC voit son patrimoine naturel menacé par le commerce illégal d'espèces protégées, le braconnage, la déforestation illégale et la pollution industrielle. Ce constat alarmant soulève une interrogation fondamentale quant à l'efficacité des instruments juridiques existants pour contrer cette nouvelle forme de criminalité. Le cadre juridique international, bien que dynamique, peine parfois à saisir la complexité et la vélocité des mutations du cybercrime. De même, au niveau national, les législations éprouvent des difficultés à s'adapter à ces nouvelles menaces.

La présente étude a pour objectif d'analyser l'évolution du cadre juridique international et national dans la lutte contre la cybercriminalité environnementale, en prenant comme cas d'étude la République Démocratique du Congo. Nous examinerons le concept de cybercriminalité (I) avant de pouvoir analyser le cadre juridique international et national (II).

I. La Cybercriminalité environnementale : une menace émergente

La cybercriminalité environnementale représente un phénomène criminel en pleine expansion, dont la compréhension détaillée de sa définition et de son étendue est cruciale pour appréhender ses spécificités dans les contextes international et congolais. Ce fléau, qui prend une ampleur considérable, occasionne des dommages environnementaux dévastateurs.

I.1. Définition et formes de la cybercriminalité environnementale

I.1.1. Définition de la cybercriminalité environnementale

Le terme « *cyber* » renvoie aux nouvelles technologies du numérique, et en particulier l'Internet. La « *criminalité* » est une traduction littérale de l'anglais *criminality*, qui concerne le droit pénal – ou *criminal law* – plutôt que la notion française de criminalité ou de criminologie. Ainsi, il serait plus juste de parler de « *cyberdélinquance* » ou de « cyberinfraction », même si le terme couvre bien l'ensemble des comportements prohibés[4].

Le terme « cybercriminalité » englobe l'ensemble des activités illégales perpétrées au moyen des technologies de l'information et de la communication (TIC). Il s'agit d'une forme de délit qui utilise Internet, les réseaux informatiques et les dispositifs numériques pour commettre des actes illégaux[5].

---

[3] UNODC, *Résumé de la stratégie mondiale de lutte Contre la cybercriminalité*, p.2, accessible sur : https://www.interpol.int/fr/content/download/5586/file/Summary_CYBER_Strategy_2017_01_FR%20LR.pdf, consulté le 15/12/2024.

[4] R. CISWICKI, « La définition fonctionnelle de la notion de cybercriminalité », in *memannuaire_securite_defense_2019-mqt02.indd*, pp.267-276, p. 267, accessible sur : https://www.afdsd.fr/wp-content/uploads/2024/09/AFDSD18Ciswicki.pdf, consulté le 18/03/2025.

[5] Nations unies, La Convention contre la cybercriminalité, pour un monde numérique et physique plus sûr, in *ONU Info. L'actualité mondiale Un regard humain*, 25 décembre 2024, accessible sur : https://news.un.org/fr/story/2024/12/1151706, consulté le 10/03/2025.

Ce type de criminalité se distingue des formes traditionnelles par son exploitation des opportunités offertes par la numérisation croissante de la société.

Plus spécifiquement, la cybercriminalité environnementale fait référence à l'utilisation des TIC pour commettre des actes criminels qui ont un impact direct sur l'environnement. Contrairement à d'autres catégories de cybercriminalité, celle-ci vise explicitement les ressources naturelles, les écosystèmes ou les infrastructures environnementales. Elle couvre un large éventail d'activités illégales, incluant le piratage de systèmes de gestion environnementale, le sabotage de centrales énergétiques, la propagation de fausses informations écologiques, ou encore le trafic en ligne d'espèces sauvages.

Ce phénomène est en constante évolution, tirant parti de l'anonymat qu'offre le monde virtuel[6] et de la complexité inhérente aux réseaux numériques. La cybercriminalité environnementale se caractérise par ses motivations environnementales, ses méthodes distinctes et ses conséquences potentiellement catastrophiques, d'où la nécessité impérieuse de reconnaître ses spécificités pour lutter efficacement contre cette menace émergente. Une action concertée à l'échelle mondiale, incluant la coopération internationale, l'élaboration de cadres juridiques adaptés et le renforcement des capacités, est indispensable pour prévenir, détecter et réprimer ce phénomène.

Plusieurs définitions de la cybercriminalité sont disponibles en raison de sa polymorphie. L'Organisation de coopération et de développement économiques (OCDE) fut la première organisation internationale à s'intéresser à la fraude informatique[7], définissant la cybercriminalité (ou abus informatique) comme « tout comportement illégal, contraire à l'éthique ou non autorisé, qui concerne un traitement automatique et/ou une transmission de données » [8].

En République Démocratique du Congo, la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication[9], en son article 4, définit la cybercriminalité comme une notion large regroupant toutes les infractions commises sur ou au moyen d'un système informatique généralement connecté à un réseau. De même, l'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique[10], à l'article 2, lit. 24, la caractérise comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, dont la commission est facilitée ou liée à l'utilisation des technologies.

I.1.2. Formes de la cybercriminalité environnementale

Il est essentiel de distinguer les crimes « cyberdépendants » des crimes dits « cyberpermettant ». Les premiers sont intrinsèquement liés aux technologies de l'information et de la communication (TIC) et n'existeraient pas sans elles (ex.: l'accès illégal à un système informatique)[11]. Les seconds, bien que

---

[6] Surtout lorsqu'il est question du Darkweb et des réseaux y dissimulés. Voy. M. EL HAYSOUFI (2023), *La lutte contre la cybercriminalité dans le Darkweb, éléments d'analyse comparative de droit français et canadien*, accessible sur : https://corpus.ulaval.ca/entities/publication/27dff728-7bd3-4976-ad6d-d0e49b0ecf55, consulté le 10/12/2024.
[7] *Ibid.,* p.269.
[8] OCDE, *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris, 1986, p. 7.
[9] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, in *JORDC*, n° spécial, 22 septembre 2021.
[10] Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, in *JORDC*, n° spécial, 65e année, 11 avril 2023.
[11] K. Bannelier-Christakis et M. Watin-Augouard, « L'ONU, la cybersécurité et la lutte contre la cybercriminalité: le difficile consensus », 2024, in *hal-04782739*, pp.1-26, p. , 20, accessible sur : https://hal.science/hal-04782739v1/document, consulté le 27/10/2024.

pouvant être commis sans les TIC, voient leur perpétration facilitée, amplifiée ou accélérée par ces technologies (ex.: le commerce illégal d'espèces sauvages en ligne).

Les formes de cybercriminalité sont multiples et variées, incluant le piratage informatique, l'usurpation d'identité, la fraude en ligne, le phishing, la diffusion de virus ou de logiciels malveillants, le cyberharcèlement, la pornographie enfantine et le terrorisme en ligne. S'agissant spécifiquement de la cybercriminalité environnementale, plusieurs manifestations sont observées :

1.1.2.1. Le commerce illégal d'espèces protégées en ligne

Des plateformes d'enchères en ligne (ex.: eBay) ou des forums spécialisés sont exploités pour la vente illégale de produits issus d'espèces protégées (ivoire, bois précieux). Les réseaux sociaux sont également utilisés pour promouvoir et faciliter ces ventes, ciblant des publics spécifiques. Le rôle des médias sociaux (Facebook, WhatsApp, Instagram) dans la facilitation du trafic d'espèces sauvages est préoccupant, leurs algorithmes et l'intelligence artificielle étant souvent inefficaces pour modérer un contenu qui connecte les trafiquants plus rapidement que les modérateurs ne peuvent les supprimer. Un appel est lancé pour que des actions législatives contraignent les entreprises de médias sociaux à modifier leurs algorithmes afin de détecter et de contrecarrer les activités illégales[12].

Le marché de la commercialisation de produits en ivoire sur Internet est en forte croissance, comme en témoignent des enquêtes menées en Europe, révélant un nombre significatif d'annonces de vente d'ivoire présumé sur des sites belges. En effet, des enquêtes réalisées par IFAW au niveau européen recensent 348 annonces sur 13 sites Internet en Belgique, dont presque la moitié concernait des objets en ivoire authentique ou présumé[13]. Ces derniers étaient les plus vendus avec 162 annonces, soit 47 % des ventes dénombrées pendant l'enquête. La majorité des annonces ont été trouvées sur les sites 2ememain.be et 2dehands.be. Un même vendeur a publié 11 annonces sur 2ememain.be et 2dehands.be au cours de l'enquête pour vendre des bracelets, sculptures et vases présumés en ivoire[14].

Le cybermarché facilite le rapprochement entre vendeurs et acheteurs en s'affranchissant des frontières et de certaines contraintes du marché national[15]. L'ONU constate l'extension des marchés d'espèces sauvages à l'espace numérique, où les modalités d'achat sont souvent réglées via des messages privés, rendant difficile la détermination de la légalité des transactions et la poursuite des vendeurs[16]. La cybercriminalité liée à la faune et à la flore sauvages inclut le braconnage virtuel, la vente en ligne de produits dérivés d'espèces menacées, et le trafic d'animaux sauvages, les criminels utilisant les plateformes en ligne pour contourner les réglementations.

1.1.2.2. **Le piratage de données environnementales**

Cela englobe le vol de données sensibles liées à l'environnement (recherches sur le changement climatique, plans de conservation, informations géospatiales sur des sites protégés, réglementations

---

[12] D. STILES, "Holding social media companies accountable for facilitating illegal wildlife trade (commentary)", in *Mongabay*, 25/10/2019, accessible sur: https://news.mongabay.com/2019/10/holding-social-media-companies-accountable-for-facilitating-illegal-wildlife-trade-commentary/, consulté le 12/12/2024.

[13] IFAW, *Recherché - mort ou vif : Le commerce d'espèces sauvages sur Internet dévoilé*, *op.cit.*, p.28, cité par C. MASHINI MWATHA*, Lutte contre le trafic international des espèces sauvages menacées d'extinction. Évaluation de la convention de Washington (CITES)*, Paris, L'Harmattan, 2024, p.167.

[14] *Ibid.*

[15] UNODC, *Résumé de la stratégie mondiale de lutte Contre la cybercriminalité*, *op.cit.,* p.2.

[16] Nations unies, *Lutte contre le trafic d'espèces sauvages*, *op.cit*, p.5, cité par C. MASHINI MWATHA*, Lutte contre le trafic international des espèces sauvages menacées d'extinction. Évaluation de la convention de Washington (CITES)*, Paris, L'Harmattan, 2024, p.229.

environnementales) à des fins illégales, telles que l'exploitation illégale de ressources ou la contrefaçon de produits écologiques.

Des attaques informatiques peuvent paralyser les systèmes de surveillance environnementale ou détruire des données cruciales. Un exemple courant est le piratage des systèmes de gestion des ressources naturelles (surveillance des forêts ou des océans) pour obtenir des informations confidentielles (quotas de pêche, données de coupe forestière) et les utiliser à des fins illégales.

1.1.2.3. **La diffusion de fausses informations (fake news)**

La propagation de fausses informations sur l'environnement peut semer la confusion, discréditer les efforts de conservation, et nuire à la réputation d'organisations ou d'activistes environnementaux via des campagnes de diffamation en ligne. Les cybercriminels peuvent créer de faux profils ou sites Internet pour manipuler l'opinion publique ou diffamer des entreprises ou des organisations de la société civile ou des institutions gouvernementales[17].

1.1.2.4. **Les attaques contre les infrastructures et les systèmes de gestion de l'environnement**

Une autre forme de cybercriminalité environnementale concerne les attaques contre les infrastructures et les systèmes de gestion de l'environnement, où les hackers peuvent cibler les systèmes de contrôle d'installations pétrolières, de centrales électriques, de stations d'épuration ou d'usines chimiques, provoquant des perturbations, des dommages et des catastrophes environnementales aux conséquences dévastatrices sur les écosystèmes et la santé publique.

I.2. L'ampleur et l'impact du phénomène

La cybercriminalité environnementale, un phénomène émergent, est difficile à quantifier précisément en raison de sa nouveauté et de son évolution constante. Néanmoins, son impact potentiel sur la planète et les sociétés est considérable.

I.2.1. L'impact sur la lutte contre le braconnage

Le commerce illégal d'espèces sauvages, exacerbé par la cybercriminalité, entraîne une perte significative de biodiversité, contribuant à la disparition de nombreuses espèces. La dégradation des écosystèmes, la pollution de l'environnement, et les risques sanitaires sont également des conséquences directes des activités criminelles en ligne. De surcroît, les escroqueries environnementales peuvent miner la confiance du public et détourner des fonds destinés à la protection de la nature.

La coordination des réseaux criminels est facilitée par les outils numériques, qui favorisent le développement de marchés noirs en ligne et rendent difficile le traçage des produits issus de la criminalité. Les conséquences sont multiples et graves, incluant la dégradation des écosystèmes, la pollution, des risques sanitaires, des coûts de réparation élevés et des pertes financières pour les entreprises et les États, ainsi que des impacts sociaux sur les populations locales et autochtones.

[17] Par exemple via des attaques Distributed Denial of Service (DDoS) contre des sites gouvernementaux pour contester des politiques environnementales.

I.2.2. Les spécificités de la cybercriminalité environnementale

La cybercriminalité environnementale présente des défis uniques en matière de répression et de prévention. On peut relever notamment :

- ***Le caractère transnational*** **:** la cybercriminalité transcende les frontières géographiques, compliquant la coordination entre les États, les enquêtes transfrontalières, les différences entre les systèmes juridiques, et la disparité des capacités des services d'application de la loi. Les criminels peuvent agir rapidement et de manière anonyme, rendant leur identification et leur arrestation particulièrement ardues ;

- ***L'évolution rapide des technologies*** **:** cette rapidité impose une adaptation constante des outils de lutte et une mise à jour permanente des législations pour contrer les méthodes évolutives des cybercriminels ;

- ***Le manque de ressources*** **:** les budgets limités et la pénurie de compétences constituent des freins majeurs à une lutte efficace contre cette criminalité ;

- ***Le caractère souvent invisible des attaques*** **:** ce qui rend difficiles la localisation des auteurs et la détection des attaques en temps réel, les conséquences pouvant se manifester bien après l'acte initial.

Les enjeux de la cybercriminalité sont considérables. Elle constitue une menace pour la sécurité des systèmes d'information et des données personnelles, entraînant des dommages significatifs pour les individus, les entreprises et les gouvernements (atteintes à la confidentialité, intégrité et disponibilité des informations, violations de la vie privée, pertes financières, vols d'identité, attaques DDoS). Ses répercussions économiques sont majeures, les entreprises étant des cibles privilégiées en raison de la valeur de leurs données et services en ligne, subissant des pertes financières considérables, une atteinte à leur réputation et une perte de confiance des clients. La cybercriminalité favorise également la criminalité organisée (blanchiment d'argent, trafic de substances illicites). Enfin, elle soulève des questions éthiques et sociales importantes concernant l'équilibre entre vie privée, sécurité et liberté d'expression dans le contexte numérique.

II. Analyse du cadre juridique international et national

Face à l'urgence de la situation, l'établissement d'un cadre juridique solide est impératif pour prévenir, détecter, poursuivre et sanctionner les actes de cybercriminalité environnementale. Ce cadre doit intégrer des lois nationales spécifiques et des instruments internationaux favorisant la coopération interétatique[18].

II.1. Les instruments juridiques internationaux

Au niveau international, plusieurs instruments juridiques visent à lutter contre la cybercriminalité environnementale. Les conventions internationales jouent un rôle crucial en établissant des normes communes et en facilitant la coopération transfrontalière.

---

[18] Les mesures juridiques ont un rôle clef dans la prévention et la lutte contre la cybercriminalité. Elles sont nécessaires notamment en matière d´incrimination, de pouvoirs procéduraux, de juridiction, de coopération internationale et en ce qui concerne la responsabilité des prestataires de services Internet. Voy. UNODC, *Étude détaillée sur la cybercriminalité. Ébauche - Février 2013*, p. xviii.

II.1.1. La convention de Budapest sur la cybercriminalité

Adoptée le 23/11/2001, la convention de Budapest est le premier instrument international contraignant d'envergure paneuropéenne en matière de cybercriminalité[19].

Cette convention sur la cybercriminalité est considérée comme la norme internationale la plus complète à ce jour puisqu'elle offre un cadre complet et cohérent en matière de cybercriminalité et de preuves électroniques. Elle fait office de ligne directrice pour tout pays élaborant une législation exhaustive en matière de lutte contre la cybercriminalité, mais aussi de cadre pour la coopération internationale entre ses États parties[20].

Bien que cette convention ne cible pas spécifiquement la cybercriminalité environnementale, ses dispositions sont applicables pour contrer les attaques numériques visant l'environnement et les ressources naturelles. Elle peut être utilisée pour lutter contre le piratage et la destruction intentionnelle de systèmes d'information environnementaux (bases de données environnementales), ainsi que contre la fraude, le vol d'identité et l'usurpation d'identité liés à des programmes, logiciels et données environnementaux.

II.1.2. Convention sur le commerce international des espèces de faune et de flore sauvages menacées d'extinction (CITES)

La CITES a intégré la lutte contre la cybercriminalité liée aux espèces sauvages avec l'adoption de la décision 17.93 lors de la CoP17. Cette décision enjoint le Secrétariat à collaborer avec INTERPOL[21] pour soutenir les efforts des parties et élaborer des lignes directrices pour une lutte plus efficace. D'autres ressources CITES, comme la résolution 11.3 (Rev CoP18) sur la conformité et l'application, et les décisions CITES 18.81-18.85 sur la criminalité liée à Internet, sont également pertinentes[22]. La CITES souligne l'importance pour les parties de renforcer leurs mesures nationales pour réglementer le commerce légal et lutter contre la criminalité liée aux espèces sauvages via Internet, en s'adaptant

---

[19] K. BARTHOLIN, « La Convention de Budapest sur la cybercriminalité du 23 novembre 2001 », in I. BOUHADANA et W. GILLES (dir.), *Cybercriminalité, cybermenaces et cyberfraudes, Paris, Institut du Monde et du Développement*, 2012, pp.95-99, cité par P. BERTHELET, P. (2018), « La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels », in *Revue québécoise de droit international / Québec Journal of International Law / Revista quebequense de derecho internacional*, pp.25–39, p.29.

[20] Conseil de l'Europe, Dépliant sur les avantages de la Convention de Budapest, p.1. (dernière mise à jour : juin 2024), accessible sur : https://rm.coe.int/cyber-buda-benefits-1-april-2024-fr/1680b51694, consulté le 18/03/2025. Il échet de noter que les États qui ont participé aux négociations de la Convention (les membres du Conseil de l'Europe, l'Afrique du Sud, le Canada, les États-Unis et le Japon) peuvent la signer et la ratifier. En vertu de l'article 37, tout autre État peut devenir partie en « adhérant » à la Convention s'il est prêt à l'appliquer.

[21] INTERPOL s'emploie également à finaliser l'élaboration de Lignes directrices sur la lutte contre la cybercriminalité liée aux espèces sauvages, comme prévu par la décision 17.93, paragraphe d). Ces lignes directrices, incluant des questions telles que les concepts de base des enquêtes sur la cybercriminalité, des enquêtes open source et de la collecte, la demande et la conservation d'éléments de preuves, fourniront aux agents chargés de la lutte contre la fraude un outil pratique sur les façons d'enquêter sur les cas de cybercriminalité liée aux espèces sauvages.

[22] Voy. les documents et notifications ci-dessous : différents rapports sur la lutte contre la cybercriminalité liée aux espèces sauvages, dont du Secrétariat (CoP18 Doc. 33.1) ; rapport du Comité permanent sur la lutte contre la cybercriminalité liée aux espèces sauvages (CoP18 Doc. 33.1 et SC70 Doc. 30.3.2)) ; celui du Comité permanent (CoP18 Doc. 33.2) ; celui du groupe de travail sur la lutte contre la cybercriminalité liée aux espèces sauvages (SC70 Doc. 30.3.1) ; rapport du Secrétariat sur la lutte contre la cybercriminalité liée aux espèces sauvages (SC70 Doc. 30.3.2) ; SC69 Doc.31.3 sur la lutte contre la cybercriminalité faunique ; CoP17 Doc.29 sur la lutte contre la cybercriminalité liée aux espèces sauvages ; les notifications n ° 2020/031 (publié le 1er avril 2020) et n° 2019/042 (publié le 8 août 2019) sur la criminalité liée aux espèces sauvages liée à Internet ainsi que n° 2017/036 (publié le 4 mai 2017) sur la lutte contre la cybercriminalité liée aux espèces sauvages.

continuellement aux nouvelles tendances[23]. Les trafiquants modifiant constamment leurs méthodes, les forces de l'ordre doivent faire preuve de réactivité[24].

II.1.3. Autres instruments et initiatives internationales

D'autres instruments, tels que la Convention sur la diversité biologique (CDB) et les conventions des Nations Unies sur la lutte contre la criminalité transnationale organisée (UNTOC), sont également pertinents.

Les organisations internationales comme l'ONU, l'OMS, l'OCDE et Interpol jouent un rôle pivot en formulant des résolutions et des recommandations pour prévenir et combattre ce phénomène croissant. L'OMS, par exemple, exhorte les États membres à élaborer des politiques et des mécanismes législatifs liés à une stratégie nationale globale de cybersanté. Elle promeut également l'interopérabilité des systèmes d'information sanitaire aux niveaux national et international, dans le respect des principes de transparence, d'accessibilité et de protection des données[25]. Pour sa part, Interpol, avec son Cybercrime Programme, vise à améliorer la coopération entre les forces de l'ordre et les autorités judiciaires pour lutter contre la cybercriminalité, incluant la dimension environnementale, en facilitant le partage d'informations, l'échange de bonnes pratiques et la formation[26].

Ces recommandations appellent à renforcer les législations nationales pour criminaliser les actes de cybercriminalité environnementale, à adopter des politiques de prévention proactive, à consolider les capacités techniques et humaines, à promouvoir la coopération internationale et à encourager la collaboration avec le secteur privé. La mise en œuvre de ces mesures dépend toutefois de l'appréciation des États membres, nécessitant une coopération internationale continue pour assurer l'uniformité et l'efficacité de la lutte mondiale.

Par ailleurs, il convient d'indiquer que le 8 août 2024, après cinq de négociations, les 193 États membres de l'ONU ont adopté par consensus un projet de convention contre la cybercriminalité. Cet instrument, premier du genre au niveau mondial, offrirait notamment aux États un outil essentiel pour faire face à une menace croissante et permettra d'apporter des réponses plus rapides, mieux coordonnées et plus efficaces, rendant ainsi le monde numérique et le monde physique plus sûrs[27].

---

[23] CITES, *Wildlife crime linked to the Internet*, https://cites.org/eng/prog/imp/wildlife_crime_online, consulté le 18/05/2025.

[24] Nations unies, *Lutte contre le trafic d'espèces sauvages*, *op.cit*, p.5 ; C. MASHINI MWATHA*, Lutte contre le trafic international des espèces sauvages menacées d'extinction. Évaluation de la convention de Washington (CITES)*, *op.cit.*, p.230.

[25] OMS, *Stratégie mondiale pour la santé numérique 2020-2025*, accessible sur : https://iris.who.int/bitstream/handle/10665/344250/9789240027558-fre.pdf, consulté le 19/05/2025.

[26] INTERPOL, Lutte contre la cybercriminalité Stratégie mondiale 2022 – 2025, accessible sur, https://www.interpol.int/fr/content/download/19815/file/Cybercrime%20Short%20strategy%20FR.pdf?inLanguage=fre-FR&version=6, consulté le 17/03/2025.

[27] Nations unies, *La Convention contre la cybercriminalité, pour un monde numérique et physique plus sûr*, *op.cit.*

II.2. Le cadre juridique national congolais

Au niveau national, il est important de disposer d'un cadre juridique permettant de lutter contre la cybercriminalité[28]. C'est ainsi que, la République Démocratique du Congo, face à la montée de la cybercriminalité environnementale, a commencé à adapter son cadre juridique.

2.2.1. La loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

La loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication (TIC)[29] vise à adapter la législation existante à l'essor rapide du domaine numérique. Elle cherche à combler les lacunes, telles que l'intégration des TIC, la sécurisation des données personnelles, l'identification des abonnés et la répression des fraudes. Le texte promeut une économie libérale, met fin aux monopoles et instaure la concurrence dans le secteur. L'objectif est de faire des télécommunications et des TIC un levier de croissance économique, de création d'emplois et de développement des infrastructures, tout en assurant la protection des utilisateurs et la sécurité nationale.

En ce qui concerne la lutte contre la cybercriminalité, la loi congolaise comporte plusieurs articles essentiels. Elle établit à l'article 153 que les actes de cybercriminalité, tels que les atteintes à l'intégrité des systèmes informatiques, les atteintes par tout moyen de diffusion publique et la fraude électronique, doivent être poursuivis et réprimés, sans préjudice des dispositions pertinentes du Code pénal, par les dispositions de son titre VII (article 154). Comme déjà relevé, l'article 4 donne une bonne définition de la cybercriminalité. Bien que cette loi mentionne la « protection de l'environnement » comme une des exigences essentielles dans l'intérêt général lié à l'utilisation des équipements et installations de télécommunications (article 4, point 42), et l'incitation de l'État pour les opérateurs à réaliser des investissements dans les domaines environnemental et social (article 167), elle n'établit pas le lien entre la cybercriminalité et les problématiques environnementales dans les définitions ou les dispositions pénales. L'important ici est que la cybercriminalité y est traitée, la cybercriminalité environnementale n'étant qu'une facette de celle-ci.

2.2.2. L'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique

L'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique vise à réguler le secteur de l'Internet en RDC, couvrant des aspects comme la protection des données personnelles, les transactions électroniques, la cybersécurité et l'infrastructure numérique. Il cherche à créer un

[28] La cybercriminalité est devenue une préoccupation majeure à l'échelle mondiale, y compris en Afrique. Les lois africaines sur la cybercriminalité sont essentielles pour lutter contre ce fléau et protéger les individus, les entreprises et les gouvernements contre les activités criminelles en ligne. De nombreux pays africains ont adopté ou amender leurs lois pour inclure des dispositions relatives à la cybercriminalité. Par exemple, en 2016, le Kenya a promulgué la Computer Misuse and Cybercrimes Act, qui vise à criminaliser certaines activités liées à la cybercriminalité, telles que le piratage informatique, le phishing, les atteintes à la vie privée et la diffusion de contenus haineux en ligne. Le Nigeria a également pris des mesures pour lutter contre la cybercriminalité avec la signature du Cybercrime (Prohibition, Prevention, etc.) Act en 2015. Le Maroc a également mis en place des mesures pour faire face à la cybercriminalité. En 2017, le pays a adopté la loi n° 103-13 relative à la lutte contre la cybercriminalité. Cette loi vise à prévenir et à réprimer les actes criminels liés à l'utilisation des TIC, tels que le piratage informatique, l'accès frauduleux aux systèmes informatiques et la diffusion de contenus illicites. La loi autorise également les forces de l'ordre à surveiller les activités en ligne pour détecter les comportements criminels. D'autres pays africains, tels que l'Afrique du Sud, le Ghana et la Tanzanie, ont également mis en œuvre des lois spécifiques sur la cybercriminalité pour renforcer leur arsenal législatif et offrir une meilleure protection contre les crimes en ligne.

[29] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, in *JORDC*, n° spécial, 22 septembre 2021.

environnement propice au développement du Net tout en garantissant la sécurité et la confiance des utilisateurs.

Les innovations apportées par le nouveau dispositif législatif incluent la réglementation des plateformes numériques, la dématérialisation des éléments de preuve …, ainsi que la sécurisation du système informatique contre les cyberattaques et la définition des infractions numériques[30].

Concernant la cybercriminalité, le Code du numérique incorpore explicitement des dispositions visant à prévenir et réprimer diverses formes d'infractions cybernétiques, telles que l'accès illégal aux systèmes informatiques, la fraude informatique, l'usurpation d'identité en ligne et la diffusion de contenus illicites.

En ce qui concerne la cybercriminalité environnementale, l'ordonnance-loi ne l'évoque pas spécifiquement ni directement comme une catégorie distincte d'infraction. Les actes de cybercriminalité ayant un impact environnemental pourraient potentiellement être traités sous des dispositions plus générales relatives aux atteintes aux systèmes informatiques ou à la fraude, si un lien direct peut être établi. Les articles qui peuvent être mobilisés sont notamment :

- Les articles 332 à 338 couvrent les atteintes aux systèmes et données informatiques. Ainsi, si le commerce illégal en ligne des produits environnementaux implique des piratages de sites web, le vol de données clients, ou la perturbation de systèmes de paiement en ligne, ces articles peuvent être invoqués ;
- L'article 339 incrimine la falsification de données informatiques. La création ou l'utilisation de fausses informations sur un site de commerce en ligne (par exemple, de faux avis, de fausses descriptions de produits, ou de faux comptes) peut être réprimée par cet article ;
- L'article 340 sur la fraude informatique. Cette disposition vise tout acte de commerce en ligne impliquant des manœuvres frauduleuses pour tromper l'acheteur ou le vendeur, ou pour obtenir un gain illicite, tombera sous le coup de cet article. Cela inclut la vente de produits contrefaits, la non-livraison de produits payés, ou les arnaques diverses ;
- Les articles 349 et 350 couvrent les actes de tromperie et de traitement illicite de données personnelles, y compris l'usurpation d'identité en ligne ;
- Les articles 356 et suivants visent les contenus abusifs et illicites. Il en résulte que la vente en ligne de produits illégaux (faune, flore, etc.), de biens contrefaits, ou la diffusion de contenus prohibés sont directement réprimées par les dispositions sur les contenus illicites.

Il est important de noter que le Code du numérique prévoit des peines de servitude pénale (prison) et des amendes, et qu'il établit également la responsabilité pénale des personnes morales pour certaines infractions. Le texte met en place des mécanismes de droit pénal de forme et de fond pour la répression de la cybercriminalité en RDC.

En substance, la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, ainsi que l'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, constituent des instruments fondamentaux définissant la cybercriminalité et ses diverses manifestations. Ces textes législatifs posent les bases de la répression des infractions commises sur ou au moyen des systèmes informatiques et des réseaux. Cependant, l'adéquation de ces dispositions face aux spécificités et à la rapidité d'évolution de la cybercriminalité environnementale nécessite une évaluation continue. Les défis résident dans la capacité à transposer

[30] M. CALENGA TSHASEKELA et H. NINDA MUHIMUZIO (2023), *La protection des droits numériques à l'aube du nouveau code du numérique en République Démocratique du Congo*, OSIRIS, accessible sur : https://www.osiris.sn/la-protection-des-droits-numeriques-a-l-aube-du-nouveau-code-du-numerique-en.html, consulté le 10/11/2024.

les principes généraux du droit pénal numérique aux atteintes environnementales, souvent complexes à prouver et à attribuer dans un contexte transnational.

Conclusion

La cybercriminalité environnementale représente un fléau contemporain complexe, dont l'ampleur et les conséquences sur la biodiversité, les écosystèmes et les ressources naturelles exigent une réponse juridique et opérationnelle percutante. Comme l'a démontré cette analyse, l'exploitation des outils numériques par les criminels environnementaux transcende les frontières géographiques, rendant le combat d'autant plus ardu.

Face à cette menace transnationale en constante évolution, l'architecture juridique, tant internationale que congolaise, doit impérativement s'adapter et se renforcer. Si des avancées significatives ont été réalisées, à l'image de la convention de Budapest offrant un cadre complet pour la cybercriminalité, ou de l'intégration par la CITES de la lutte contre le cybercrime lié aux espèces sauvages, des lacunes subsistent, notamment en ce qui concerne la spécificité de la cybercriminalité environnementale dans certaines législations nationales, comme celle de la République Démocratique du Congo.

L'efficacité de cette lutte repose sur plusieurs piliers indissociables. Premièrement, une coopération internationale accrue est fondamentale pour harmoniser les législations, faciliter les enquêtes transfrontalières et surmonter les disparités des systèmes juridiques. Les récentes initiatives de l'ONU, de l'OCDE et d'Interpol, qui appellent au renforcement des législations nationales et à l'échange de pratiques bienveillantes, sont des pas dans la bonne direction. L'adoption prochaine de la Convention de l'ONU contre la cybercriminalité est, à cet égard, une avancée prometteuse.

Deuxièmement, il est crucial d'adapter et de consolider les cadres juridiques nationaux, à l'instar de la RDC qui, avec la loi n°20/017 du 25 novembre 2020 sur les TIC et l'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, pose les bases de la répression de la cybercriminalité. Néanmoins, l'intégration explicite de la dimension environnementale dans les définitions et les dispositions pénales permettrait une meilleure appréhension et sanction des actes de cybercriminalité ayant un impact direct sur la nature.

Enfin, au-delà des aspects purement juridiques, une approche holistique s'impose. L'investissement dans la cybersécurité, le développement des capacités techniques et humaines des services répressifs, l'intégration de l'intelligence artificielle pour détecter et contrer les activités illégales en ligne, ainsi qu'une sensibilisation publique généralisée, sont autant de pistes essentielles pour endiguer cette menace.