Les violences numériques en RDC : Entre banalisation des faits et répression inefficace de la cybercriminalité

Blaise LOLEKA RAMAZANI

Doctorant en Droit
Avocat au Barreau de Kinshasa/Matete
Assistant à la Faculté de Droit de l'UPN
Membre du Conseil d'administration de Droit-numerique.cd

MOTS-CLÉS

Violence numérique
Cyberviolence
Cybercriminalité
Cyberharcèlement
Cyberintimidation
deepfakes
Sextorsion
Revenge Porn
Sextape
Manosphère
VBG
ANCY

RÉSUMÉ

La révolution numérique a transformé en profondeur tous les aspects de la vie en société, donnant naissance à un nouvel espace de communication porté, entre autres, par les réseaux sociaux. Leur usage abusif est devenu source de propagation des violences numériques. Depuis plusieurs années maintenant, il s'observe, sur les réseaux sociaux, une recrudescence de discours haineux, injurieux et diffamatoires, de cyberharcèlement, de sextapes et de *deepfakes* visant tout le monde, y compris les personnalités publiques. Dans la société congolaise, ces contenus émanent aussi bien de citoyens résidant au pays que des Congolais de la diaspora. Ces derniers profitent, en outre, de leur situation géographique pour s'affranchir des poursuites judiciaires au niveau national. Cette situation fait d'Internet un espace de non-droit où l'État peine à déployer ses moyens de contrainte et de coercition. La présente étude appréhende la notion de « violences numériques » en définissant ses contours et en examinant les formes les plus courantes qu'elles peuvent revêtir. Elle analyse ensuite les mécanismes de leur répression, en mettant en lumière les initiatives congolaises de lutte contre ces fléaux.

Keywords :

Digital violence
Cyberviolence
Cybercrime
Cyberbullying
Cyberstalking
Deepfakes
Sextortion
Revenge porn
Sextape
Manosphere
GBV (Gender-Based Violence)
ANCY

ABSTRACT :

The digital revolution has profoundly transformed every aspect of social life, giving rise to a new communication space driven, among other things, by social media. Their misuse has become a source of proliferation for digital violence. For several years now, there has been a resurgence on social networks of hateful, insulting, and defamatory speech, cyberbullying, sextapes, and deepfakes targeting everyone, including public figures. In Congolese society, this content originates from both citizens residing in the country and Congolese in the diaspora. The latter also take advantage of their geographic location to evade legal prosecution at the national level. This situation turns the Internet into a lawless space where the State struggles to deploy its means of enforcement and coercion. This study conceptualizes the notion of "digital violence" by defining its boundaries and examining its most common forms. It then analyzes the mechanisms for their suppression, highlighting Congolese initiatives to combat these scourges.

INTRODUCTION

Au sens purement classique, la violence en droit pénal est un acte d'agression de nature à porter atteinte à l'intégrité physique ou psychique de la personne contre laquelle il est dirigé. Elle comprend non seulement toutes les atteintes effectivement portées à l'intégrité corporelle mais aussi, les actes ayant entrainé un trouble psychologique, même sans contact avec la victime.[1] La révolution numérique a transformé en profondeur tous les aspects de la vie en société. Elle a bouleversé le rapport de l'homme avec lui-même et vis-à-vis du monde.[2] Le monde, les sociétés dans lesquelles nous vivons se sont totalement « *internetisés*[3] ». Cette « internetisation » du monde a donné naissance à un nouvel espace de communication qu'est le cyberespace. Le cyberespace est non seulement un espace d'informations, mais aussi un espace d'actions et de rencontres des plus diversifiées avec des échanges de tous genres.[4] Il a créé de nouvelles opportunités de même qu'il a ouvert la porte à de nouvelles formes de criminalité et de violences

[1] G. CORNU, *Vocabulaire juridique,* 12e éd., Paris, PUF Quadrige, 2018, p. 2264 (V. Violence-pén).
[2] X. LEONETTI, *Guide de cybersécurité : droits, méthodes et bonne pratiques*, L'Harmattan, Paris, 2015, p.13.
[3] M. QUEMENER, *Cybersociété, entre espoirs et risques,* L'Harmattan, Coll. Justice & Démocratie, Paris, 2013, p.7.
[4] B. LOLEKA RAMAZANI, *L'enquête pénale en droit congolais du numérique : nécessité d'intégration des nouveaux outils d'investigation*, Mémoire présenté et défendu en vue de l'obtention du Diplôme d'Études Appro-ondies en Droit, sous la dir. Prof. K. Ndukuma Adjayi, UCC, 2025, p. 1.

en ligne. Ces violences sont qualifiées de *« violences numériques, cyberviolences, violences en ligne ou violences électroniques »*.

Il s'agit en réalité de tout acte commis, facilité, aggravé par l'usage des NTIC qui entraine ou susceptible d'entrainer un préjudice physique ou psychologique, y compris d'autres atteintes aux droits et libertés fondamentaux.[5] En d'autres termes, les violences numériques englobent « tous les actes agressifs, harcelants ou abusifs commis par le biais des technologies numériques qui portent atteinte à la dignité, à la sécurité ou aux droits d'une personne ». Les effets de ces actes ne se limitent pas seulement en ligne. Ils donnent souvent lieu à des violences hors ligne, dans la vie réelle, comme des actes de coercition, des violences physiques et même le féminicide[6]. Leurs effets sont réels sur la victime avec des impacts tant psychologiques (anxiété, dépression, perte d'estime de soi, troubles du sommeil), sociaux (stigmatisation, exclusion, difficultés scolaires/professionnelles), que physiques (suicide, automutilation, etc.).

Les violences numériques ciblent toute personne, homme comme femme de tous les âges. Toutefois, les statistiques démontrent qu'elles touchent beaucoup plus les femmes que les hommes. Selon ONU Femmes, une femme sur 3 dans le monde subit des violences dans sa vie et 58% des femmes sont confrontées à des violences numériques[7] particulièrement celles qui ont une forte visibilité publique en ligne, à savoir : les militantes, les journalistes, les femmes politiques, les défenseuses des droits de l'homme et les jeunes femmes dites influenceuses sur les réseaux sociaux. Les répercussions des violences numériques sont encore plus graves pour les femmes confrontées à des formes plus croisées de discrimination, notamment en raison de leur race, de leur handicap, de leur nationalité, de leur identité de genre, de leur tribu ou ethnie.

Les violences commises en ligne ne sont pas le fruit du hasard. Elles s'amplifient grâce aux propriétés du cyberespace. Ce dernier abaisse les barrières morales, facilite le passage à l'acte de l'agresseur et rend plus vulnérable les victimes. Sans être exhaustif, ces propriétés sont entre autres : l'anonymat des auteurs, le caractère parfois transfrontière des violences, la volatilité des données numériques, l'expansion de l'IA, créant une véritable culture d'impunité sur Internet. Le cyberespace permet la commission de plusieurs formes de violences. Les formes les plus proéminentes sont entre autres : le harcèlement en ligne, le chantage et la diffusion d'images intimes sans consentement (*sextapes*), les discours haineux et sexistes, la cyberintimidation, les *deepfakes*, tels que des images pornographiques truquées, ou des contenus audios modifiés par l'IA, la désinformation, l'usurpation d'identité, etc.

Dans la société congolaise, les contenus violents émanent aussi bien des Congolais résidant au pays que ceux de la diaspora. Ces derniers profitent de leur situation géographique

[5] UNWOMEN, « La violence numérique est une violence réelle : le combat d'une activiste pour la sécurité et les droits humains », 18 novembre 2025, disponible sur : [https://www.unwomen.org/fr/nouvelles/reportage/2025/11/la-violence-numerique-est-une-violence-reelle-le-combat-dune-activiste-pour-la-securite-et-les-droits-humains] (consulté le 5 avril 2026).

[6] Le féminicide correspond à l'homicide intentionnel d'une femme en raison de son sexe. Il représente à ce jour l'expression la plus extrême des violences sexistes. Lire J. DEBORDE, « Féminicide, pas français ? », *in* Libération.fr, 23 novembre 2017.

[7] [https://www.unwomen.org/fr/rejoignez-nous/16-jours-d-activisme], (consulté le 29 mars 2026).

pour s'affranchir des poursuites judiciaires au niveau national. Cette situation fait d'Internet un espace de non-droit où l'État peine à déployer ses moyens de contrainte et de coercition. Elle soulève plusieurs interrogations qui peinent à trouver des réponses adéquates :

Quelles sont les formes que les violences numériques peuvent revêtir sur Internet, espace dématérialisé où toute personne est susceptible d'être auteur ou victime du cybercrime ? Pourquoi le système pénal [congolais] ne semble pas réprimer efficacement ce type d'atteintes à la personne ? Est-ce lié aux difficultés techniques de réguler les échanges dans le cyberespace marqué par l'anonymat de ses acteurs ? Ou alors les violences numériques ne sont-elles pas des infractions au regard de la loi congolaise ? Pour y répondre, la présente étude se propose de comprendre, dans un premier temps, la notion de « violences numériques » en définissant ses contours et en examinant les formes les plus courantes qu'elles peuvent revêtir **(1)**. Dans un second temps, elle analyse les mécanismes de répression de ces violences, tout en mettant en lumière les initiatives congolaises de lutte contre ces fléaux **(2).**

1. La compréhension technique des violences numérique

La compréhension des violences commises dans l'environnement numérique commande que ses notions soient circonscrites **(A)**. C'est en suite qu'il faudrait analyser les facteurs qui favorisent leur propagation dans le cyberespace **(B)**.

A. Les notions des violences numériques

En raison du développement des TIC, les violences exercées contre les individus ont pris de nouvelles formes. On parle aujourd'hui des violences numériques qu'il convient de définir, d'identifier ses cibles et l'étendue du préjudice qu'elles peuvent causer aux victimes.

La définition des violences numériques. Il s'agit de tous les actes agressifs, harcelants ou abusifs commis au moyen des outils numériques qui portent atteinte à la dignité, à la sécurité ou aux droits d'une personne.[8] La notion de violence suppose l'absence de consentement de la part de la personne qui la subit. Les actes qui sont considérés comme violents sont ceux qui portent atteinte à l'intégrité de la personne visée en la blessant intentionnellement ou non, physiquement, s'il s'agit de coups, ou de façon psychologique, quand il s'agit de chocs visuels, de propos menaçants, dénigrants ou insultants, incluant les discours de haine, racistes, antisémites ou sexistes.[9]

Ces actes ne se produisent pas seulement en ligne, ils peuvent se traduire en violences physiques ou psychologiques envers les personnes qui en sont victimes dans la vraie vie. C'est généralement le cas lorsque, par exemple, l'entourage de la victime réagit négativement au contenu en ligne la concernant. Les actes violents peuvent commencer sur Internet et se répandre

[8] C. Blaya, « Etude du lien entre cyberviolence et climat scolaire : enquête auprès des collégiens d'Ile de France », *in* Les dossiers des sciences de l'éducation [En ligne], n°33, 1er mars 2015, p. 3. Disponible sur : [http://journals.openedition.org/dse/815] (consulté le 16 mars 2026).

[9] S. Jehel, « Les adolescents face aux violences numériques entre adhésion et résistances aux logiques de violence », Terminal [En ligne], n° 123, le 31 décembre 2018, p.1. Disponible sur : [http://journals.opene-ition.org/terminal/3226] (consulté le 16 mars 2026).

dans la vie réelle, ou vice-versa, créant un continuum très dangereux de violence en ligne et hors ligne. De plus, l'atteinte à la victime n'est pas limitée à un moment et un environnement donnés, les contenus circulant sur Internet 24h/24 et 7j/7.[10] Ces contenus violents sont difficilement effaçables et circulent en dehors du contrôle de leur victime.

Les cibles des violences numériques. Les actes de cyberviolences ciblent en général les femmes et les hommes de tous les âges (mineurs et adultes). Toutefois, ils visent plus particulièrement les femmes et les jeunes filles, notamment celles qui ont une forte visibilité publique en ligne telle que les journalistes, les militantes, les femmes politiques, les défenseuses des droits humains et les jeunes femmes dites influenceuses sur les réseaux sociaux numériques. Les effets s'amplifient encore plus pour les femmes exposées à des formes plus croisées de discrimination, notamment en raison de leur race, de leur handicap, de leur identité de genre ou de leur orientation sexuelle. Cela a conduit à l'apparition d'une catégorie de violences numériques dites *« violences numériques basées sur le genre (VNBG) »*. Elles font allusion à toute forme de violence commise en ligne pour servir d'arme contre les femmes et les filles, au seul motif de leur genre.

C'est dans ce cadre que la campagne mondiale des 16 jours d'activisme contre la violence basée sur le genre pour l'année 2025 avait pour thème : « *Tous unis pour mettre fin aux violences numériques faites aux femmes et aux filles* » et pour laquelle nous sommes intervenus en tant que formateur pour le compte de UNHCR et de ADSSE devant la communauté de réfugiés vivant à Kinshasa.[11]

Les formes courantes des violences numériques. L'omniprésence d'Internet et des réseaux sociaux [numériques] fait en sorte que les violences numériques se diversifient.[12] Elles peuvent inclure (sans se limiter) :

- le harcèlement en ligne (messages répétés et non désirés, commentaires insultants ou menaçants) ;
- la sextorsion (chantage avec images intimes, menace de diffusion sans consentement, extorsion d'argent ou de faveurs sexuelles) ;
- la vengeance pornographique (diffusion d'images intimes sans consentement pour humilier la victime) ;
- les discours haineux et sexistes (commentaires dénigrants sur le physique, remise en cause de compétence parce que femme, discours misogynes…) ;
- la cyberintimidation (infliger, de manière délibérée et répétitive, des préjudices au moyen des outils numériques dans le but de causer du tort à une personne. Il s'agit d'une variante du cyberharcèlement) ;

[10] C. BLAYA, *op.cit.*, p. 3.
[11] Dans le cadre de cette campagne, UNHCR et ADSSE avaient organisé, en date du 26 novembre 2025 dans l'Amphithéâtre de l'INRB, une journée de sensibilisation de la communauté des réfugiés vivant à Kinshasa. Nous avions animé le module portant sur les violences numériques faites aux femmes et aux filles.
[12] L. CHARTON et C. BAYARD, « Les violences contre les femmes et les technologies numériques : entre oppression et agentivité », *in* Revue Recherches féministes, Vol. 34, n°1, 2021, pp. 312-330.

- les hypertrucages (*deepfakes*) générés par l'IA (vidéos pornographiques truquées, des images, ou des contenus audios modifiés par l'IA) ;
- la désinformation ;
- la traque pour surveiller les activités d'une personne ;
- l'usurpation d'identité (créer un faux profil et se faire passer pour une autre personne à des fins malveillantes) ;
- le *doxing* (publier les informations personnelles et privées de quelqu'un sans son consentement dans l'intention de lui causer du tort).

L'impact des violences numériques pour les victimes. Comme pour les violences commises en personne, ou dans le monde « réel », les violences numériques peuvent avoir des conséquences néfastes pour les victimes. Si les violences classiques sont généralement limitées au contact physique entre l'auteur et sa victime, les violences numériques peuvent se produire en tout lieu et en tout temps en raison de l'usage des technologies numériques comme moyen de commission des actes violents.[13]

À cet effet, les conséquences qu'elles produisent sont de plusieurs ordres. Elles peuvent être soit psychologiques (stress, anxiété, dépression, perte d'estime de soi, trouble du sommeil, phobie, etc.) soit physiques (suicide, automutilation, etc.), soit sociales (stigmatisation, exclusion, difficultés scolaires/professionnelles), voire numériques (autocensure, abandon des réseaux sociaux, etc.). Les violences numériques peuvent aussi causer des préjudices économiques aux personnes qui en sont victimes.[14] Il en est ainsi lorsqu'un agresseur menace de diffuser les images intimes de sa victime si celle-ci ne lui renvoie pas une somme d'argent.

Chez les enfants mineurs, les conséquences des violences numériques peuvent être encore plus graves d'autant que ces derniers ont souvent accès à des contenus violents et choquants en ligne. En plus de leurs conséquences psychologiques, elles peuvent avoir un impact sur le développement de l'enfant, ses valeurs et ses perceptions.[15]

B. Les facteurs des violences numériques

Dans le cyberespace, plusieurs facteurs favorisent la commission des actes violents. Ces facteurs sont liés aux propriétés du cyberespace dont l'anonymat et le pseudonymat, son caractère transfrontière, la volatilité des données numériques, l'absence de responsabilisation des plateformes de réseaux sociaux, la normalisation de la violence dans la manosphère, l'expansion de l'IA, et l'insuffisance de soutien pour les victimes.

L'anonymat et le pseudonymat. L'anonymisation est le fait d'utiliser un ensemble de techniques informatiques dans le but de rendre impossible, en pratique, toute identification de

[13] Conseil de l'Europe, « Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018 : Cybercrime Convention Committee (T-CY) – Working Group on cyberbullying and other forms of online violence, especially against women and children », 9 juillet 2018, p. 40.
[14] Assemblée Parlementaire de la Francophonie, *Rapport final : la cyberviolence envers les femmes et les enfants dans l'espace francophone*, 19 janvier 2021, p. 9.
[15] *Ibidem.*

la personne par quelque moyen que ce soit et de manière irréversible.[16] De manière plus simple, l'anonymat est le fait d'agir ou de communiquer sans utiliser ou présenter son nom ou son identité légale. Pour rester anonymes, les internautes font recours à plusieurs outils numériques tels que les VPN, Tor, Proxys, etc. En revanche, le pseudonymat consiste à faire usage d'une fausse identité numérique pour interagir en ligne tout en dissimulant son identité réelle.[17]Contrairement à l'anonymat où aucune identité n'est révélée, le pseudonyme maintient une identité persistante fictive. Il est détaché de l'identité légale. Le pseudonymat offre un certain degré d'anonymat car il permet aux individus de masquer leur identité réelle. Ces deux techniques facilitent la commission des actes de violence numérique d'autant que les cyberdélinquants n'ont aucune crainte d'être immédiatement identifiés et traduits en justice.

Le caractère transfrontière des cyberviolences. Le caractère international et transfrontière des violences résulte de la nature même du cyberespace. Ce dernier est un espace dématérialisé dans lequel s'opèrent les échanges déterritorialisés entre citoyens de toutes nations à une vitesse instantanée. Il abolit toute notion de distance et de frontière.[18] L'Internet offre la possibilité aux cybercriminels de se livrer à quasiment n'importe quelle activité criminelle au plan international.[19] Un auteur peut être à Paris et viser une victime à Kinshasa en quelques secondes. Contrairement aux violences physiques qui obligent (toujours) une présence en personne de l'auteur et de la victime, les violences numériques s'affranchissent dans bien des cas, des frontières étatiques. Le délinquant n'a plus besoin de se déplacer. Cette barrière physique crée une culture d'impunité sur Internet. C'est pour cette raison que nombreux sont des Congolais de la diaspora pour la plupart, qui s'adonnent à des actes de violence en ligne, notamment des discours injurieux, diffamatoires ou tribaux, le cyberharcèlement […] sans crainte d'être poursuivis d'autant qu'ils se [re]trouvent en dehors des frontières nationales.

La volatilité des données numériques. Dans l'environnement numérique, les preuves s'avèrent difficiles à rapporter.[20] C'est le cas par exemple lorsqu'un internaute tient des propos diffamatoires contre une personne sur Internet mais n'en garde aucune trace sur son téléphone ou son disque dur. Il s'agit là de la nature volatile des données informatiques. Cette volatilité résulte de la possibilité de modifier et de supprimer des éléments de preuve de manière quasi-instantanément.[21] Un exemple patent de la volatilité est la fonctionnalité *« messages éphémères »* de la plateforme de messagerie *WhatsApp*. Ainsi, dans une discussion individuelle, chacun des deux utilisateurs peut activer les messages éphémères. Une fois cette fonctionnalité

[16] CNIL, « L'anonymisation des données personnelles, Mise au point sur les techniques utilisables et sur leurs enjeux », 19 mai 2020, Disponible sur [https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles] (consulté le 29 mars 2025).
[17] B. Loleka Ramazani, *L'enquête pénale en droit congolais du numérique : nécessité d'intégration des nouveaux outils d'investigation, op.cit.,* p. 48.
[18] K. Ndukuma Adjayi (sous la dir.), A. Diangienda Mvete, B. Loleka Ramazani, *Droit du commerce électronique : Enjeux civils, consuméristes, cybercriminels, d'extranéité et de déterritorialité*, L'Harmattan, Paris, 2021, p.332.
[19] *Idem*, p. 333.
[20] Ch. Feral-Schuhl, *Cyberdroit : Le droit à l'épreuve de l'internet*, 4e éd., Dalloz, Paris, 2006, p. 657.
[21] A. Caprioli, « Traçabilité et droit de la preuve électronique », Droit & Patrimoine, n° 93, mai 2001, p. 68-75, mise à jour le 20 octobre 2013 *in* [https://www.caprioli-avocats.com], (consulté le 20/03/2026).

activée, les nouveaux messages envoyés dans la conversation disparaitront au terme de la durée programmée. Cette fonctionnalité peut rendre difficiles les investigations pénales en ce qu'elle a vocation de faire disparaitre les éléments de preuves d'un acte criminel. Dans une telle situation, il est conseillé à la victime de conserver ne fût-ce que les captures d'écran à titre de preuve.

L'absence de responsabilisation des plateformes des réseaux sociaux. Avec le développement du *Web 2.0*, une véritable sociabilité de l'Internet s'est mise en place autour des plateformes qui rassemblent des individus ayant les mêmes centres d'intérêts. Ces plateformes de réseaux sociaux sont utilisées par leurs membres pour maintenir le contact avec leur groupe et apprendre très vite à organiser, voire mettre en scène, leur vie privée.[22] Le fonctionnement économique de ces plateformes, peu régulées et de façon opaque et arbitraire, favorise la circulation des contenus violents, sexuels et haineux en particulier sur *YouTube, TikTok, Facebook, Instagram, Twitter, Telegram et WhatsApp*.[23]

Dans la circulation des contenus sur ces plateformes, les individus peuvent occuper des positions diverses telles que : récepteurs, partageurs, likeurs, émetteurs, témoins, victimes, agresseurs voire complices.[24] Leur conception doit être règlementée afin de limiter la propagation des contenus violents. Au-delà de leur mission de modération via des algorithmes, chaque plateforme devrait définir dans les CGU ce qu'elle considère comme « contenu violent », afin de pouvoir le retirer. Elles doivent également proposer aux utilisateurs des outils leur permettant de signaler facilement les contenus illicites.[25] Dans bien des cas, elles déclinent leur responsabilité face aux contenus violents mis en ligne par les utilisateurs pour la simple raison qu'elles ne sont pas des éditeurs de contenu mais de simples hébergeurs.

La normalisation de la violence dans la manosphère. La manosphère est un ensemble décentralisé et inter-plateforme de communautés en ligne, comme des groupes de discussion, des forums et des blogs, unis par leur opposition au féminisme.[26] Dans la manosphère, les hommes sont présentés comme les victimes du climat sociétal actuel, avec un contenu axé sur différentes thématiques telles que des représentations dénigrantes des femmes et des filles, des hostilités communes à l'égard des mouvements féministes, et des mythes nuisibles sur l'égalité des sexes et la violence à l'égard des femmes. La manosphère se décompose souvent en plusieurs mouvements qui prônent tous la haine contre les femmes. Les plus remarquables

[22] L. GRYNBAUM, C. GRENOFFIC et L. MORLET, *Précis du droit des activités numériques*, 1ère Ed., Paris, Dalloz, 2014, p. 30.
[23] CEMEA, « Région Normandie Observatoire des pratiques numériques des adolescents, […] », 2018. Disponible sur : http://educationauxecrans.fr/index.php/le-dispositi -ulté le 10 a ril 2026).
[24] S. JEHEL, « Les adolesce ts face aux violences numériques entre adhésion et résistances aux logiques de violence », *op.cit.,* p. 2.
[25] A. FAVREAU, *L'essentiel du droit du numérique,* Gualino Lext nso, Clamecy, 2024, p. 141.
[26] Rapport du S de l'ONU, « Intensificat on de l'action menée pour éliminer toutes les formes de violence à l'égard des fe mes et des filles : violence c ntre les femmes et les filles facilitée par les technologies », n°A/79/500, octobre 2024, p. 10.

sont : *Pickup Artist* (PUA)[27], Men *Going Their Own Way* (MGTOW)[28], Activistes des droits des hommes (MRA), et Incels[29].[30]

De manière générale, la manosphère est caractérisée par la normalisation de la violence à l'égard des femmes. Elle encourage le cyberharcèlement, les menaces de mort contre les femmes, le partage non consenti de contenus intimes, voire à des tueries de masse. Comme tous les autres facteurs, la manosphère favorise la culture d'impunité d'autant que les agresseurs font recours à plusieurs techniques pour étendre leur champ d'action et éviter les sanctions. Ces techniques sont entre autres l'anonymat et le pseudonymat, le contournement de la modération des plateformes par l'usage d'un langage codé, l'inversion de la culpabilité, etc. Cette atmosphère d'impunité permet aux groupes de la manosphère de fonctionner comme de véritables « incubateurs de la haine », où la violence n'est pas uniquement tolérée, mais parfois présentée comme acte de résistance contre l'égalité des sexes.

L'expansion de l'IA générative. Le développement de l'IA générative permet de créer des contenus (vidéo, image, texte, code, etc.) à partir des requêtes en langage naturel appelées « *prompts* ». À la différence de l'IA classique qui se limite à analyser et classer les données, l'IA générative produit de contenus originaux qui imitent la création humaine. Malgré les aspects positifs, l'IA peut être utilisée à des fins malveillantes, notamment pour faciliter la commission des actes violents. Elle peut créer automatiquement de contenus violents tels que les messages blessants, les discours haineux ou les campagnes pour nuire à l'intégrité et à la réputation de personnes sur Internet. Elle permet aussi de créer des *deepfakes* (vidéos et images truquées à caractère sexuel, enregistrements audios, etc.), avec la même intention de nuire à autrui et de le discréditer.[31] L'un des exemples d'IA générative qui encourage la violence est celle développée par la plateforme X au nom de « Grok AI ». Cette IA permet à ses utilisateurs, majoritairement des hommes, de déshabiller les femmes et les enfants, de générer des insultes sexistes et des discours haineux via des chatbots d'IA. Bref, l'IA générative permet de générer à l'infini de tels contenus, brouillant ainsi les pistes entre réalité et virtuelle.[32] Les agresseurs

[27] Le terme PUA désigne une un mouvement d'hommes qui e concentrent sur l'amélioration de leur compétences en sé uction des femmes.

[28] Le terme MGT W signifie littéralement « les hommes s ivent leur propre chemin ». Il s'agit d'un mouvement masculiniste qui prône le désengagement total des relations avec les femmes. Ses adeptes estiment que les femmes sont énales, superficielles, manipulatrices et toxiques. Les MGTOW détestent les femmes et choisissent de rest r célibataires pour les puni en se concentrant exclusivement sur leur propre liberté et épanouis--ement person el.

[29] Le terme « I cel », est une abréviation de « célibataires involontaires, en anglais Involuntary celibate ». Il s'agit d'une communau é des hommes qui ne se sentent pas attrayants physiquement ou qui n'ont pas eu d succès avec es femmes en amour dans la vraie vie.

[30] Commission E ropéenne, « Incels : première a alyse du phénomène (dans l'UE), et impa t et difficultés associées su le plan de la prévention et de la lutte contre l'extrémisme v olent », 2021, p.4

[31] A. FADOUA HACHIMI, « Cyberint midation et humiliation à l'ère de l'intelligence artificielle : reconfigurations de la violen e numérique », Aleph, Vol. 12, n°5, 15 février 2026, Disponible sur : [https://aleph.edinum.org/1587 #]

[32] Rapport de l Fondation pour l'Enfance, « L'IA générativ , nouvelle arme de la pédocriminalité », octobre 2024, p. 10. Disponible sur : [https://w w.fondation-enfance.org/ p-content/uplo ds/2024/10/Fondation-enfance-Rapport-Cyber-Web.pdf]

qui en font usage se sentent moins responsables à cause de l'anonymat et peuvent à cet effet propager à grande échelle les contenus violents.

L'insuffisance des systèmes de soutien pour les victimes. Près de la moitié des victimes de violences numériques dans le monde en général et en RD Congo en particulier ne bénéficient pas [souvent] d'un cadre de soutien suffisant. Malgré le lancement en novembre 2025 de la campagne nationale « #jedénonce 2025 » par le Réseau des journalistes pour la promotion des droits de la femme (RJPF) appelant les Congolais à soutenir les victimes des violences numériques.[33], le paysage numérique congolais reste dominé par l'absence d'un cadre de soutien adéquat pour les victimes de ce fléau mondial. Ainsi, bon nombre de victimes finissent par normaliser les violences et subissent un isolement forcé sur toutes les plateformes de communication électronique par peur des jugements, du blâme ou de la stigmatisation.

2. Le cadre congolais de répression des violences numériques

Au-delà de la compréhension technique et théorique du phénomène, il est fondamental d'examiner la manière dont le droit pénal congolais réprime les actes de violence en ligne. Cet examen se fait sous deux axes complémentaires : l'étude des incriminations courantes de violences numériques **(A)** et l'analyse de quelques initiatives institutionnelles de lutte contre ce fléau en RDC **(B)**.

A. Les incriminations courantes de violences numériques

Au vu des caractéristiques des violences numériques telles que décrites précédemment, il est évident qu'elles soient incriminées par la loi pénale. En effet, si on se réfère à l'arsenal pénal congolais, on constate que toute atteinte à la dignité et à l'honneur sur Internet, qu'elle relève de l'atteinte à l'image, d'actes répétés ou de violences basées sur le genre, est punissable par la loi. Cela inclut la pornographie infantile, le revenge porn, la sextorsion, le cyberharcèlement, l'usurpation d'identité, les violences numériques basées sur le genre, etc.

- ***La pornographie infantile***

Autrement appelée la cyberpédonographie, la pornographie infantile correspond à une forme particulièrement grave d'exploitation sexuelle des enfants.[34] Ce phénomène prend de l'ampleur sur le plan mondial avec l'explosion des technologies numériques. À ce jour, Internet facilite la création de plus de 100 000 sites Internet dédiés à la pornographie mettant en scène les enfants.[35] Ayant pris en compte l'impact des réseaux numériques dans la propagation des contenus pédopornographiques, le législateur congolais avait déjà, à travers la loi n°06/018 du 20 juillet 2006 sur les violences sexuelles, introduit l'article 174-m dans le Code pénal. Cet article punit de cinq à dix ans de servitude pénale au titre de la pédopornographie, toute per-

[33] ACP, « 16 jours d'activisme, l s congolais appelés à soutenir les victimes des violences numériques », 25 novembre 202 , Disponible sur : [https://w w.acp.cd/genre/ les-congolais-appeles-à-soutenir-les-victimes-des-violences-numériques] consulté le 01mai 2026).
[34] M. Quemener, *Cybersociété entre espoirs et risques, op.cit,* p. 144.
[35] *Ibidem.*

sonne qui aura fait toute représentation, par tout moyen (sur Internet y compris), d'un enfant s'adonnant à des activités sexuelles ou toute représentation des organes sexuels d'un enfant, à des fins sexuelles.

Le dispositif pénal en la matière a évolué au fil du temps afin de prendre en compte tout type de comportement ayant trait à la pédopornographie en ligne. C'est ainsi qu'en 2020, la loi relative aux télécoms et aux TIC définit la pornographie infantile comme *« toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite »*.[36] Son article 193 punit d'une peine de servitude pénale principale de cinq à dix ans et/ou d'une amende de cinq millions à 15 millions de Francs congolais, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet, importe ou fait importer, exporte ou fait exporter une image ou une représentation comportant un caractère de pornographie infantile par le biais d'un système de communication électronique.

Tenant compte du développement grandissant de ce phénomène, le code du numérique a aggravé la peine de servitude pénale, allant jusqu'à 15 ans de servitude pénale et de 2 000 à 1 000 000 francs congolais d'amende.[37]

– ***La vengeance pornographique (Revenge Porn)***

Dérivée de l'anglais *revenge porn*, la vengeance pornographique consiste à se venger d'une personne en rendant publics des contenus dits pornographiques qui l'incluent. Cela dans le but évident de porter atteinte à son honneur et à sa réputation. Ces contenus compromettants peuvent être réalisés avec ou sans l'accord de la victime alors que dans les deux cas, elle n'a jamais donné son consentement pour leur diffusion ou publication.[38]

Un tel agissement est constitutif de l'infraction prévue à l'article 181 de la loi relative aux télécoms et aux TIC. Cet article punit le fait pour toute personne, de transmettre ou de mettre en circulation sur la voie des télécoms et des TIC des signaux, images et messages obscènes, […]. Le taux de la peine est fixé entre six mois et un an de servitude pénale et/ou d'une amende d'un à dix-millions de francs congolais.

– ***La sextorsion***

Le terme anglais « *sextorsion* » est une contraction des mots « *sex* » et « *extortion* » (terme anglais qui désigne le chantage). Il s'agit d'une forme de chantage exercé sur une personne dont on détient des images compromettantes afin de recevoir de cette dernière une rançon.[39] Dans la pratique, cela est possible lorsque par exemple le cybercriminel se fait passer

[36] Article 4 po nt 76, loi n°20/017 du 20 novembre 2020 relative aux télécommunications et aux technologies de l'information t de la communication, préc.
[37] Article 357, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.
[38] K. NDUKUMA ADJAYI (sous la dir), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du com erce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité e de* déterritoria ité, *op.cit.,* p. 320.
[39] *Idem,* p. 320.

pour une personne attirante derrière un faux compte TikTok. Il va par la suite entrer en contact avec sa cible. Après avoir établi une relation de confiance, il demande à cette dernière les photos ou vidéos la montrant nue ou en train de réaliser un acte sexuel. Une fois que la cible aura envoyé les images ou vidéos demandées, le criminel lui brandit la menace de les diffuser si elle ne lui paie pas une rançon. Il en est de même lorsqu'un criminel parvient à installer un logiciel malveillant dans l'ordinateur ou le Smartphone à l'insu de la victime.

Cette infraction peut être punie sur base de l'article 358 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique qui incrimine le cyberharcèlement et de l'article 84 du Code pénal qui punit l'extorsion. Toutefois, lorsque la menace ou le chantage de publier les images de la victime est exercé en raison de son genre, le juge peut appliquer l'article 174u du Code pénal congolais tel que modifié et complété par l'ordonnance-loi n°23/023 du 11 septembre 2023 qui incrimine les violences basées sur le genre à travers les réseaux de communication ou d'information.

– ***Le cyberharcèlement***

Le cyberharcèlement est issu du terme anglais *« cyberbullying »* qui signifie brutaliser. Il se traduit en français par « cyberharcèlement, cyberintimidation, ou harcèlement virtuel ».[40] Il fait référence à l'usage d'Internet pour harceler une personne de diverses manières. Le harcèlement peut avoir une connotation sexuelle, des contacts inappropriés ou une surveillance intrusive de la vie privée. Il se caractérise par les menaces, l'espionnage, les fausses accusations, le vol d'identité et la manipulation. Les cyberharceleurs font usage de courriers électroniques et de tous les moyens de communication pour accomplir leurs méfaits. C'est notamment le cas lorsqu'une personne reçoit de manière répétitive sur sa messagerie, plusieurs messages de menace de mort.

Au sens classique, le Code pénal tel que complété par la loi n°06/018 du 20 juillet 2006 sur les violences sexuelles ne contenaient pas de dispositions réprimant le harcèlement de manière générale. Il se limitait uniquement à réprimer le harcèlement sexuel.[41] Il a fallu attendre jusqu'en 2023 pour que le législateur puisse renforcer le dispositif de répression avec la montée des NTIC. C'est ainsi que l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique prévoit et punit de manière générale le harcèlement commis par le biais des outils numériques.

Cette incrimination consiste dans le fait « *d'initier une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un SI dans le but d'encourager un comportement haineux, tribal et hostile aux bonnes mœurs et aux valeurs patriotiques*[42]». Le coupable est puni d'un mois à deux ans de SP et de 500 000 à 10 000 000 de Francs congolais d'amende. Il en est de même de celui qui aura harcelé à travers les outils numériques alors qu'il savait ou aurait dû savoir que son comportement

[40] M. QUEMENER, *Cybersociété entre espoirs et risques, op.cit,* p. 153.
[41] Article 174d Code pénal.
[42] Article 358, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

affecterait gravement la tranquillité de la personne visée.[43] De plus, le fait de relayer une fausse information contre une personne pas le biais des réseaux sociaux, ou des plateformes numériques est également constitutif de harcèlement. Son auteur est puni d'un à six mois de SP et/ou d'une amende de 500 000 à 1 000 000 de Francs congolais.[44]

– ***Le tribalisme, le racisme et la xénophobie en ligne***

La diffusion de propos à caractère raciste, tribaliste et xénophobe est facilitée à ce jour par l'Internet, vecteur qui atteint un vaste public et qui rapproche aussi les auteurs de tels messages.[45] Les messages, images, vidéos et contenus racistes, tribalistes ou xénophobes qui circulent sur Internet peuvent relever, sur le plan pénal, des mêmes catégories juridiques que ceux diffusés par la voie de l'écrit et sont susceptibles de constituer des infractions. Dans l'arsenal pénal congolais, ces actes sont réprimés par trois textes distincts, à savoir l'ordonnance-loi n° 66-342 du 07 juin 1966 portant répression du racisme et du tribalisme, la loi relative aux télécoms et aux TIC et l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique.

Aux termes de l'article 194 de la loi relative aux télécoms et aux TIC, il est coupable de racisme et de xénophobie, « *toute personne qui crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou théories, de nature raciste ou xénophobe, par le biais d'un système de communication électronique sera punie d'une peine de cinq à dix ans de servitude pénale principale et/ou d'une amende d'un à dix-millions de Francs congolais* ».

En revanche, l'article 356 du code du numérique punit au titre de racisme, de tribalisme et de xénophobie, *« le fait de créer, de télécharger, de diffuser ou de mettre à la disposition du public par le biais d'un système informatique des écrits, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste, tribaliste ou xénophobe […] ».* Le coupable est puni d'une servitude pénale d'un mois à deux ans et/ou d'une amende de 1 à 10 000 000 de francs congolais.

– ***Les violences numériques basées sur le genre (VNBG)***

Au fil du temps, la vie en société devient de plus en plus dépendante des technologies numériques. Ces dernières deviennent des moyens privilégiés pour commettre des actes de violence basée sur le genre. En vue de lutter efficacement contre cette catégorie de violence liée au genre de la victime, le législateur congolais a inséré une disposition dans le Code pénal à travers l'ordonnance-loi n°23/023 du 11 septembre 2023 modifiant et complétant le décret du 30 janvier 1940 portant code pénal congolais. Son article 174-u incrimine le fait de « *se procurer, de publier ou de menacer de publier des informations sur internet de nature à porter atteinte à l'honneur ou à la réputation d'une personne en raison de son genre* ». Le coupable est puni

[43] Article 359, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.
[44] Article 360, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.
[45] K. NDUKUMA ADJAYI (sous la dir), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du com erce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité e de déterritoria ité, op.cit.,* p. 321.

d'une servitude pénale principale de trois à cinq ans et/ou d'une amende de 5 à 10 millions de francs congolais. En cas de récidive, le coupable est puni de 5 à 10 ans de SPP et/ou d'une amende de 10 millions de francs congolais.

– ***L'usurpation d'identité numérique***

L'identité numérique est l'ensemble des contenus publiés sur Internet qui permettent de définir un individu.[46] Elle se construit grâce à des contenus mis en ligne sur diverses plateformes [numériques], notamment sur les médias sociaux : blogs personnels, profils sur les réseaux sociaux, contenus partagés, commentaires, etc. À l'image de l'identité classique, l'identité numérique à de nombreuses facettes avec nos adresses IP, nos e-mails, pseudonymes, nos alias, URL, avatars informatiques ou toutes autres données permettant de nous identifier en ligne.[47]

L'usurpation d'identité se trouve dans le comportement d'une personne qui s'attribue une identité à laquelle il ne peut prétendre.[48] Elle fait référence à l'utilisation des éléments d'identité d'une personne sans son consentement afin d'accomplir des actes illicites.[49] Elle devient une infraction lorsqu'elle est préjudiciable soit à l'égard de la personne dont l'identité a été usurpée, soit pour les tiers trompés par l'utilisation de la fausse identité. Les usurpateurs d'identité exploitent les informations personnelles de leurs victimes pour réaliser plusieurs actions illégales sur les réseaux numériques. Dans la plupart de cas, ces actions consistent à l'utilisation frauduleuse des comptes existants, à ouvrir de nouveaux comptes au nom de la victime, à obtenir frauduleusement des allocations, services ou documents administratifs, à négocier des données personnelles sans autorisation[50] ou obtenir tout avantage quelconque au nom de la victime dont l'identité a été usurpée.

L'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique réprime l'infraction d'usurpation d'identité à son article 351. Cette disposition incrimine *« le fait d'usurper l'identité d'autrui ou les données permettant de s'attribuer faussement et de manière illicite l'identité d'autrui dans le but de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts* ». Le coupable est puni de 1 à 5 ans de SP et de 20 à 100 millions de francs congolais au titre d'amende.[51] De la même manière, toute personne qui aura transféré,

[46] B. LOLEKA RAMAZANI, « Le droit con olais face aux enjeux de protection de l'identité num rique : quel regard prospectif ? », *op.cit.*, p. 5.
[47] GUY DE FELCOURT, *L'usurpation d'identité ou 'art de la fr ude sur les données personnelles*, CNRS Editi n, Paris, 2011, p. 106.
[48] C. LACROIX, « Rép. Pén », Dalloz, j in 2012, V° usurpation d'identité, n° , cité par É. STELLA, *L'adaptation du droit pén l aux réseaux sociaux en ligne*, Thèse en v e de l'obtention du grade de Docteur en droit privé et sciences cri inelles présentée et soutenue publiquement le 12 décembre 2019, sous la dir. Frédéric STASIAK, Université d Lorraine, Lorraine, 2019, p. 158.
[49] B. LOLEKA RAMAZANI, « Le droit con olais face aux enjeux de protection de l'identité num rique : quel regard prospectif ? », Dossier n 5, *in* Droit-numérique.cd 05 janvier 2025, p. 9. Disponible sur : [https://d oitnumerique.cd/le-droit-congolais-face-aux-enjeux-de-protection-de-lidentité-numérique-quel- regard-prospectif/] (consulté le 04 février 2025).
[50] OCDE, « Document exp oratoire sur le vol d'identité en igne », *op.cit,* p. 6.
[51] Article 351 l.1, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

possédé ou utilisé un moyen de s'identifier à une autre personne dans l'intention de commettre l'infraction, d'aider ou d'encourager une activité illégale sera punie d'une peine de deux à cinq ans de servitude pénale et/ou d'une amende de 5 à 100 millions de francs congolais.[52]

De plus, l'auteur de l'usurpation d'identité peut également être sanctionné sur base de l'article 69 du code de la famille. Toutefois, cet article se limite uniquement à punir « l'usurpation volontaire et continue d'un nom d'un tiers ». Son auteur est puni de sept jours à trois mois de servitude pénale et/ou d'une amende allant de 500.000 à 1.000.000 de francs congolais.

B. Quelques initiatives institutionnelles de lutte contre des violences numériques en RDC

Ayant conscience de l'ampleur de la cybercriminalité en général et des comportements violents en ligne, l'État congolais n'est pas resté passif. Il a adopté des mesures concrètes instituant les organes chargés de prévenir, de détecter et de réprimer ces actes criminels. Ces organes sont entre autres : le Conseil National de Cyberdéfense, l'Agence Nationale de Cybersécurité et le Tribunal pénal économique et financier.

1. Le Conseil National de cyberdéfense et ses plateformes de signalement

Le Conseil National de Cyberdéfense (CNC) est un service spécialisé au sein du Cabinet du Président de la République créé par ordonnance n° 23/170 du 15 août 2023 pour renforcer la sécurité numérique du pays. Le CNC incarne la volonté de la RD Congo de se doter d'une structure de coordination stratégique pour faire face aux défis de la cyberdéfense. Son rattachement direct à la Présidence et son autonomie administrative et financière[53] soulignent son importance dans le paysage sécuritaire national.

Même si l'ordonnance n° 23/170 du 15 août 2023 portant création du CNC ne lui confère pas textuellement la mission de lutter contre la cybercriminalité en général, une lecture croisée de ce texte démontre qu'il peut exercer cette mission par extension et par rattachement, sans préjudice du principe général de droit selon lequel « la compétence est d'attribution ». En exerçant ses missions de supervision des systèmes nationaux de cyberdéfense et de cyber-renseignement telles que prévues à l'article 2 de l'Ordonnance n° 23/170 du 15 août 2023, le CNC englobe nécessairement la lutte contre la cybercriminalité. Cette dernière notion est intrinsèquement liée à la cyberdéfense et au cyber-renseignement.

C'est dans ce cadre que le CNC avait mis en place deux plateformes de signalement des contenus violents sur Internet. Il s'agit de « https://cyberalerte.cnc.cd/ » et de «https://alertevip.cnc.cd/ ». Le premier concerne le signalement des cybermenaces contre tous les citoyens et le second concerne les cybermenaces contre les personnalités publiques et politiques. Ces deux plateformes ont été créées pour servir de point de contact centralisé pour tous les citoyens, entreprises et institutions publiques afin de :

[52] Article 351 l.2, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.
[53] Article 1er, Ordonnance n°23/170 du 15 août 2023 portant création, organisation et fonctionnement d'un service spécial sé au sein du Cabinet du Président de la République dénommé Conseil National de Cyberdéfense, en sigle « CNC ».

- signaler des incidents de cybersécurité (piratage, hameçonnage, ransomware, fraudes en ligne, etc.) ;
- dénoncer des contenus illicites circulant sur Internet (cyberharcèlement, discours de haine, *fake news*, etc.) ;
- demander de l'assistance en cas de suspicion d'attaque.

Elles proposent un formulaire en ligne où les internautes peuvent facilement décrire l'incident, fournir des preuves (captures d'écran, emails, URL, etc.) et laisser leurs coordonnées pour un suivi. Les signalements sont reçus et traités par les équipes d'experts du CNC, qui peuvent alors initier des investigations, alerter les autorités compétentes ou coordonner la réponse à l'incident. Ces plateformes offrent un canal officiel et unique pour tous les signalements, ce qui permet une meilleure coordination de la réponse nationale. Elles encouragent la population à participer activement à la sécurisation de l'espace numérique congolais.

2. Le rôle de l'Agence Nationale de Cybersécurité en matière de cybercriminalité

La RD Congo s'est engagée dans une transformation numérique ambitieuse et structurée, tout en mettant en place les garanties nécessaires pour protéger son cyberespace et assurer un développement technologique sécurisé et durable. C'est dans cette ligne de conduite que le Code du numérique crée un organisme public en guise de cadre institutionnel pour le secteur de la cybersécurité, à savoir : l'Agence Nationale de Cybersécurité (ANCY).[54] Son organisation et son mode de fonctionnement sont définis par ordonnance présidentielle n°26/033 du 16 mai 2026 portant organisation et fonctionnement d'un Organisme public dénommé Agence Nationale de Cyberdéfense.[55]

L'ANCY est un établissement public doté de la personnalité juridique, chargé d'assurer la protection et la résilience des infrastructures numériques en RD Congo. Placée sous l'autorité directe du Président de la République, elle constitue l'organe national de référence en matière de cybersécurité et de sécurisation des systèmes d'information.[56]

Elle est responsable de plusieurs missions essentielles prévues aux articles 278 du code du numérique et 3 de l'Ordonnance n°26/033 du 16 mai 2026. Ces missions sont entre autres : *[…] - accompagner et collaborer dans la lutte contre la Cybercriminalité avec d'autres organismes et institutions publics ; - contribuer, en ce qui concerne ses missions, à l'application des accords, traités et conventions relatifs à la Cybersécurité et à la lutte contre la Cybercriminalité ratifiée par la RDC ; […].*

Les agents assermentés de l'ANCY, qui réalisent des enquêtes en cybersécurité, ont le statut d'Officier de police judiciaire (OPJ) à compétence restreinte. Cela signifie qu'ils ont le pouvoir d'enquêter sur des incidents de cybersécurité mais uniquement dans leur domaine de

[54] Article 274, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, préc
[55] Ordonnance n 26/033 du 16 mai 2026 portant organisation et fonctionnement d'un Organisme public dénommé Agence Nationale de Cyberdéfense, en sigle « ANCY », JO RDC, 6 e année, n° sp cial, 22 mai 2026.
[56] Article 275, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, préc

compétence.[57] Ils prêtent serment selon les règles du droit commun. Lorsqu'ils réalisent une enquête, ils rédigent deux types de rapports : un rapport administratif, envoyé à leur hiérarchie et un autre rapport judiciaire, transmis au Ministère public, qui peut engager des poursuites judiciaires si nécessaire.

Malgré la signature de l'Ordonnance n°26/033 du 16 mai 2026 portant organisation et fonctionnement de l'ANCY, cet organisme public n'est pas encore opérationnel sur le plan pratique à l'heure où nous écrivons…

3. La compétence des juridictions congolaises en matière de cybercriminalité

À l'échelon mondial, Internet offre la possibilité aux cyberdélinquants de se livrer à quasiment n'importe quelle activité criminelle au plan international.[58] Il est en ce sens primordial que tous les États du monde fassent évoluer leurs législations, de façon que les infractions commises dans le cyberespace ne restent pas impunies. C'est dans cette lancée que le législateur congolais du code du numérique a fait évoluer les critères de compétence du juge congolais pour faire face au caractère universel et mondial du réseau Internet. Pour ce faire, les solutions envisagées par le code du numérique sont multiples.

De manière générale, les articles 328 et 329 du code du numérique fixent les règles de compétence des juridictions congolaises pour poursuivre les infractions commises dans l'environnement numérique. Ainsi, l'article 329 établit les règles spéciales de compétence des juridictions congolaises en dehors de celles de droit commun. Ainsi, les juridictions congolaises sont compétentes lorsque :

- *« l'infraction a été commise sur internet sur le territoire de la RDC ou non dès lors que le contenu illicite est accessible depuis la RDC » ;*[59]

Il ressort de cette disposition que le juge congolais est compétent pour toute infraction commise sur Internet dès lors que le contenu illicite est accessible depuis la RDC. Le juge peut appliquer la loi congolaise aux sites Internet même établis hors du territoire national, à la seule condition qu'ils soient accessibles depuis la RDC.

Cependant, le caractère ubiquiste de l'Internet amène à rendre disponibles les sites Internet dans le monde entier. Le code du numérique ne précise pas si l'accessibilité du site doit être volontaire, c'est-à-dire qu'il doit s'agir du ciblage du public congolais ou de l'accessibilité passive c'est-à-dire la simple disponibilité technique. Ce principe d'accessibilité pourrait entrainer une interprétation trop large qui risquerait d'engorger les tribunaux ou de viser les acteurs étrangers qui n'ont pas de lien réel direct avec la RDC sachant que le droit pénal congolais

[57] Article 280 1 1, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, préc
[58] K. NDUKUMA ADJAYI (sous la dir), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du com erce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité e de déterritorialité, op.cit,* p. 333
[59] Article 329 oint 1, ordonnance-loi n° 23/01 du 13 mars 2023, préc.

est basé sur le principe de territorialité de l'infraction.[60] S'agit-il d'une compétence mondiale ou universelle ? La question demeure…

– *« La personne physique ou morale s'est rendue coupable, sur le territoire de la RDC, 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 »*[61] ;

Cette disposition consacre le principe de la double incrimination ou de la réciprocité législative. Il s'agit là d'une condition pour que le juge congolais puisse assoir sa compétence. L'infraction doit être punie à la fois par la loi congolaise et par la loi étrangère pour poursuivre un complice en RD Congo. Cette condition de la double incrimination nous parait potentiellement restrictive. Elle pourrait être la source d'impunité car si la loi étrangère ne prévoit pas de sanction pour l'infraction, le juge congolais ne pourra pas poursuivre le complice, et ce, malgré la gravité de l'acte.

– *« l'infraction a été commise par des Congolais hors du territoire de la RDC et que les faits sont punis par la législation du pays où ils ont été commis »*[62].

Cet alinéa renforce la compétence des juridictions congolaises pour les infractions commises par des Congolais à l'étranger. Il suffit que les faits soient punis par la loi du pays dans lequel ils ont été commis pour que le juge congolais soit compétent. Comme pour l'alinéa 2 précité, cet alinéa consacre également la condition de la double incrimination afin d'assoir la compétence extraterritoriale des juridictions congolaises en matière de cybercriminalité.

Là encore, sa mise en application pose problème. Ce problème se présente sous deux aspects. Le premier aspect commande que l'infraction soit commise par un ressortissant congolais à l'étranger (principe d'extranéité). Le deuxième impose que l'infraction poursuivie soit punie par la loi étrangère afin que les juridictions congolaises puissent établir leur compétence. Dans un tel contexte, l'application de la loi pénale interne dépendra nécessairement de la loi pénale du lieu de la commission de l'infraction. De manière générale, l'article 329 sous examen est progressiste dans sa portée extraterritoriale. Toutefois, il manque des précisions techniques, ce qui pourrait limiter son efficacité dans la pratique.

4. La compétence du Tribunal pénal économique et financier en matière de cybercriminalité

L'évolution du cadre juridique congolais a conduit à une spécialisation plus poussée de la compétence matérielle des juridictions congolaises en matière de cybercriminalité. Ainsi, pour réprimer efficacement les infractions cybercriminelles, l'ordonnance-loi n°26/007 du 14 mars 2026 portant création, organisation, fonctionnement et compétences du tribunal pénal économique et financier (TPEF) confie cette compétence à cette nouvelle juridiction [à créer]. Aux termes de son article 6 point 9, le TPEF connait, à titre exclusif, des infractions « *[…] liées aux*

[60] Article 149 l.3, Constitution, Article 2, code pénal, rticle 67, loi organique n°13/011-B du 11 avri 2013 portant orga isation, fonctionnement et compétence des juridictions de l'ordre judici ire.
[61] Article 329 oint 2, ordonnance-loi n° 23/01 du 13 mars 2023, préc.
[62] Article 329 oint 3, ordonnance-loi n° 23/01 du 13 mars 2023, préc.

TIC et aux services associés notamment celles prévues et punies aux articles 168 à 198 de la loi n°20/017 du 25 novembre 2020 relative aux télécoms et aux TIC ainsi que les articles 308 à 382 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique ».

Cette énumération n'est pas exhaustive d'autant que bon nombre d'infractions commises dans l'environnement numérique sont prévues par d'autres textes en dehors de ceux cités à l'article 6 sous examen. C'est notamment le cas du décret du 30 janvier 1940 portant code pénal tel que modifié et complété à ce jour[63], l'ordonnance-loi n°23/023 du 11 septembre 2023[64], et l'ordonnance-loi n°66-342 du 07 juin 1966 portant répression du racisme et du tribalisme, etc.

Cependant, l'alinéa 2 de cet article 6 instaure un régime de compétence conditionnelle basé sur deux critères pour que le TPEF soit valablement saisi. Le premier critère est lié à l'exigence d'une enquête administrative préalable. Ce critère nécessite que les infractions prévues à l'article 6 al. 1er pour lesquelles le TPEF est saisi fassent l'objet d'une enquête administrative préalable par une administration spécialisée. Pour ce qui concerne la cybercriminalité, il peut s'agir soit du Conseil national de la cyberdéfense, soit de l'Agence nationale de cybersécurité [à créer]. Le deuxième critère est lié à la gravité de l'infraction et à la présence d'un élément d'extranéité. En effet, ce critère exige que le montant du préjudice causé par l'infraction soit supérieure ou égal à 100 000 dollars américains et/ou lorsque l'infraction poursuivit comporte un élément d'extranéité (quel que soit le montant du préjudice). Il s'agit d'un verrou procédural pour éviter la surcharge des affaires au sein du TPEF. Ce verrou permet à cette juridiction de se concentrer sur les affaires à fort enjeu stratégique.

Cela laisse supposer que toutes les infractions commises dans l'environnement numérique dont les violences numériques ne relèvent pas exclusivement de la compétence matérielle du TPEF notamment lorsque le montant du préjudice pour l'État n'atteint pas 100 000 USD et/ou si elles ne comportent pas d'élément d'extranéité. Dans cette hypothèse, ces infractions demeurent tout naturellement de la compétence des juridictions de droit commun.

Pour traiter efficacement les matières techniques relevant de son champ de compétence, le TPEF est organisé en sections spécialisées. Selon l'article 11 de l'ordonnance-loi n°26/007 du 14 mars 2026 précitée, c'est la 5e section de la Chambre de première instance qui est chargée de la répression de toutes les infractions du domaine des télécommunications et du numérique.

[63] Cf. les articles 174-d et 174-m du code pé al réprimant respectivement le harcèlement sexuel et la pédopornographie.
[64] Cette ordonn nce-loi introdui l'article 174-u dans le co e pénal réprimant les violences basées sur le genre à travers les éseaux de communication ou d'information

En guise d'épilogue

« Le temps du monde fini commence », disait Paul Valèry en 1931. Dans un monde fini, tout se répète, tout se conserve. Les violences numériques persistent et sont de plus en plus banalisées dans notre société. Elles appellent à une responsabilisation des plateformes et du droit en vue de rendre plus effective leur répression. Même si le cadre législatif a évolué pour combler le vide législatif autrefois décrié, l'effectivité des sanctions est trop faible en raison de l'immatérialité et du caractère transfrontière du cyberespace défiant les frontières étatiques. Ce dernier constitue désormais un lieu de refuge pour les cyberdélinquants et nourrit le sentiment d'impunité à cause de l'anonymat et de la volatilité des preuves qui le caractérisent.

Malgré l'augmentation des plaintes devant les juridictions congolaises ces dernières années, la pratique judiciaire prouve que rares sont les cas qui ont connu des peines très exemplaires et dissuasives. La difficulté de la preuve électronique et le manque de spécialisation de certains acteurs judiciaires conduisent fréquemment à des classements sans suite au parquet ou à des peines symboliques devant le juge sans considération des dispositions pénales appropriées liées aux violences subies. Ce décalage entre la gravité du préjudice subi par les victimes et la banalisation de la sanction pénale ne permet pas d'imposer l'autorité de l'État dans le cyberespace congolais et encourage sérieusement les cyberdélinquants à commettre leurs méfaits.

Face à la complexité de ces violences, il est nécessaire de renforcer les mesures de prévention et de répression adaptées aux enjeux de l'ère. Ces mesures peuvent inclure l'harmonisation du cadre de répression, l'investissement dans l'éducation numérique (Littératie numérique), la formation des acteurs judiciaires devant combattre à armes égales avec les cybercriminels, la responsabilisation des plateformes numériques dans la modération de contenus en langues nationales, le lancement des campagnes massives de sensibilisation dans les médias, les milieux éducatifs et de travail, la mise en place d'un cadre de soutien aux victimes […]. La prise en compte de ces mesures permettra la convergence entre rigueur juridique, effectivité de la sanction et éducation citoyenne. Grâce à cette convergence, le droit pourra alors espérer transformer le cyberespace congolais en un lieu de liberté où la sécurité est assurée, et dans lequel l'écran ne peut plus servir de bouclier à la violence...

BIBLIOGRAPHIE INDICATIVE

I. TEXTE CONSTITUTIONNEL

Constitution de la République Démocratique du Congo, modifiée par la loi no 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 JO RDC, 52e année, n° spécial, du 05 février 2011.

II. LÉGISLATION CONGOLAISE

Loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétence des juridictions de l'ordre judiciaire.

Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication in JO RDC, 62e année, n° spécial, du 22 septembre 2021.

Loi n°06/018 du 20 juillet 2006 sur les violences sexuelles.

Loi n°16/008 du 15 juillet 2016 complétant et modifiant la loi n°87-010 du 1er août 1987 portant code de la famille, in JO RDC, n° spécial.

Décret du 30 janvier 1940 tel que modifié, complété et mis à jour au 05 octobre 2006, portant Code pénal, in JO RDC, 47e année, n° spécial, du 05 octobre 2006.

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

Ordonnance-loi n°23/023 du 11 septembre 2023 modifiant et complétant le décret du 30 janvier 1940 portant code pénal congolais.

Ordonnance n° 23/170 du 15 août 2023 portant création, organisation et fonctionnement d'un service spécialisé au sein du Cabinet du Président de la République dénommé Conseil National de Cyberdéfense, en sigle « CNC ».

Ordonnance-loi n°26/007 du 14 mars 2026 portant création, organisation, fonctionnement et compétences du tribunal pénal économique et financier (TPEF).

III. OUVRAGES

CORNU G., *Vocabulaire juridique*, 12e éd, PUF Quadrige, Paris, 2018.

FAVREAU A., *L'essentiel du droit du numérique,* Gualino Lextenso, Clamecy, 2024.

FERAL-SCHUHL CH., *Cyberdroit : Le droit à l'épreuve de l'internet*, 4e éd., Dalloz, Paris, 2006.

GRYNBAUM L., LEGOFFIC C. et MORLET-HÏDARA L., *Précis de Droit des activités numériques*, 1ère éd., Dalloz, Paris, 2014.

GUY DE FELCOURT, *L'usurpation d'identité ou l'art de la fraude sur les données personnelles*, CNRS Edition, Paris, 2011.

LEONETTI X., *Guide de cybersécurité : droits, méthodes et bonne pratiques*, L'Harmattan, Paris, 2015.

NDUKUMA ADJAYI K. (sous la dir.), DIANGENDA MVETE A. et LOLEKA RAMAZANI B., *Droit du commerce électronique : enjeux civils, consuméristes, cybercriminels, d'extranéité et de déterritorialité*, L'Harmattan, coll. « Enjeux et droits numériques », Paris, 2021.

QUEMENER M., *Cybersociété, entre espoirs et risques,* L'Harmattan, Coll. Justice &Démocratie, Paris, 2013.

IV. ARTICLES GÉNÉRAUX ET EN LIGNE

ACP, « 16 jours d'activisme, les congolais appelés à soutenir les victimes des violences numériques », 25 novembre 2025, Disponible sur : [https://www.acp.cd/genre/ les-congolais-appeles-à-soutenir-les-victimes-des-violences-numériques] (consulté le 01mai 2026).

BLAYA C., « Etude du lien entre cyberviolence et climat scolaire : enquête auprès des collégiens d'Île de France », *in* Les dossiers des sciences de l'éducation [En ligne], n°33, 1er mars 2015, p. 3. Disponible sur : [http://journals.openedition.org/dse/815] (consulté le 16 mars 2026).

CAPRIOLI A., « Traçabilité et droit de la preuve électronique », Droit & Patrimoine, n° 93, mai 2001, p. 68-75, mise à jour le 20 Octobre 2013 *in* [https://www.caprioli-avocats.com], (consulté le 20/03/2026).

CEMEA, « Région Normandie Observatoire des pratiques numériques des adolescents, […] », 2018. Disponible sur : [http://educationauxecrans.fr/index.php/le-dispositif/observatoire-des-pratiques-des-jeunes] (consulté le 10 avril 2026).

CHARTON L. et BAYARD C., « Les violences contre les femmes et les technologies numériques : entre oppression et agentivité », *in* Revue Recherches féministes, Vol. 34, n°1, 2021, pp. 312-330.

CNIL, « L'anonymisation des données personnelles, Mise au point sur les techniques utilisables et sur leurs enjeux », 19 mai 2020, Disponible sur [https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles] (consulté le 29 mars 2025).

FADOUA HACHIMI A., « Cyberintimidation et humiliation à l'ère de l'intelligence artificielle : reconfigurations de la violence numérique », Aleph, Vol. 12, n°5, 15 février 2026, Disponible sur : [https://aleph.edinum.org/15874#]

JEHEL S., « Les adolescents face aux violences numériques entre adhésion et résistances aux logiques de violence », Terminal [En ligne], n° 123, le 31 décembre 2018, p.1. Disponible sur : [http://journals.openedition.org/terminal/3226] (consulté le 16 mars 2026).

LOLEKA RAMAZANI B., « Le droit congolais face aux enjeux de protection de l'identité numérique : quel regard prospectif ? », Dossier n°5, *in* Droit-numérique.cd, 05 janvier 2025, p. 9. Disponible sur : [https://droitnumerique.cd/le-droit-congolais-face-aux-enjeux-de-protection-de-lidentité-numérique-quel- regard-prospectif/] (consulté le 04 février 2025).

UNWOMEN, « La violence numérique est une violence réelle : le combat d'une activiste pour la sécurité et les droits humains », 18 novembre 2025, disponible sur : [https://www.unwomen.org/fr/nouvelles/reportage/2025/11/la-violence-numerique-est-une-violence-reelle-le-combat-dune-activiste-pour-la-securite-et-les-droits-humains] (consulté le 5 avril 2026).

V. THÈSES ET MÉMOIRES

LOLEKA RAMAZANI B., *L'enquête pénale en droit congolais du numérique : nécessité d'intégration des nouveaux outils d'investigation*, Mémoire présenté et défendu en vue de l'obtention du Diplôme d'Études Approfondies en Droit, Sous la dir. Prof. K. Ndukuma Adjayi, UCC, 2025.

STELLA É., *L'adaptation du droit pénal aux réseaux sociaux en ligne*, Thèse en vue de l'obtention du grade de Docteur en droit privé et sciences criminelles présentée et soutenue publiquement le 12 décembre 2019, sous la dir. Frédéric STASIAK, Université de Lorraine, Lorraine, 2019.

VI. AUTRES DOCUMENTS

CONSEIL DE L'EUROPE, « Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018: Cybercrime Convention Committee (T-CY) – Working Group on cyberbullying and other forms of online violence, especially against women and children », 9 juillet 2018.

ASSEMBLÉE PARLEMENTAIRE DE LA FRANCOPHONIE, *Rapport final : la cyberviolence envers les femmes et les enfants dans l'espace francophone*, 19 janvier 2021.

RAPPORT DE LA FONDATION POUR L'ENFANCE, « L'IA générative, nouvelle arme de la pédocriminalité », octobre 2024.

RAPPORT DU SG DE L'ONU, « Intensification de l'action menée pour éliminer toutes les formes de violence à l'égard des femmes et des filles : violence contre les femmes et les filles facilitée par les technologies », n°A/79/500, 8 octobre 2024.

TABLE DES MATIÈRES

Droit Numérique.cd

Droit-Numerique.cd est un cadre d'études dédié à l'analyse, la réflexion et la diffusion des connaissances juridiques relatives aux enjeux du numérique en République démocratique du Congo. Nous sommes enregistrés sous le numéro SIREN 931152144.

Pourquoi nous contacter ?

Partenariats

Collaborons pour renforcer l'écosystème numérique en RDC.

Consultations juridiques

Obtenez des conseils sur les questions légales liées au numérique.

Participation

Nous pouvons contribuer dans vos études, séminaires, et autres activités.

Suggestions

Partagez vos idées ou proposez des sujets que vous aimeriez voir abordés

contact@droitnumerique.cd

+ 33 6 05 50 17 84

www.droitnumerique.cd