■ ARTICLE DE RECHERCHE / RESEARCH ARTICLE

Cybercriminalité en République Démocratique du Congo : enjeux juridiques, lacunes normatives et perspectives de réforme

ROLLY NKULU MUKANYA
Chef de Travaux, Faculté de Droit, Université de Lubumbashi

KABEYA TSHIKUKA ILUNGA Aline
Assistante, Faculté de Droit, Université de Lubumbashi

Received: 8 April 2026
Accepted: 3 June 2026
Available online: 5 July 2026

How to cite:
NKULU MUKANYA, R. & KABEYA TSHIKUKA ILUNGA, A. (2026). Cybercriminalité en République Démocratique du Congo : enjeux juridiques, lacunes normatives et perspectives de réforme. International Journal of Social Sciences and Scientific Studies, 6(3), pp. 5680-5693.

Résumé

La cybercriminalité constitue aujourd'hui l'une des menaces les plus sérieuses pour les sociétés modernes, bouleversant les cadres juridiques traditionnels. En République Démocratique du Congo (RDC), l'expansion rapide des technologies de l'information et de la communication (TIC), bien qu'elle offre des opportunités de développement, expose également le pays à de nouvelles formes de criminalité numérique. Cet article analyse les enjeux juridiques de la cybercriminalité en RDC, en mettant en lumière les lacunes normatives et institutionnelles actuelles, et en formulant des perspectives de réforme. La problématique centrale s'articule autour de l'inadéquation du cadre juridique congolais face à la cybercriminalité. Le Code pénal congolais, hérité de l'ère coloniale, ne couvre pas adéquatement les infractions liées aux technologies numériques. L'absence d'une loi spécifique sur la cybercriminalité, combinée à la faiblesse des infrastructures technologiques de la justice, constitue un obstacle majeur. Pour répondre à ces défis, l'article propose une approche multidimensionnelle incluant l'adoption d'une législation spécifique, la formation des acteurs judiciaires, le renforcement de la coopération internationale et le développement de l'infrastructure numérique judiciaire. La méthodologie adoptée repose sur une approche qualitative, combinant l'analyse documentaire, l'examen de la jurisprudence comparée, et la méthode comparative avec d'autres pays africains ayant légiféré en la matière. L'étude contribue à combler un vide dans la littérature juridique congolaise sur la question et propose une base de réflexion pour les réformateurs institutionnels.

Cybercrime is one of the most serious threats to modern societies, disrupting traditional legal frameworks. In the Democratic Republic of Congo (DRC), the rapid expansion of information and communication technologies (ICTs), while offering development opportunities, also exposes the country to new forms of digital crime. This article analyses the legal challenges of cybercrime in the DRC, highlighting current normative and institutional gaps, and proposing reform perspectives. The central issue revolves around the inadequacy of the Congolese legal framework in addressing cybercrime. The Congolese Penal Code, inherited from the colonial era, does not adequately cover technology-related offences. The absence of specific cybercrime legislation, combined with weak technological infrastructure within the justice system, constitutes a major obstacle. To address these challenges, the article proposes a multidimensional approach including the adoption of specific legislation, training of judicial actors, strengthening international cooperation, and developing digital judicial infrastructure. The methodology adopted is based on a qualitative approach combining documentary analysis, comparative case law review, and the comparative method with other African countries that have legislated in this area. The study helps fill a gap in Congolese legal literature on the topic and provides a basis for reflection for institutional reformers.

Mots-clés : Cybercriminalité, droit pénal, RDC, technologies numériques, réforme législative, Convention de Budapest, sécurité informatique

© 2026 IJSSASS. All rights reserved.

© 2026 IJSSASS. All rights reserved.

INTRODUCTION

La révolution numérique a transformé en profondeur les sociétés contemporaines. Si les technologies de l'information et de la communication (TIC) ont ouvert de nouvelles perspectives de développement économique et social, elles ont également généré des formes inédites de criminalité. La cybercriminalité, définie comme l'ensemble des infractions commises via les réseaux informatiques ou visant les systèmes d'information, constitue désormais un enjeu majeur de sécurité publique, tant au niveau national qu'international (Wall, 2007). La cybercriminalité est un phénomène mondial en pleine expansion. Selon le rapport du CSIS (Center for Strategic and International Studies), les cyberattaques coûtent à l'économie mondiale plus de 600 milliards de dollars par an.

En République Démocratique du Congo (RDC), la pénétration croissante d'Internet et de la téléphonie mobile a favorisé l'émergence de pratiques illicites telles que le phishing, le piratage informatique, la fraude bancaire électronique, le chantage en ligne et la diffusion de contenus illicites. Or, le cadre juridique congolais, largement hérité de l'ère coloniale, n'a pas été adapté à ces nouvelles réalités (Ngoie Mwenze, 2020).

Le présent article se propose d'examiner les enjeux juridiques de la cybercriminalité en RDC, d'identifier les insuffisances du cadre normatif et institutionnel actuel, et de formuler des propositions de réforme en vue d'un renforcement de la lutte contre ce phénomène. Les questions centrales qui guident cette recherche sont les suivantes : Dans quelle mesure le cadre juridique congolais est-il adapté à la répression de la cybercriminalité ? Quelles sont les lacunes normatives et institutionnelles identifiables ? Quelles réformes pourrait-on envisager pour améliorer la réponse pénale face à la cybercriminalité ?

Pour mener à bien cette analyse, une méthodologie qualitative a été retenue, combinant la recherche documentaire (textes légaux, rapports institutionnels, doctrine juridique), l'analyse juridique critique et la méthode comparative. Cette dernière permet de confronter l'expérience congolaise à celles d'autres pays africains (Sénégal, Côte d'Ivoire, Rwanda) ayant déjà légiféré en matière de cybercriminalité.

I. CADRE CONCEPTUEL ET THÉORIQUE

1.1. Définitions et typologies de la cybercriminalité

Le terme « cybercriminalité » est souvent employé de manière générique pour désigner un ensemble hétérogène d'infractions liées aux nouvelles technologies. Selon la Convention de Budapest de 2001, on distingue quatre grandes catégories d'infractions : les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques (accès illégal, interception illicite, atteinte à l'intégrité des données, etc.) ; les infractions informatiques (falsification et fraude informatiques) ; les infractions liées au contenu (pornographie infantile, incitation à la haine, etc.) ; les infractions liées aux atteintes à la propriété intellectuelle.

D'autres auteurs, comme Sieber (1998), proposent une classification selon le rôle de la technologie dans la commission de l'infraction : la technologie comme cible (piratage, sabotage), la technologie comme outil (escroquerie en ligne, phishing) et la technologie comme environnement de l'infraction (cybermanipulation, cyberstalking).

En RDC, les formes les plus répandues de cybercriminalité incluent : les escroqueries en ligne (arnaques sur les réseaux sociaux, faux recrutements, faux investissements) ; les fraudes bancaires électroniques (mobile money fraud, phishing bancaire) ; le chantage et l'extorsion en ligne (sextorsion, diffusion de données personnelles) ; les atteintes à la vie privée numérique (piratage de comptes, diffusion d'images intimes) ; la diffusion de fausses informations (fake news) à caractère subversif ou déstabilisant (Ngoie Mwenze, 2020).

1.2. Cadre théorique : la théorie de la régulation numérique

L'analyse des défis posés par la cybercriminalité s'inscrit dans la théorie de la régulation numérique développée par Lessig (1999). Selon cet auteur, le cyberespace est régulé par quatre forces : la loi, les normes sociales, le marché et l'architecture technique. L'efficacité de la lutte contre la cybercriminalité dépend de la synergie entre ces différentes modalités de régulation.

Dans le contexte congolais, c'est principalement la dimension légale qui présente des défaillances majeures. L'absence de législation spécifique, couplée à la faiblesse des capacités institutionnelles et techniques, crée un environnement favorable à l'expansion de la

© 2026 IJSSASS. All rights reserved.

cybercriminalité (Mutonkole Mwamba, 2021).

Cette carence juridique est renforcée par l'absence de structures spécialisées au sein de la police et de la justice pour traiter les infractions numériques. Les magistrats et officiers de police judiciaire ne bénéficient généralement pas de formations adaptées aux spécificités de la preuve numérique.

II. ÉTAT DES LIEUX DU CADRE JURIDIQUE CONGOLAIS

2.1. Le Code pénal congolais face à la cybercriminalité

Le Code pénal congolais, dont les dispositions fondamentales remontent au décret du 30 janvier 1940, n'a pas été conçu pour appréhender les réalités numériques contemporaines. Les principales infractions susceptibles d'être invoquées dans le cadre de la cybercriminalité sont : l'escroquerie (art. 98 du Code pénal), le faux en écriture (art. 124 et s.), l'abus de confiance (art. 95), et l'atteinte à la vie privée. Ces dispositions, bien que partiellement applicables, sont inadaptées aux spécificités du crime numérique.

Le principal problème réside dans le principe de légalité des incriminations (nullum crimen, nulla poena sine lege), qui exige une qualification précise des faits. Or, des actes comme le phishing, le piratage de systèmes informatiques ou l'usurpation d'identité numérique ne trouvent pas de correspondance directe dans les textes en vigueur. Des infractions comme le piratage de systèmes informatiques ou la diffusion de logiciels malveillants ne trouvent aucune base légale dans le Code pénal actuel (Mutonkole Mwamba, 2021).

Par ailleurs, la notion de preuve numérique n'est pas encadrée par la législation procédurale congolaise. Le Code de procédure pénale ne prévoit ni la saisie de données informatiques, ni la réquisition auprès des fournisseurs d'accès Internet, ni les procédures de perquisition numérique.

2.2. Les lois sectorielles existantes

Quelques textes sectoriels abordent indirectement la question de la cybercriminalité : la Loi n° 013/2002 du 16 octobre 2002 sur les télécommunications fixe les conditions d'exploitation des réseaux et prévoit certaines sanctions liées à la fraude dans les télécommunications ; la Loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, plus récente, contient quelques dispositions relatives à la sécurité des systèmes d'information, mais reste insuffisante en matière de qualification pénale des cybercrimes.

Ces textes, bien qu'utiles, ne constituent pas un cadre cohérent de lutte contre la cybercriminalité. Ils ne définissent ni les infractions spécifiques, ni les procédures de répression, ni les mécanismes de coopération internationale indispensables dans ce domaine.

2.3. Le projet de loi sur la cybercriminalité

Un projet de loi sur la cybercriminalité a été élaboré et déposé devant le Parlement. Ce texte s'inspire largement de la Convention de Budapest et de la Convention de Malabo de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (2014). À ce jour, ce projet n'a pas encore été adopté, laissant un vide juridique important. Le retard dans l'adoption de ce projet illustre les limites de la volonté politique face à la complexité technique et juridique du sujet (Kalongo Mbikayi, 2022).

III. ANALYSE COMPARÉE : EXPÉRIENCES AFRICAINES

3.1. Le Sénégal

Le Sénégal a adopté la Loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité, faisant de ce pays l'un des pionniers en Afrique subsaharienne. Cette loi incrimine spécifiquement l'accès frauduleux à un système informatique, l'atteinte à l'intégrité des données, la fraude informatique et la production de dispositifs illicites. Le Sénégal a également créé une brigade spéciale de lutte contre la cybercriminalité et a adhéré à la Convention de Budapest (Ndiaye, 2019).

3.2. La Côte d'Ivoire

La Côte d'Ivoire a adopté la Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité. Ce texte incrimine un large éventail d'infractions numériques et prévoit des peines sévères. La Plateforme de Lutte contre la Cybercriminalité (PLCC), créée en 2011 en partenariat avec la Direction de l'Informatique et des Traces Technologiques (DITT), constitue un modèle de référence en Afrique de l'Ouest (Coulibaly, 2018).

3.3. Le Rwanda

© 2026 IJSSASS. All rights reserved.

Le Rwanda dispose de la Loi n° 60/2018 du 22 août 2018 relative à la prévention et à la répression de la cybercriminalité. Ce texte est considéré comme l'un des plus complets d'Afrique. Il couvre non seulement les infractions classiques mais aussi les aspects de preuve électronique et de coopération internationale. Le Rwanda a également investi massivement dans l'infrastructure numérique et dans la formation des magistrats à la gestion des dossiers impliquant des preuves numériques (Harelimana, 2021).

3.4. Leçons pour la RDC

L'analyse comparée met en évidence plusieurs facteurs clés de succès : l'adoption d'une législation spécifique couvrant l'ensemble des infractions numériques ; la création de structures spécialisées (brigades, plateformes) ; l'investissement dans la formation des acteurs judiciaires ; la coopération régionale et internationale ; le développement de l'infrastructure technologique.

Tableau 1. Synthèse comparative des cadres juridiques de cybercriminalité en Afrique

Critère	Sénégal	Côte d'Ivoire	Rwanda	RDC
Loi spécifique	Oui (2008)	Oui (2013)	Oui (2018)	Non (projet en cours)
Structure spécialisée	Oui (Brigade)	Oui (PLCC/DITT)	Oui	Non
Adhésion Budapest	Oui	Non	Oui	Non
Conv. Malabo	Signée	Ratifiée	Signée	Non signée
Formation juges	Oui	Oui	Oui	Très limitée
Preuve numérique	Encadrée	Encadrée	Encadrée	Non encadrée

Sources : Législations nationales; rapports de l'UIT et de l'UA.

IV. LACUNES NORMATIVES ET INSTITUTIONNELLES EN RDC

4.1. Lacunes normatives

Absence de définition légale des infractions numériques : Le droit pénal congolais ne définit pas les notions de système informatique, de donnée numérique, d'accès frauduleux ou de fraude informatique. Cette lacune rend impossible toute poursuite efficace.

Inadéquation procédurale : Le Code de procédure pénale ne prévoit pas de dispositions spécifiques relatives à la collecte, la conservation et la présentation de la preuve électronique. Les enquêteurs sont démunis face à des éléments de preuve volatils et techniquement complexes.

Absence de cadre juridique pour la coopération internationale en matière de cybercriminalité : La cybercriminalité est par nature transnationale. L'absence d'adhésion de la RDC à la Convention de Budapest ou à la Convention de Malabo limite considérablement les possibilités de coopération en matière d'entraide judiciaire et d'extradition.

4.2. Lacunes institutionnelles

Absence de structure spécialisée de lutte contre la cybercriminalité : Contrairement au Sénégal ou à la Côte d'Ivoire, la RDC ne dispose ni de brigade spécialisée, ni de plateforme de signalement des infractions numériques.

Insuffisance de la formation des acteurs judiciaires : Les magistrats et officiers de police judiciaire congolais ne bénéficient pas de formations continues en matière de cybercriminalité, de preuve numérique ou de forensique informatique.

Faiblesse de l'infrastructure technologique judiciaire : Le système judiciaire congolais souffre d'un déficit chronique en équipements informatiques, en logiciels d'analyse forensique et en capacités de stockage sécurisé des preuves numériques.

V. PERSPECTIVES DE RÉFORME

5.1. Adoption d'une loi spécifique sur la cybercriminalité

La priorité absolue est l'adoption d'une loi spécifique sur la cybercriminalité qui devrait : définir les infractions numériques de manière précise et exhaustive ; prévoir des peines proportionnées à la gravité des infractions ; encadrer les procédures de collecte de preuves numériques ; établir un cadre de coopération internationale ; prévoir la responsabilité des fournisseurs de services en matière de conservation des données.

5.2. Création d'une structure spécialisée

La mise en place d'une unité spécialisée de lutte contre la cybercriminalité, sur le modèle de la PLCC ivoirienne ou de la brigade sénégalaise, serait un pas décisif. Cette structure devrait disposer de compétences techniques en forensique numérique et bénéficier d'un mandat clair.

© 2026 IJSSASS. All rights reserved.

5.3. Formation des acteurs judiciaires

Un programme de formation continue destiné aux magistrats, avocats et officiers de police judiciaire devrait être mis en place, en partenariat avec des organismes internationaux (ONUDC, UIT, Interpol). La formation devrait couvrir : la qualification juridique des cyberinfractions, la gestion de la preuve numérique, les techniques d'investigation numérique, la coopération judiciaire internationale.

5.4. Adhésion aux instruments internationaux

La RDC devrait envisager l'adhésion à la Convention de Budapest sur la cybercriminalité et la ratification de la Convention de Malabo. Ces instruments offrent un cadre normatif harmonisé et facilitent la coopération internationale en matière d'enquêtes et de poursuites transfrontières.

5.5. Développement de l'infrastructure numérique judiciaire

L'investissement dans l'équipement technologique du système judiciaire est indispensable : laboratoires de forensique numérique, logiciels d'analyse de données, systèmes sécurisés de stockage de preuves électroniques, et bases de données centralisées des incidents cyber.

CONCLUSION

La cybercriminalité constitue un défi majeur pour la République Démocratique du Congo, dont le cadre juridique et institutionnel demeure largement insuffisant pour faire face à cette menace croissante. L'analyse du droit positif congolais révèle des lacunes fondamentales tant sur le plan normatif que procédural et institutionnel.

L'étude comparée des expériences sénégalaise, ivoirienne et rwandaise démontre qu'une réponse efficace à la cybercriminalité repose sur une approche intégrée combinant législation spécifique, structures spécialisées, formation des acteurs et coopération internationale.

Face à l'ampleur du phénomène et à son impact croissant sur l'économie et la sécurité des citoyens congolais, l'adoption urgente d'une législation spécifique et le renforcement des capacités institutionnelles constituent des impératifs incontournables. La présente étude a voulu contribuer, modestement, à la réflexion sur les voies et moyens d'une réponse pénale adaptée aux réalités numériques du XXI■ siècle en RDC.

BIBLIOGRAPHIE

Castells, M. (2001). La galaxie Internet. Paris : Fayard.

Coulibaly, I. (2018). La lutte contre la cybercriminalité en Côte d'Ivoire : bilan et perspectives de la PLCC. Revue Ivoirienne de Droit et de Criminologie, 12(2), 45–67.

Conseil de l'Europe. (2001). Convention sur la cybercriminalité (Convention de Budapest). STCE n° 185, Budapest.

CSIS – Center for Strategic and International Studies. (2020). The Hidden Costs of Cybercrime. Washington, DC : McAfee.

Harelimana, J. (2021). Cybercrime legislation in Rwanda : Challenges and achievements. East African Law Journal, 8(1), 89–110.

Kalongo Mbikayi, D. (2022). Le défi de la cybersécurité en République Démocratique du Congo. Revue de Droit Congolais, 15(3), 78–95.

Lessig, L. (1999). Code and Other Laws of Cyberspace. New York : Basic Books.

Mutonkole Mwamba, C. (2021). Les insuffisances du droit pénal congolais face à la cybercriminalité. Annales de la Faculté de Droit, Université de Lubumbashi, 24, 112–130.

Ndiaye, M. (2019). La répression de la cybercriminalité au Sénégal : une analyse critique de la loi de 2008. Revue Sénégalaise de Droit Pénal, 5(1), 33–50.

Ngoie Mwenze, R. (2020). Cybercriminalité et sécurité numérique en RDC : état des lieux et défis. Cahiers Congolais de Droit et de Société, 18, 67–85.

République Démocratique du Congo. (1940). Décret du 30 janvier 1940 portant Code pénal congolais.

République Démocratique du Congo. (2002). Loi n° 013/2002 du 16 octobre 2002 sur les télécommunications.

République Démocratique du Congo. (2020). Loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux TIC.

République de Côte d'Ivoire. (2013). Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.

République du Rwanda. (2018). Loi n° 60/2018 du 22 août 2018 relative à la prévention et à la répression de la cybercriminalité.

République du Sénégal. (2008). Loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité.

Sieber, U. (1998). Legal Aspects of Computer-Related Crime in the Information Society. Université de Würzburg.

Union africaine. (2014). Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo).

Union internationale des télécommunications (UIT). (2020). Global Cybersecurity Index 2020. Genève : UIT.

Wall, D. S. (2007). Cybercrime : The Transformation of Crime in the Information Age. Cambridge : Polity Press.

© 2026 IJSSASS. All rights reserved.