

CHAIRE DE DYNAMIQUE SOCIALE (C.D.S)

MOUVEMENTS & ENJEUX SOCIAUX

Revue Internationale
des Dynamiques Sociales

WWW.MESRIDS.ORG
MAI - JUIN 2026
KINSHASA-R.D.C

M.E.S., n°153
Mai - Juin 2026



SOMMAIRE

- François Momindo Wetshingolo, *Déficit des politiques publiques et embouteillages dans la ville de Kinshasa*1
- Guy Ekofa Nsimba, *L'impuissance de la justice constitutionnelle congolaise face au néopatrimonialisme : reconstruction du patriotisme constitutionnel pour faire passer un passé qui ne veut pas passer*9
- Michel Diumu Omasombo, Daniel Mulenda Lomena, Nadège Ingrid Gouanlong Kamgang, *Déterminants d'un modèle intégré de la logistique multimodale de transport autour du port en eaux profondes de Banana : analyse des chaînons manquants pour l'ambiversion économique de la RD Congo*..17
- Ruphin Mutwangwefa Soki, Joseph Ibula Matadiwamba, *La prohibition du mariage des mineurs en droit congolais face aux résistances coutumières : analyse juridique et socio-anthropologique*.....32
- Bonfils Omba Onyakonde, Salomon Osako Okonda, *Gouvernance participative et stratégies de communication dans les projets REDD+ : analyse critique du modèle d'intervention de la BCI en RDC*...39
- Sammy D'Elsan Bialu Kalambayi, *Du trafic aérien au rôle de la douane congolaise dans le contrat d'affrètement d'aéronefs pour une meilleure intégration nationale en RD Congo*.....44
- Kazadi Kyamalala-Tata, *Violence sexuelle dans les couples face à la judiciarisation : enjeux, limites et perspectives en droit positif congolais*.....52
- David Otshudiema Yonga, Dominique Tumaini Tcheru, Crispin Ebango Molanga, *Les méthodes d'investigation de la police judiciaire en droit comparé : entre modernisation technologique et protection des droits fondamentaux. Analyse comparée des systèmes français, belge et congolais*.....58
- Christian Basa Ntolo, *La justice constitutionnelle comme garantie du constitutionnalisme en Afrique francophone noire : cas de la République Démocratique du Congo*.....66
- Serge Pelo Mbozo, *L'ordre mondial à l'épreuve de la multipolarité : la redéfinition du régionalisme africain*.....73
- Timothée Ngongo Tambwe, *Stratégie nationale de cybersécurité en RD Congo : vers un cyberspace de confiance, sécurisé et résilient*.....80
- Prosper Kabulo Kasongo, *La province de Lomami à l'épreuve du développement local : défis et enjeux*...88
- Antoine Lokuli Iloko Y'ompso, *La complexité de la coutume dans le système juridique congolais*.....97
- Joseph Bruno Ndjaya, M.F.J. Nepanepa Kibundila, Amani Isiaka Mwanamasoma, *Impact des pratiques de gestion des ressources humaines sur la performance organisationnelle des entreprises congolaises (Onatra et OCC)*.....105
- Eugénie Mapatano Lena Yusse, *Analyse de l'architecture institutionnelle dans la négociation minière en République démocratique du Congo*.....112
- Issiaka Abdallah Bukinga Matala, *Production des imprimés de valeur sécurisés et performance productive de l'économie congolaise*.....121
- Jordely Mambu Ngalula, Irady Nkwimi Dilangay, *Le contrôle juridictionnel des actes de gouvernement par la Cour constitutionnelle en droit congolais : fondements et perspectives*.....131
- Jospin Lisele, Marie-Thérèse Ngalula, Jean Kabangu Bafuila, *La protection des frontières de la RDC grâce aux drones : une étude à l'aune de la théorie réaliste face aux groupes armés transfrontaliers*.....138
- Maurice Eke Ahoka, *Impact socio-économique de l'épargne des ménages de la cité de Lodja*144
- Adonis Landu Makindu, *L'utilité juridique et pratique de la lettre de voiture dans l'acte uniforme relatif aux contrats de transport des marchandises par route*.....150

– Sammy D’Elsan Bialu Kalambayi, <i>Le positionnement ambigu de la RDC dans le libre-échange régional : diagnostic sur les barrières non tarifaires congolaises et formule pour leur démantèlement</i>	157
– Bienvenu N’kasime Mandro, Anderson Nzalongo Kwilu, <i>État et fabrication du risque politique dans les contextes institutionnels fragiles : cas de la République Démocratique du Congo</i>	165
– Patrick Kadima Nteksha, Andy Muleka Mulumba, <i>De la prépondérance masculine à l’égalité conjugale en droit positif congolais : la réforme du Code de la famille de 2016</i>	175
– Paul Samangua Okitalange, <i>La France et la reconfiguration sécuritaire de l’Est de la RD Congo : concurrences géopolitiques et limites du multilatéralisme</i>	181
– Emmanuel Shako Emambulu, <i>La désinvolture face au risque cyber dans le contexte congolais : un frein à la mise en mouvement de l’action judiciaire en matière de cybercriminalité</i>	187
– Bernadette Muisaka Kamono, Joséphat Tshianda Kapinga, Jeanne Nyakato Beangere, <i>Influence des comportements parentaux sur le bien-être des adolescents scolarisés dans la ville de Kinshasa</i>	193
– Packson Minzinga Pakinzi, <i>La sacralité de la vie humaine face aux contraintes organisationnelles : analyse éthique de la mortalité maternelle à Kinshasa</i>	199
– Isaac Pelendo Zugbangba, Guelord Kakenza Kitumba, Delly Lufungula Mubiala, <i>Perception des enseignants de la politique de gratuité de l’éducation de base et son influence sur leur motivation professionnelle dans la province éducationnelle Kinshasa-Lukunga (RDC)</i>	207
– Nathan Mubunda Lukata, <i>La présomption irréfutable d’irresponsabilité pénale des enfants de moins de 14 ans en RDC : entre protection légale et réalité judiciaire</i>	211
– Jonathan Nomba Mbaya, <i>De la recevabilité d’une requête de sursis à exécution en instance de tierce opposition devant le juge administratif congolais : difficultés pratiques et palliatifs</i>	217
– Jonathan Lukengu Mukadi, <i>La police des cimetières en droit congolais : étude critique du cadre normatif et perspectives de réforme</i>	225
– Hervé Omombo Wembo, Djéssy Mbuyi-Tshishimbi, <i>Sécurité alimentaire mondiale et prédation foncière : la RD Congo, nouvel eldorado des grandes puissances</i>	235
– Antoine Muyaya Tshifuaka, <i>L’encadrement juridique de la procédure disciplinaire dans l’administration publique en RD Congo : une analyse jurisprudentielle</i>	243
– Eugène Ziakwau Buna, <i>L’ORBi comme instrument de visibilité, d’accessibilité et de diffusion des connaissances produites à l’Université de Kinshasa : analyse bibliologique et enjeux stratégiques</i>	251
– Nothel Lonkange Bolisomi, <i>La fonction préventive de l’inspection du travail en droit congolais : analyse critique de son pouvoir de conciliation à la lumière du Code du travail et des normes internationales</i>	259
– Irady Nkwimi Dilangay, Jordely Mambu Ngalula, <i>La protection du droit de manifester en public par le juge constitutionnel congolais</i>	268
– Dieudonné Nkishi Kazadi, <i>Les “fallacies” de Paulin Punga Kumakinga : déconstruction critique d’une entreprise de sacralisation du statu quo constitutionnel en République Démocratique du Congo</i>	275
– Gerry Mwantote Mpia Nsuba, Giscard Mpangi Moseseli, <i>Conditions ergonomiques et bien-être au travail des agents de l’administration centrale de l’Office congolais de contrôle</i>	287
– Joseph Momba Songo, <i>La charge de la preuve du motif valable de licenciement en droit congolais : de l’asymétrie probatoire à la nécessité d’un rééquilibrage normatif</i>	294
– Jean Makayi Lokale, <i>Le caractère secret de l’instruction préjuridictionnelle : entre exigence de confidentialité et contraintes politico-judiciaires devant la Cour de cassation en RD Congo</i>	300
– Georges Mbayo Mbayo, <i>La création du consulat général du Kenya à Goma : controverse de lege ferenda en relations consulaires</i>	308
– Lyse Yanga Mawete, Joël Ipara Motema, Brigitte Iyeli, <i>Représentations sociales et religieuses du handicap à Kinshasa : lecture anthropologique interprétative et enjeux de développement inclusif</i>	316
– Raymond Badiala Minga, <i>De l’exercice de la souveraineté populaire dans la Constitution du 18 février 2006 en RD Congo : de l’idéal normatif à la pratique politique contemporaine</i>	325
– Jean Baptiste Lokando Ekoto, <i>Axes stratégiques, réalisations et impact de la réforme sur la mise en œuvre du budget-programme en RD Congo</i>	331

- Francis Ekondji Liloka, *De l'efficacité des voies de recours dans la procédure de passation des marchés publics : étude comparée entre la République démocratique du Congo et la France*.....339
- Kawaya Sefu Papa, *Migration et développement : papier thématique*346
- Joséphat Tshianda Kapinga, Bernadette Muisaka Kamono, Jeanne Nyakato Beangere, *Impact des discours de haine et de violence sur la psychologie des enfants de Kinshasa en situation d'échec scolaire*353
- Coco Dunguzabolo Kanza, *L'effectivité du dispositif anti-blanchiment en RD Congo : entre conformité normative et impunité structurelle*.....359
- David Ngay Nguz, Miriam Mbensa Diawakwikila, *Les infractions du numérique et leur répression en RD Congo : analyse critique de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique*.....367
- Achille Umba Di Mamona, *Revue de littérature sur les approches psychologiques de la conformité fiscale dans des pays en voie de développement*.....373
- Josephine Kasongo Vumilia, *Performance du District Health Information Software 2 dans la surveillance des maladies évitables par la vaccination : influence des attitudes des utilisateurs dans la province du Tanganyika (RDC)*.....382
- Léon Mingidim À Manyimabel, *Pour l'administration de la justice contre les auteurs des changements anticonstitutionnels de gouvernement*.....390
- Freddy Muganza Beya, *Stabilité financière, qualité institutionnelle et performances macroéconomiques en RD Congo : analyse du rôle modérateur des institutions*.....397
- Lucie Mwadi Lufika, *Le développement du tourisme balnéaire à Kinshasa : opportunités, contraintes et perspectives stratégiques*.....410
- Raymond Badiala Minga, *Les procédés de la démocratie participative et délibérative comme leviers de revitalisation de la souveraineté populaire en République démocratique du Congo*.....416

LA DÉSINVOLTURE FACE AU RISQUE CYBER DANS LE CONTEXTE CONGOLAIS :

*un frein à la mise en mouvement de l'action judiciaire
en matière de cybercriminalité*

par

Emmanuel SHAKO EMAMBULU

*Apprenant en D.E.S., Département de Droit pénal et criminologie,
Faculté de Droit, Université de Kinshasa*

Résumé

Malgré l'expansion rapide de l'Internet et des réseaux sociaux, la société congolaise reste marquée par une faible culture de cybersécurité et une perception minimisée des menaces numériques. La cybercriminalité est souvent considérée comme un phénomène mineur, ce qui entraîne une faible dénonciation des faits par les victimes. Cette situation est aggravée par la méfiance envers la justice, l'absence de mécanismes accessibles de signalement et la faible spécialisation des acteurs judiciaires. Le ministère public adopte rarement une attitude proactive, bien qu'il ait le pouvoir de se saisir d'office. Cette banalisation du risque cyber entretient le « chiffre noir » de la cybercriminalité, d'où la nécessité de renforcer la sensibilisation, les mécanismes de signalement et les capacités des acteurs judiciaires.

Mots clés : cybercriminalité, cybersécurité, dénonciation, perception, risque cyber, signalement

Abstract

Despite the rapid expansion of the Internet and social media, Congolese society remains characterized by a weak cybersecurity culture and a minimized perception of digital threats. Cybercrime is often regarded as a minor phenomenon, which results in a low rate of reporting by victims. This situation is aggravated by mistrust toward the justice system, the absence of accessible reporting mechanisms, and the limited specialization of judicial actors. As a result, the public prosecutor rarely adopts a proactive approach despite having the authority to initiate proceedings ex officio. This trivialization of cyber risk contributes to maintaining the « dark figure » of cybercrime, hence the need to strengthen public awareness, reporting mechanisms, and the capacities of judicial actors.

Keywords : cybercrime, cybersecurity, reporting, perception, cyber risk, notification

INTRODUCTION

La transformation digitale progressive en RDC ne s'est pas accompagnée d'une culture suffisamment développée de la cybersécurité ni d'une perception adéquate des risques liés au cyberspace. Ces derniers désignent la probabilité qu'un événement y survienne et porte atteinte au système d'information et/ou aux données numériques¹ et peuvent être le résultat d'un acte malveillant ou accidentel.²

Dans le contexte congolais, les comportements à risque tels que le partage imprudent de données personnelles, la faible sécurisation des systèmes informatiques ou encore la tolérance sociale face aux escroqueries numériques tendent à être normalisés. Cette banalisation du risque cyber se manifeste tant au niveau des utilisateurs que des institutions publiques et privées.

Or, cette perception minimisée du danger cybernétique constitue un obstacle à la mobilisation des mécanismes de répression. Elle se traduit notamment par le déficit de dénonciation formelle des infractions, la faible collaboration des victimes avec les autorités judiciaires, ainsi qu'une mise en mouvement quasi-inexistante de l'action publique en matière de cybercriminalité.

Ainsi, le problème réside dans le décalage entre l'ampleur croissante des menaces cybernétiques et la réaction encore insuffisante du système judiciaire, largement influencée par la banalisation sociale et institutionnelle du risque cyber.

Par ce qui précède donc, il est ici question de voir dans quelle mesure la banalisation du risque cyber dans le contexte congolais constitue un obstacle à la mise en mouvement effective de l'action judiciaire, spécialement l'action publique, en matière de cybercriminalité.

Pour y répondre, l'on adopte un cadre théorique mixte combinant l'effectivité du droit et l'approche systémique. Elle analyse l'écart entre la validité formelle des normes et leur application concrète dans la perspective de Hans Kelsen.³ Elle conçoit également la répression de la cybercriminalité comme le produit

¹ C. DELCAMP, *Les risques numériques et la cyber assurance*, Support de formation « La gestion des risques cyber de la prévention à la couverture assurantielle », Cité par A. JELSCH-BISEL, *Evaluation du risque cyber des établissements de santé*, Mémoire de Master, Institut de science financière et d'assurances, Lyon, 2023, p. 11.

² *Idem*.

³ Lire H. KELSEN, *Théorie pure du droit*, Traduction française, Dalloz, 1962. Lire aussi M. DORAY, « Le (néo)normativisme, constructivisme inachevé », *In Les Annales de droit*, 8/2014, Mis en ligne le 14 mars 2018, Consulté le 07 mars 2025 à 22h07' sur URL : <http://journals.openedition.org/add/727>

d'interactions institutionnelles, selon une vision relationnelle inspirée de Michel Foucault cité par Dan Kaminski.⁴ Et sur le plan méthodologique, la réflexion repose sur une double démarche. Elle combine une analyse juridique téléologique des textes et une approche socio-criminologique qualitative fondée sur l'observation, des entretiens et une analyse thématique du travail de l'Officier du Ministère Public face à la cybercriminalité.

Cela étant, il nous reviendra d'abord d'apporter des clarifications essentielles sur la notion de cyberrisque et sa perception dans le contexte congolais (I). Il s'agira, par la suite, d'analyser les effets de la banalisation sur la mise en mouvement de l'action judiciaire (II).

I. LA NOTION DU RISQUE CYBER ET SA PERCEPTION DANS LE CONTEXTE CONGOLAIS

La cybercriminalité est souvent sous-estimée par une partie de la population congolaise en raison de la banalisation des risques numériques. Les menaces du cyberspace sont perçues comme lointaines ou invisibles, alors qu'elles peuvent provoquer des pertes financières, des atteintes à la réputation, des sabotages informatiques ou des violations de données personnelles.⁵ Dans cet état de choses, il nous revient ici d'analyser précisément ces risques (1), en montrant comment leur méconnaissance et leur minimisation par les citoyens contribuent à entretenir une perception faussement rassurante du phénomène (2) et tout cela en vue de démontrer que cette négligence collective ne résulte pas d'une absence de danger, mais d'un déficit d'attention, de culture numérique et de compréhension des impacts juridiques et sociaux que ces infractions peuvent engendrer.

1.1. Le risque cyber : qu'entendre ?

Dans un monde de plus en plus connecté et numérisé, la maîtrise des risques cyber est devenue un enjeu incontournable pour les organisations, qu'elles soient publiques ou privées.⁶

En effet, le risque cyber correspond à tous les risques découlant de l'utilisation des données électroniques et de leur transmission, y compris les outils technologiques tels qu'Internet et les réseaux de télécommunications.⁷ Il regroupe une grande variété d'incidents et de conséquences possibles.⁸

La Stratégie nationale de cybersécurité de la RDC renseigne une augmentation notable des cyberattaques ces dernières années, marquée par une fréquence et une complexité croissantes. Ces attaques visent de plus en plus les Etats et les entreprises.⁹ Par ailleurs, l'usage accru des technologies numériques par les organisations publiques et privées, bien qu'il favorise leur développement et leur efficacité, les rend également plus dépendantes et donc plus vulnérables aux cybermenaces.¹⁰

La République démocratique du Congo, comme plusieurs pays africains, est régulièrement victime de cyberattaques visant notamment les systèmes informatiques de l'administration, comme le piratage du site du Ministère de l'Enseignement supérieur et universitaire en 2024.¹¹ Cette situation révèle un manque de sensibilisation et de compréhension des risques cyber, qui conduit de nombreuses victimes à ne pas reconnaître ou signaler les infractions.¹² Selon le rapport Security Navigator d'Orange Cyberdefense, ces attaques pourraient entraîner des pertes importantes pour l'Afrique et leur fréquence, notamment les cas d'extorsion, est en forte hausse.¹³ Toutefois, l'ampleur réelle du phénomène pourrait être sous-estimée en raison de la digitalisation croissante et des difficultés à identifier les auteurs des attaques.¹⁴

⁴ D. KAMINSKI, *Condamner. Une analyse des pratiques pénales*, Toulouse, éd. Erès, 2015, p. 54.

⁵ A. BONNAC, *Tarifification du cyber-risque pour les collectivités locales : une modélisation inspirée par le modèle pandémique*, Mémoire de Master, Institut de science financière et d'assurances, Lyon, 2020, p. 14.

⁶ Guide des risques cyber 3.0, IFASI, France, 2025, P.8

⁷ CRO Forum, *Cyber resilience The cyber risk challenge and the role of insurance*, Décembre 2014, définition traduite, Cité par A. JELSCH-BISEL, *Op. cit.*, p. 11.

⁸ *Idem.*

⁹ Commission Technique pour la Cybersécurité (CTC), *Stratégie nationale de cybersécurité de la République Démocratique du Congo 2022-2025*, Présidenc.cd, Kinshasa, Juillet 2022, p. 14.

¹⁰ *Idem*, p.15.

¹¹ N. DJUMA SOSTHENE, « Augmentation des cyberattaques en RDC : Quelle réglementation pour lutter contre ce fléau ? », in *Droit-Numérique.cd - Dossier N° 2 – Août 2024*, p.1

¹² ONUDC, *Cours en ligne sur la cybercriminalité*, Module : Enquêter sur la cybercriminalité. Disponible sur <https://elearningunodc.org/course/view.php?id=749>

¹³ Rapport disponible sur <https://www.orangecyberdefense.com/fr/insights/livres-blancs-et-reportings/security-navigator-2025>

¹⁴ « En Afrique, la menace cyber enfle au rythme de la digitalisation. », In *Les Echos*, Disponible sur <https://www.lesechos.fr/thema/articles/en-afrique-la-menace-cyber-enfle-au-rythme-de-la-digitalisation-2085287>

Une cyberattaque est une atteinte malveillante visant des systèmes informatiques tels que les ordinateurs, serveurs, réseaux ou appareils connectés. Elle peut cibler divers équipements numériques, qu'ils soient reliés ou non à Internet.¹⁵ Toutefois, les atteintes à la sécurité informatique peuvent aussi résulter d'erreurs humaines ou de négligences.¹⁶

La culture nous renseigne que le risque cyber a évolué avec le développement des réseaux depuis les années 1980, passant de simples virus informatiques à des attaques sophistiquées, comme les ransomwares.¹⁷ Des incidents majeurs, tels que les attaques contre Yahoo en 2013, eBay en 2014 ou le rançongiciel WannaCry ransomware en 2017, ont montré l'ampleur mondiale des dommages pouvant toucher entreprises et institutions.¹⁸

1.2. La perception du risque cyber dans le contexte congolais

L'avènement des technologies de l'information et de la communication a profondément transformé les modes de vie, les relations sociales ainsi que les activités économiques à l'échelle mondiale. La République démocratique du Congo n'échappe pas à cette dynamique. Depuis une décennie, on observe une expansion rapide de l'accès à Internet, favorisée par la démocratisation des smartphones, la multiplication des opérateurs de télécommunications et l'essor des plateformes numériques. Cette mutation technologique, porteuse d'opportunités indéniables pour le développement, s'accompagne néanmoins d'un accroissement significatif des risques liés à l'usage du cyberspace.

En effet, l'environnement numérique, par son caractère immatériel, transnational et évolutif, favorise l'apparition de nouvelles formes de criminalité. La cybercriminalité, entendue comme un ensemble des infractions pénales spécifiques liées aux TIC telles que définies par le code du numérique ainsi que celles prévues dans d'autres lois particulières dont la commission est facilitée ou liée à l'utilisation des technologies,¹⁹ constitue une menace croissante pour les individus, les entreprises et les institutions. En RDC, elle se manifeste notamment par le piratage de comptes, les arnaques sentimentales et l'exploitation frauduleuse des données numériques.

Dans l'imaginaire collectif, les faits de cybercriminalité sont souvent perçus comme des incidents mineurs ou de conflits privés sans portée juridique. Cette situation traduit une banalisation du risque cyber, caractérisée par une sous-estimation des dangers liés aux technologies numériques. Ainsi, dans la société congolaise, plusieurs comportements à risque comme le partage imprudent d'informations personnelles, l'utilisation de mots de passe faibles ou la négligence des mesures de sécurité sont devenus des pratiques courantes.

Cette banalisation se traduit par la tendance de nombreux citoyens à minimiser les incidents numériques, souvent perçus comme de banals problèmes de réseaux sociaux. Beaucoup hésitent à porter plainte et privilégient des solutions informelles, sans reconnaître la dimension pénale des faits. Cette attitude, liée au manque d'information, à une faible culture numérique et à la rareté des poursuites visibles, contribue à sous-estimer dangereusement la cybercriminalité.

II. LES EFFETS DE LA BANALISATION SUR LA MISE EN MOUVEMENT DE L'ACTION JUDICIAIRE

La banalisation du risque cyber entraîne une faible mobilisation du système judiciaire face à la cybercriminalité. De nombreuses victimes ne portent pas plainte, estimant les poursuites inutiles ou les auteurs difficiles à identifier (i). Par ailleurs, le ministère public, pourtant garant des poursuites pénales, utilise rarement son pouvoir de saisine d'office. Et même lorsque des plaintes existent, les infractions numériques sont parfois perçues comme moins graves que les infractions classiques. Ces éléments viennent donc limiter leur priorisation dans le traitement judiciaire (ii).

¹⁵ Club de la sécurité de l'information français, *Assurance des risques cyber. Guide pratique*, Disponible sur <https://clusif.fr/publications/assurance-risques-cyber-guide-pratique>, Cité par Manu Claeys, *Gestion des risques cyber au sein des entreprises*, Mémoire de Master 60 en Sciences de gestion, Université de Namur, 2018-2019, p.8.

¹⁶ MANU CLAEYS, *Gestion des risques cyber au sein des entreprises*, Mémoire de Master 60 en Sciences de gestion, Université de Namur, 2018-2019, P18.

¹⁷ A. BONNAC, *Op. cit.*, p. 14.

¹⁸ *Idem.*

¹⁹ Voir Article 2. 24 de l'Ordonnance-Loi n°23/010 du 13 Mars 2023 portant code du numérique.

2.1. Déficit de dénonciations formelles en matière de cybercriminalité

La lutte contre la cybercriminalité en République démocratique du Congo est affaiblie par la faible dénonciation²⁰ des faits par les victimes. Très peu d'infractions numériques sont signalées aux autorités, ce qui prive le ministère public d'informations nécessaires pour engager des enquêtes. Cette sous-déclaration s'explique notamment par l'absence d'une plateforme nationale de signalement en ligne, ce qui décourage les victimes et entretient une sous-estimation du phénomène. Ainsi, comme le souligne l'Office des Nations Unies contre la drogue et le crime, la mise en place de mécanismes de signalement accessibles constitue un moyen important pour encourager les plaintes et améliorer la lutte contre la cybercriminalité.²¹

Plusieurs pays ont mis en place des plateformes en ligne de signalement de la cybercriminalité permettant aux victimes de déclarer facilement les infractions numériques. C'est le cas notamment de la Nouvelle-Zélande avec *Netsafe*, le Royaume-Uni avec « *Action Fraud* », les Etats-Unis avec l'IC3 (**Internet Crime Complaint Center/FBI**), la France avec **cybermalveillance.gouv.fr** et la plateforme *17Cyber*, l'Australie avec *ReportCyber* (portail « *Report and Recover* ») proposée par l'ACSC (**Australian Cyber Security Centre**) et le Canada avec « *Report Cyber and Fraud* », où des portails dédiés reçoivent les plaintes, orientent les victimes et transmettent les dossiers aux autorités compétentes.²²

Ces systèmes offrent plusieurs avantages, notamment l'accessibilité permanente 24h/24, la collecte standardisée des informations, l'orientation rapide vers les services compétents et la production de données utiles pour les enquêtes et les politiques publiques. Ainsi, les expériences étrangères montrent que ces plateformes constituent un outil efficace de lutte et de prévention contre la cybercriminalité.²³ Et d'ailleurs, Europol²⁴ propose sur son site web une page détaillée qui répertorie les différents mécanismes de signalement de la cybercriminalité disponibles dans les Etats européens.²⁵

Au-delà de cet aspect, la faible dénonciation de la cybercriminalité en RDC s'explique en grande partie par la méfiance des citoyens envers l'appareil judiciaire et par la peur de représailles. Beaucoup de victimes ignorent les procédures de plainte, manquent d'informations sur leurs droits et doutent de la capacité des autorités à traiter des infractions techniques. Cette situation est aggravée par la lenteur des procédures, la crainte de divulguer des informations sensibles, le sentiment de honte ou les risques d'atteinte à la réputation.²⁶

Selon l'Office des Nations Unies contre la drogue et le crime, ces facteurs contribuent à la sous-déclaration des infractions, ce qui renforce le « chiffre noir »²⁷ de la cybercriminalité et limite la capacité du ministère public à engager des poursuites²⁸, surtout qu'il se véhicule dans la pratique judiciaire que rarement, le Ministère public se saisit d'office, d'une infraction.²⁹ Ainsi, la sensibilisation³⁰ des citoyens et le renforcement de la confiance envers les institutions apparaissent fondamentales pour encourager les plaintes.³¹

²⁰ La dénonciation est prise ici au sens général du terme, signifiant tout simplement un mécanisme pour les particuliers de porter à la connaissance d'une autorité judiciaire les susceptibles d'être qualifiés d'infractions. Qu'ils soient victimes ou non, l'élément important est le fait de porter une telle information à la connaissance de l'autorité judiciaire, peu importe la forme.

²¹ ONUDC, *Op. Cit.*, Module : Enquêter sur la cybercriminalité.

²² *Idem.*

²³ *Ibid.*

²⁴ Europol est l'agence de l'Union européenne chargée de soutenir la coopération policière entre les Etats membres dans la lutte contre la criminalité grave et organisée. Elle intervient notamment contre le terrorisme ; la cybercriminalité ; le trafic de drogues et d'êtres humains, etc.

²⁵ ONUDC, *Op. Cit.*, Module : Enquêter sur la cybercriminalité.

²⁶ ONUDC, *Op. Cit.*, Module : Enquêter sur la cybercriminalité.

²⁷ Le chiffre noir de la criminalité est l'écart, plus ou moins important, qui existe entre la criminalité réelle et la criminalité connue au niveau apparent.

²⁸ ONUDC, *Op. Cit.*, Module : Enquêter sur la cybercriminalité.

²⁹ R.-N. PUNGWE NEMBA, *Guide pratique des magistrats du parquet. Les fonctions du Ministère Public en République Démocratique du Congo*, Tome I En matière répressive, 2^e éd., KONGO EDITIONS, Kinshasa, 2020, p. 54.

³⁰ C. MUPILI KABYUMA, *Droit pénal et droits de l'homme à l'épreuve de la cybercriminalité. Enjeux de la révolution numérique et nouvelles pistes de régulation de l'espace médiatique*, L'Harmattan Rd Congo, Paris, 2024, p.111.

³¹ *Idem.*, p.240.

2.2. Le déficit d'attitude pro-active de l'organe poursuivant en matière de cybercriminalité

En droit congolais, le magistrat du parquet peut se saisir d'office des infractions menaçant l'ordre public. Cependant, en pratique, cette faculté est rarement utilisée.³² Les infractions relatives à la cybercriminalité n'ont pas échappé à cette réalité.

En effet, les articles 66³³ et 67³⁴ de la loi-organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire confie au Ministère public, au nom de l'Etat, la responsabilité de rechercher et de poursuivre les infractions, **sans qu'une plainte préalable soit nécessaire**, notamment lorsque l'ordre public est en cause. C'est pourquoi en 2011, le Procureur Général de la République Flory Kabange Numbi dans sa circulaire n°2/008/IM/PGR/2011 du 07 mars 2011 relative à l'action des parquets, avait classé la saisine d'office comme un mode de recherche des infractions dans l'intérêt exclusif de l'ordre public.³⁵

Se fondant sur l'article 7 de l'ordonnance-loi n°82/020 du 31 mars 1982 portant code de l'organisation et de la compétence judiciaires (texte en vigueur de l'époque) qui stipulait qu'en matière répressive le Ministère Public recherche des infractions (contenu de l'actuel article 67 de la loi-organique de 2013), pour cette autorité judiciaire, ces termes généraux justifient pleinement l'exercice d'office de l'action publique.³⁶

Selon des analyses doctrinales du droit congolais, la saisine d'office du Ministère public est le fait pour l'OMP de se saisir directement des faits infractionnels sans qu'il soit nécessaire qu'une plainte ou une dénonciation soit portée à son attention.³⁷ Dans le cas où il en est saisi, il a l'obligance d'informer son chef d'office, car il est interdit au magistrat d'instruire une affaire sans son autorisation.³⁸

Par ailleurs, il est vrai que les infractions à la législation du numérique sont constatées par les officiers de police judiciaire à compétence restreinte ou générale selon le cas, et que lorsqu'ils sont saisis ou constatent les faits infractionnels aux dispositions du code du numérique, ils en informent l'officier du Ministère public compétent conformément aux dispositions du code de procédure pénale.³⁹ Cependant, bien qu'ils ne soient pas expressément cités dans la constatation des infractions à la législation du numérique, les officiers du Ministère public peuvent exercer eux-mêmes toutes les attributions des officiers de police judiciaire.⁴⁰

Par ce qui précède, il convient de relever ici que derrière le déficit d'attitude proactive de l'organe poursuivant en cette matière se cache notamment l'absence de spécialisation des magistrats du parquet, conduisant ainsi à une sorte de priorisation des infractions classiques.

En effet, le vécu judiciaire renseigne que les magistrats du parquet accordent une priorité aux infractions classiques portant atteinte aux personnes, à l'ordre public ou aux biens matériels, jugées plus urgentes. Par conséquent, les infractions relatives à la cybercriminalité sont souvent reléguées au second plan. Cette situation s'explique notamment par une perception institutionnelle ambivalente de la cybercriminalité, considérée comme moins urgente en raison de son caractère immatériel et de l'absence apparente de trouble immédiat à l'ordre public.⁴¹ Pourtant, une telle perception tend à minimiser sa gravité, alors même que la cybercriminalité peut affecter profondément l'économie numérique, la confiance dans les institutions et la sécurité nationale.⁴²

CONCLUSION

Au terme de cette réflexion, il apparaît que la désinvolture face au risque cyber en République démocratique du Congo alimente la faible mobilisation de l'action judiciaire en matière de cybercriminalité. Malgré l'augmentation des usages numériques et des menaces dans le cyberspace, ces infractions sont

³² R.-N. PUNGWE NEMBA, *Op. cit.*, p. 54.

³³ « Le Ministère public surveille l'exécution des actes législatifs, des actes réglementaires et des décisions de justice. Il poursuit d'office cette exécution dans les dispositions qui intéressent l'ordre public. »

³⁴ « En matière répressive, le Ministère public recherche les infractions aux actes législatifs et réglementaires qui sont commises sur le territoire de la République. Il reçoit les plaintes et dénonciations, accomplit tous les actes d'instruction et saisit les Cours et tribunaux. »

³⁵ Circulaire du Procureur Général de la République n°2/008/IM/PGR/2011 du 07 mars 2011 relative à l'action des parquets, Section 3. Recherche des infractions dans l'intérêt exclusif de l'ordre public, *In Circulaires et Instructions générales*, 2011, p. 23.

³⁶ *Idem.*

³⁷ R.-N. PUNGWE NEMBA, *Op. cit.*, p. 54.

³⁸ *Idem.*

³⁹ Article 318 de l'ordonnance-loi n°23/010 du 13 Mars 2023 portant code du numérique.

⁴⁰ Article 11 alinéa 1 du décret du 06 août 1959 portant code de procédure pénale tel que modifié et complété à ce jour.

⁴¹ ONUDC, *Op. cit.*, Module 1. Introduction à la cybercriminalité.

⁴² *Idem.*

souvent perçues comme mineures ou sans réelle gravité. Cette perception contribue à la réticence des victimes à signaler les faits aux autorités compétentes.

Cette banalisation influence également le fonctionnement de l'appareil judiciaire. Le ministère public agit le plus souvent de manière réactive et dépend largement des plaintes déposées par les victimes. La complexité technique des infractions numériques, le manque de spécialisation et la tendance à accorder la priorité aux infractions classiques contribuent ainsi à limiter l'effectivité des poursuites en matière de cybercriminalité.

Face à cette situation, au-delà du cadre juridique approprié, la lutte contre la cybercriminalité nécessite une prise de conscience accrue du risque numérique, d'où la nécessité de renforcer la sensibilisation des citoyens, d'améliorer les mécanismes de signalement des infractions et de développer les compétences techniques des acteurs judiciaires afin de garantir une réponse pénale plus efficace et adaptée aux défis du numérique.

BIBLIOGRAPHIE INDICATIVE

Instruments juridiques

- Décret du 6 août 1959 portant code de procédure pénale, tel qu'il a été modifié, complété et actualisé au 11 septembre 2023 BO 1959, in J.O. RDC.
- Loi organique n° 13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire, in JO RDC, 54^e année, numéro spécial du 4 mai 2013.
- Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, in J. O. RDC, numéro spécial du 11 avril 2023.
- Circulaire du Procureur général de la République n° 2/008/IM/PGR/2011 du 7 mars 2011 relative à l'action des parquets, in *Circulaires et instructions générales*, 2011.

Doctrines et autres

- BONNAC (A.), *Tarification du cyberrisque pour les collectivités locales : une modélisation inspirée par le modèle pandémique*, Mémoire de master, Institut de science financière et d'assurances, Lyon, 2020.
- CRO Forum, « Cyber resilience The cyber risk challenge and the role of insurance, décembre 2014.
- DJUMA SOSTHENE (N.), « Augmentation des cyberattaques en RDC : quelle réglementation pour lutter contre ce fléau ? », in *Droit-Numérique.cd* – Dossier n° 2 – Août 2024.
- JELSCH-BISEL (A.), *Évaluation du risque cyber des établissements de santé*, mémoire de master, Institut de science financière et d'assurances, Lyon, 2023.
- KAMINSKI (D.), *Condamner. Une analyse des pratiques pénales*, Toulouse, éd. Erès, 2015.
- MANU CLAEYS, *Gestion des risques cyber au sein des entreprises*, Mémoire de master 60 en Sciences de gestion, Université de Namur, 2018-2019.
- MUPILI KABYUMA (C.), *Droit pénal et droits de l'homme à l'épreuve de la cybercriminalité. Enjeux de la révolution numérique et nouvelles pistes de régulation de l'espace médiatique*, L'Harmattan Rd Congo, Paris, 2024.
- Office des Nations Unies contre la Drogue et le Crime, *Cours en ligne sur la cybercriminalité*, Disponible sur <https://elearning.unodc.org/course/view.php?id=749>
- PUNGWE NEMBA (R.-N.), *Guide pratique des magistrats du parquet. Les fonctions du ministère public en République démocratique du Congo*, tome I, en matière répressive, 2^e éd., KONGO ÉDITIONS, Kinshasa, 2020.

Centre de recherche d'interface université-société

COMITÉ DE RÉDACTION ET ADMINISTRATION

- Directeur-Editeur : Sylvain Shomba Kinyamba, Professeur Ordinaire
- Rédacteur en Chef : Gaston Mwene Batende, Professeur Emérite
- Rédacteur en Chef adjoint : Patrick Develtere, Professeur Ordinaire
- Secrétaire de rédaction : Michel Kandolo Edungu, Chef de Travaux
- Relation avec les partenaires : Jean Pierre Mpiana, Professeur Ordinaire
- Archivage et logistique : Ingrid Mulamba Feza, Professeure Associée

CONSEIL SCIENTIFIQUE

Professeurs Baeke Viviane, Batamba Balembu Antoine ; Bongeli Yeikeo Ya Ato Emile ; Develtere Patrick ; Ekala Pierre ; Gretry Lucille ; Huib Huyse ; Inswan Bidum Pierre ; Kaminar Théo-Macaire ; Kapalayi Mutanga Roger-Vincent ; Labana Lasay'abar Jean Berck Mans ; Malemba N'sakila Gilbert ; Matabisi Nico ; Mbalanda Willy ; Mbela Hiza Login ; Mbuyi Musongela François ; Mokonda Bonza Floratin ; Mukoka Nsenda François ; Mulamba Feza Ingrid ; Muluma Munanga Albert ; Musa Alokpo Dieudonné ; Musao Kalombo Célestin ; Mutunda Mwembo Pierre ; Mpiana Tshitenge Jean Pierre ; Mwabila Malela Clément ; Mwene Batende Gaston ; Ndeke Zamba Casimir ; Ngoma Binda Elie ; Ngoy Bisongo Colby ; Nkuanzaka Inzanza Adélard ; Ongevela Van Jan, Osokonda Okenge Basile, Ponsar Paul, Reyhler Luc ; Sekimonyo Wa Magango Côme ; Shomba Kinyamba Sylvain ; Wingenga Jeannot ; Yandju Marie-Claire ; Yere Afobe Innocent Zimango Gama Romain.

Immeuble CDS n°3, Trafic, Route de l'Ouest,
Campus de l'Unikin, Tél. : 0999903563 /
shombakin@yahoo.fr,
www.mesrids.org
Dépôt légal : MR 3.02103.57117
N° ISSN : 2790-3095 (impr.)
N° ISSN : 2790-3109 (ligne)

