
M.E.S., Numéro 144, Novembre – Décembre 2025

<https://www.mesrids.org>

Dépôt légal : MR 3.02103.57117

N°ISSN (en ligne) : 2790-3109

N°ISSN (impr.) : 2790-3095



Revue Internationale des Dynamiques Sociales
Mouvements et Enjeux Sociaux
Kinshasa, novembre - décembre 2025

CYBERCRIMINALITÉ ET RÉPONSE PÉNALE EN RD CONGO : étude comparative et proposition d'un modèle garantiste de cyberpolice

par

Étienne - Léon MOLADJA KABAMBA¹

David OTSHUDIEMA YONGA²

Chef de Travaux, Université de Lodja (UNILOD)

(Tous) Apprenants au Diplôme d'Etudes Spécialisées (DES/DEA),

Département de Droit Pénal et Criminologie,

Faculté de Droit, Université de Kinshasa

Résumé

La cybercriminalité en République démocratique du Congo s'impose comme un défi majeur à la fois juridique et sécuritaire. L'étude met en évidence les limites de la réponse institutionnelle actuelle et s'appuie sur une comparaison avec les modèles français, belge et africains pour formuler une proposition novatrice : la création d'une Direction nationale de la cyberpolice (DN-Cyber). Cette structure viserait à renforcer les capacités opérationnelles tout en garantissant le respect des droits fondamentaux. Le modèle proposé s'inscrit dans une perspective garantiste, conciliant sécurité numérique, souveraineté nationale et légalité procédurale. Il constitue une étape décisive vers la construction d'un cadre congolais de gouvernance numérique crédible et respectueux de l'État de droit.

Mots-clés : *cybercriminalité, RDC, cyberpolice, garantisme, sécurité numérique, droit comparé*

Abstract

Cybercrime in the Democratic Republic of the Congo has emerged as a major legal and security challenge. This study identifies the shortcomings of current institutional responses and, through a comparison with French, Belgian, and African models, proposes the creation of a National Cyber Police Directorate (DN-Cyber). The proposed framework strengthens operational capacity while safeguarding fundamental rights. Rooted in a garantist legal approach, it seeks to balance digital security, national sovereignty, and procedural legality, paving the way for a credible Congolese model of digital governance grounded in the rule of law.

Keywords : *cybercrime, DRC, Cyber Police, Garantism, Digital Security, Comparative Law*

INTRODUCTION

L'essor fulgurant des technologies numériques opère une mutation profonde des cadres politique, économique et social en République démocratique du Congo. Cette ubérisation ou transformation numérique de la société s'accompagne néanmoins d'une prolifération de cybermenaces : escroqueries financières digitalisées, désinformation à grande échelle, atteintes à l'intégrité des données personnelles et pratiques d'extorsion ciblant les franges les plus exposées de la population.

Face à ce défi sociétal inédit qui conjugue protection des libertés fondamentales et impératif de sécurité publique, l'État congolais se trouve dans l'obligation de concevoir et de déployer une police du numérique – ou cyberpolice, cyberpolicier, la cyberpolicrière³ – structurellement viable et juridiquement irréprochable.

La présente analyse propose un diagnostic opérationnel et juridique, établit une étude comparative des modèles étrangers (notamment français, belge et de cinq pays francophones africains), et élabore une architecture institutionnelle et procédurale sur-mesure pour la RDC. Ce modèle s'ancre dans l'arsenal législatif existant, incluant la loi organique n°11/013 du 11 août 2011, la loi n°20/017 et l'ordonnance-loi n°23/010, tout en intégrant les impératifs de la sécurité numérique contemporaine. Cette refondation institutionnelle se veut ainsi le point de départ d'une cyberstratégie nationale résiliente, à même de concilier innovation technologique et souveraineté numérique.

I. ÉTAT DES LIEUX EN RD CONGO

La RDC dispose aujourd'hui d'un corpus juridique récent relatif au numérique : la loi n°20/017 du 25 novembre 2020 (TIC)⁴, et surtout l'Ordonnance-loi n°23/010 du 13 mars 2023 (Code du numérique)⁵

¹ Chercheur en Droit pénal de l'état civil et de l'identité ; Directeur Central de l'Identification dactyloscopique des nationaux/Agence Nationale de Renseignements

² Chercheur en politique criminelle comparée ; Commissaire Supérieur (Lieutenant-Colonel) au sein de la Police Nationale Congolaise

³ La cyberpolice désigne l'institution ou l'unité spécialisée dans la lutte contre la cybercriminalité, tandis que le cyberpolicier (ou la cyberpolicrière) désigne l'agent individuel membre de cette unité

⁴ Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de la communication et de l'information, in Journal officiel de la RDC, Numéro spécial, Kinshasa, 22 sept.2021

qui complète et actualise le régime des télécommunications, la cybersécurité⁶ et la protection des données. Parallèlement, la Loi organique n°11/013 du 11 août 2011 définit l'organisation de la Police nationale congolaise (PNC) et mentionne une direction dédiée aux télécommunications et nouvelles technologies⁷, sans toutefois instituer une unité nationale spécialisée en cyberpolice. Ces textes posent des bases solides (définitions d'infractions, régime de levée du secret des correspondances, obligations des opérateurs), mais l'écart entre la norme et la pratique demeure considérable en matière de capacités techniques, de formation des officiers de police judiciaire (OPJ) et d'instruments de coopération interinstitutionnelle⁸.

II. LES ABUS NUMÉRIQUES EN RDC : TYPOLOGIE ET EXEMPLES CONCRETS

Les abus observés sont à la fois techniques et sociaux. Voici les principales catégories avec exemples concrets en RDC :

2.1. Fraudes mobiles et escroqueries financières

Des opérations de « SIM swap », d'usurpation d'identité et de faux transferts sur les plateformes de mobile money provoquent la perte de sommes conséquentes pour des ménages et des petites entreprises ; l'anonymat partiel des cartes SIM circulant sur le marché facilite ces délits (voir dispositions d'identification des abonnés)⁹.

2.2. Sextorsion¹⁰ et cyberharcèlement¹¹

La réponse étatique face à la sextorsion doit impérativement adopter une approche résolument centrée sur la victime. Ce paradigme d'action suppose la mise en place de circuits de signalement sécurisés et confidentiels, intégrés au sein d'une plateforme dédiée, couplée à une procédure accélérée de retrait des contenus illicites. Ce dispositif doit s'articuler avec une prise en charge psychosociale adaptée, une assistance juridique accessible et une coopération technique réactive avec les géants du numérique pour contenir la viralité des données compromettantes.¹²

La menace persistante de diffusion de contenus intimes génère un flux considérable de capitaux extorqués, ciblant principalement les femmes et les jeunes générations. L'absence persistante d'enquêtes spécialisées entraîne une impunité structurelle et la récurrence des infractions¹³. Les mécanismes répressifs doivent être conçus en synergie étroite avec ces mesures protectionnelles, afin de prévenir toute revictimisation et d'encourager le signalement des faits – condition sine qua non d'une lutte efficace contre cette forme insidieuse de criminalité numérique.

Le 22 août 2025, le Parquet près le Tribunal de Grande Instance de Kinshasa/Gombe a pris une réquisition exemplaire (n°267 RMP 50641/Pr 021/BAS) ordonnant à la Police nationale congolaise d'identifier et d'interpeller les auteurs de publications diffamatoires et d'images manipulées circulant sur les plateformes Facebook, WhatsApp, TikTok, X et YouTube. Ces actes visaient un officier du ministère public à la suite d'un réquisitoire officiel. Les faits sont juridiquement qualifiés d'outrages envers un

⁵ Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, in Journal officiel de la RDC, numéro spécial, Kinshasa, 11 avril 2023

⁶ La cybersécurité est la discipline globale de la protection du monde numérique. La cyberpolice est l'un des acteurs qui œuvrent dans ce domaine, mais dont le rôle est spécifiquement policier et judiciaire

⁷ Article 40.3, Loi organique n°11/013 du 11 août 2011 définit l'organisation et le fonctionnement de la Police nationale congolaise, in Journal Officiel de la RDC, n° spécial, 57^e Année, Kinshasa, 23 août 2011

⁸ Loi n°20/017 du 25 novembre 2020, Op.cit.; Ordonnance-loi n°23/010 du 13 mars 2023, Op.cit.; Loi organique n°11/013 du 11 août 2011, Op.cit.

⁹ Article 42.3, Ordonnance-Loi n°20/017, Op.cit., Disposition relative à l'obligation d'identification des abonnés

¹⁰ La sextorsion se définit comme une variante sophistiquée de l'extorsion numérique, consistant en la menace de divulguer des contenus à caractère sexuel dans le but d'obtenir un avantage financier, sexuel ou toute autre forme de rétribution. Ce phénomène criminel en plein expansion s'inscrit dans le champ de la cybercriminalité sexuelle, combinant subtilement chantage à caractère sexuel, atteinte à la vie privée et exploitation digitale. Les victimes, souvent piégées par la diffusion initiale volontaire ou non de contenus intimes, se retrouvent soumises à un chantage numérique les contraignant à céder aux exigences de l'agresseur sous la menace d'une divulgation publique

¹¹ Le cyberharcèlement constitue une autre facette préoccupante de la violence numérique. Il se manifeste par l'usage répété et malveillant des technologies de l'information et de la communication pour envoyer des messages, images ou propos diffamatoires, altérant gravement la dignité, la réputation ou l'intégrité psychologique des cibles. Cette forme de harcèlement, caractérisée par l'effet multiplicateur des plateformes digitales et la possibilité d'anonymat, fait désormais l'objet d'incriminations spécifiques dans les législations modernes relatives à la cybercriminalité.

¹² Justin W. Patchin & Sameer Hinduja, Op.cit., pp.30–54

¹³ Ordonnance-loi n°23/010, Op.cit., Livre IV relatif à la cybercriminalité et protection pénale des systèmes informatiques

officier du ministère public (article 136, alinéa 2, du Code pénal) et de harcèlement par communication électronique (article 358 du Code du numérique).

Ce dossier révèle, dans sa dimension pratique, les défis structurels et technologiques que rencontre la justice congolaise face aux nouvelles formes de cyberviolences. Il met en lumière la complexité de l'identification des auteurs dans un espace numérique sans frontières. Il souligne aussi la mise en œuvre encore hésitante des incriminations issues du Code du numérique ainsi que la persistance des mécanismes procéduraux classiques dans un contexte qui exige pourtant des outils d'investigation numérique plus adaptés.

Ainsi, cette affaire illustre avec acuité la nécessité urgente de créer une cyberpolice à dimension garantiste, disposant de compétences techniques autonomes et respectueuse des droits procéduraux fondamentaux. Elle incarne, en somme, la tension actuelle entre innovation juridique et archaïsme institutionnel dans la lutte contre la cybercriminalité en République Démocratique du Congo.

2.3. Désinformation et ingérences électorales

En période électorale, la circulation de « fake news¹⁴ » via les réseaux sociaux et groupes privés accentue la polarisation et pèse sur la tenue d'un débat public serein. L'encadrement légal existe, mais l'application est déficiente faute d'une cellule de surveillance et d'intervention opérationnelle¹⁵.

La lutte contre les ingérences électorales requiert la création d'une cellule spécialisée de veille et de vérification en temps réel, chargée d'assurer un monitoring continu de l'espace numérique. Placée au carrefour de la coopération institutionnelle, cette cellule devra travailler en étroite collaboration avec les plateformes numériques, les organes publics compétents et la société civile. Ses missions consisteront notamment à cartographier les acteurs impliqués, à identifier les vecteurs de diffusion de l'ingérence, et à proposer des réponses ciblées et proportionnées, qu'il s'agisse de l'apposition de labels d'authenticité, de la diffusion de contre-discours éclairants, ou de la mise en œuvre d'actions juridiques précises. Le tout devra s'opérer dans un strict respect de la liberté d'expression, sans recourir à des restrictions généralisées de contenus, afin de préserver l'intégrité du débat démocratique¹⁶.

2.4. Atteinte aux infrastructures et risques stratégiques

Attaques visant des services publics ou des prestataires critiques (santé, finance) ; sans capacité centralisée d'analyse d'incidents, la réponse demeure lente¹⁷. Ces constats montrent qu'au-delà du droit, la RDC a besoin d'une institution opérationnelle qu'est la cyberpolice, capable de transformer la réglementation en résultats concrets pour la population¹⁸.

III. COMPARAISON JURIDIQUE ET INSTITUTIONNELLE : FRANCE, BELGIQUE ET CINQ PAYS FRANCOPHONES AFRICAINS

- **France** : la France a renforcé, par la loi n°2023-22 du 24 janvier 2023 (LOPMI)¹⁹, les moyens du ministère de l'Intérieur et des services (y compris outils et effectifs) pour lutter contre la cybercriminalité ; sur le plan opérationnel, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et d'autres structures spécialisées coexistent avec des plateformes de signalement (PHAROS pour contenus illicites) et des unités dédiées aux fraudes et escroqueries (Thésée). L'expérience française illustre

¹⁴ L'expression « fake news », littéralement « fausses nouvelles » désigne des informations fabriquées de toutes pièces, détournées ou manipulées, présentées comme véridiques dans l'intention de tromper, d'influencer l'opinion publique, de manipuler des décisions politiques ou de porter atteinte à l'honneur d'une personne ou d'une institution. Diffusées principalement via les réseaux sociaux et les plateformes numériques, ces fausses nouvelles exploitent la rapidité de circulation de l'information pour créer la confusion, altérer la confiance dans les médias et parfois même compromettre l'ordre public. Dans plusieurs systèmes juridiques, leur diffusion intentionnelle est incriminée sous diverses qualifications, notamment la propagation de fausses nouvelles, la désinformation ou la manipulation de masse, toutes réprimées par les législations pénales relatives à la sécurité de l'État ou à la protection de l'ordre public.

¹⁵ Loi n°20/017, Op.cit., Dispositions sur la conservation et la coopération avec les opérateurs ; Ordonnance-loi n°23/010, Op.cit., Missions de l'Autorité de régulation du numérique

¹⁶ Frédéric Douzet (et contrib.), in Les guerres de l'information à l'ère numérique, PUF / Cairn, 2022 (chapitre sur la cartographie des acteurs et réponses institutionnelles)

¹⁷ Ordonnance-loi n°23/010, Op.cit., Livre IV sur la sécurité et protection pénale des systèmes informatiques

¹⁸ Synthèse fondée sur la loi n°20/017, Op.cit. et l'Ordonnance-loi n°23/010, Op.cit.

¹⁹ France, LOI n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI), in Journal, France, 24 janvier 2023

- l'importance d'une coordination nationale entre unités judiciaires, autorités administratives et opérateurs privés, tout en maintenant un strict contrôle judiciaire pour les mesures intrusives²⁰.
- **Belgique** : la Belgique s'est dotée d'un cadre pénal précoce (loi du 28 novembre 2000 relative à la criminalité informatique) et d'unités fédérales (Federal Computer Crime Unit) spécialisées. La leçon belge est double : (i) une législation claire facilite l'action pénale ; (ii) l'organisation fédérale nécessite des protocoles de coopération entre niveaux central et régional²¹.
 - **Sénégal** : le Sénégal a adopté la loi n°2008-11 du 25 janvier 2008 sur la cybercriminalité, complétée par un dispositif national de protection des données et une commission dédiée. Le Sénégal illustre l'articulation entre texte pénal, autorités de protection des données et outils administratifs de régulation²².
 - **Maroc** : le Maroc a intégré les infractions relatives aux systèmes de traitement automatisé des données via la loi n°07-03 (11 novembre 2003) qui a introduit des incriminations spécifiques au Code pénal. Le Maroc est un exemple d'incorporation disciplinaire des infractions informatiques au droit pénal général²³.
 - **Côte d'Ivoire** : la Côte d'Ivoire a promulgué la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, adoptant des incriminations larges et des sanctions sévères, tout en amorçant une stratégie nationale de cybersécurité. Ce modèle montre l'importance d'un texte spécifique moderne et d'une coordination entre justice et régulation²⁴.
 - **Tunisie** : la Tunisie a promulgué le Décret-loi n°2022-54 du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication ; ce texte est récent et très large, mais a fait l'objet de critiques concernant l'équilibre entre sécurité et libertés. Cela souligne la nécessité d'encadrer strictement les mesures intrusives (interceptions, filtrage) par des garanties procédurales robustes²⁵.
 - **Cameroun** : le Cameroun a adopté la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité. L'expérience camerounaise insiste sur l'importance des dispositifs nationaux de réponse aux incidents et sur la formation des forces de l'ordre²⁶.

Grosso modo, les pays ayant des résultats opérationnels probants cumulent : un texte spécifique et clair, des unités policières spécialisées et formées, des obligations de coopération imposées aux opérateurs, des garanties procédurales pour protéger les droits fondamentaux, des mécanismes de collaboration internationale. Ces éléments forment le tronc commun d'une bonne pratique transposable à la RDC²⁷.

IV. PROPOSITION D'UN MODÈLE CONGOLAIS DE POLICE DU NUMÉRIQUE : STRUCTURE, PRÉROGATIVES ET GARANTIES

En s'inspirant des bonnes pratiques identifiées, nous proposons un modèle institutionnel pragmatique et garantiste²⁸ pour la RDC.

²⁰ France, Loi n°2023-22 du 24 janvier 2023, Op.cit.

²¹ Belgique, Loi du 28 novembre 2000 relative à la criminalité informatique, Moniteur belge, Bruxelles, prom. 28 novembre 2000

²² Sénégal, Loi n°2008-11 du 25 janvier 2008 relative à la cybercriminalité, in Journal officiel du Sénégal, Dakar, 25 janvier 2008

²³ Maroc, Articles 607-3 à 607-11, Loi n°07-03 du 11 novembre 2003 complétant le Code pénal en matière d'infractions aux systèmes de traitement automatisé des données (Bulletin officiel marocain).

²⁴ Côte d'Ivoire, Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, in Journal officiel, Yamoussoukro, 19 juin 2013

²⁵ Tunisie, Décret-loi n°2022-54 du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication, in Journal officiel, Tunis, 16 septembre 2022

²⁶ Cameroun, Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité, in Journal officiel, Yaoundé, 21 décembre 2010

²⁷ France, LOPMI 2023 ; Belgique, Loi du 28 novembre 2000 ; Sénégal, Loi 2008 ; Maroc, Loi 07-03 2003 ; Côte d'Ivoire, Loi 2013-451 ; Tunisie, Décret-loi 2022-54 ; Cameroun, Loi 2010/012

²⁸ Le terme garantiste qualifie une conception du droit pénal et du procès pénal centrée sur la protection des droits fondamentaux de la personne, en particulier ceux du justiciable et du prévenu, face au pouvoir répressif de l'État. L'approche garantiste privilégie les principes de légalité, de présomption d'innocence, de droit à un procès équitable et de proportionnalité des peines, considérant que la mission première du droit pénal n'est pas seulement de punir, mais surtout de garantir les libertés individuelles contre l'arbitraire. Cette orientation doctrinale, héritée notamment

4.1. Structure organisationnelle proposée

- **Direction nationale de la cyberpolice** (DN-Cyber) au sein de la Police judiciaire (PNC), une cellule opérationnelle à compétence nationale, dotée d'antennes provinciales. (Se rattacher à l'art. 40.3 de la loi organique n°11/013 précitée ; missions à préciser par arrêté ministériel)²⁹.
- **Unité d'analyse et de réponse aux incidents** (CSIRT-PNC), en coopération technique avec l'Agence Nationale de Cybersécurité prévue par le Code du numérique³⁰.

Toute mesure intrusive, qu'il s'agisse d'une interception de communications, d'une perquisition technique ou d'un accès à des données sensibles, doit être soumise à un encadrement juridique strict. Celui-ci suppose notamment une réquisition judiciaire dûment motivée, une durée d'exécution limitée, le respect du principe de proportionnalité, ainsi qu'un contrôle a posteriori exercé par une autorité indépendante. Si le Code du numérique congolais confère déjà certaines prérogatives en la matière, notamment pour les interceptions ou les autorisations délivrées par l'Agence nationale compétente, il demeure néanmoins nécessaire de renforcer ce dispositif par l'instauration de mécanismes explicites de contrôle judiciaire et parlementaire, accompagnés d'audits réguliers. Une telle exigence constitue une garantie essentielle pour concilier sécurité publique, protection des droits fondamentaux et respect de l'État de droit³¹.

- **Plateforme nationale de signalement** (inspirée de Pharos / Thésée) pour centraliser les plaintes, alertes et remonter les dossiers vers la DN-Cyber et le parquet³².

Pour garantir la compétence, le respect de la déontologie et la continuité de l'action publique dans le domaine crucial de la cybercriminalité, la création d'une instance nationale d'accréditation et de certification professionnelle dédiée aux opérateurs de la DN-Cyber s'avère indispensable. Cette instance aura pour mission fondamentale de structurer les parcours professionnels, depuis la qualification initiale jusqu'à l'accréditation continue, en passant par une spécialisation « *frontline*³³ ». Placée sous le signe de l'indépendance tout en œuvrant en étroite coordination avec les ministères concernés, cette autorité sera chargée de plusieurs prérogatives essentielles. Elle définira des référentiels de formation exigeants, couvrant des domaines aussi critiques que l'informatique judiciaire, la protection des données et le respect des droits fondamentaux. Elle sera également l'organe de validation de la conformité des cursus universitaires et techniques, et tiendra un registre public des agents accrédités, garantissant ainsi une parfaite transparence³⁴.

L'objectif ultime de cette réforme est triple. Il s'agit, d'une part, de mettre un terme à la disparité actuelle des formations pour élever l'ensemble des compétences sur le territoire. D'autre part, cette harmonisation vise à sécuriser la chaîne de preuves numériques, condition sine qua non de leur admissibilité devant les tribunaux. Enfin, et c'est là son ambition fondamentale, cette instance contribuera à renforcer la protection des droits des justiciables dans un environnement numérique en constante évolution. L'accréditation devra impérativement intégrer des modules obligatoires en informatique légale. Ils couvriront notamment le recueil et la préservation des preuves numériques, le maintien rigoureux de la chaîne de conservation, les méthodes d'analyse spécialisées, ainsi que les règles de présentation devant l'autorité judiciaire afin de garantir l'admissibilité des éléments produits. Ces modules devront faire l'objet de mises à jour régulières, en adéquation avec l'évolution technologique et jurisprudentielle, et être sanctionnés par des évaluations pratiques destinées à mesurer la compétence opérationnelle des apprenants³⁵.

de la pensée du juriste italien Luigi Ferrajoli, s'oppose aux tendances répressives qui privilégient l'efficacité de la sanction au détriment des droits procéduraux

²⁹ Loi organique n°11/013 du 11 août 2011, Op.cit. et Ordonnance-loi n°23/010, Op.cit.

³⁰ Article 5 et 323, Ordonnance-loi n°23/010 du 13 mars 2023, Op.cit.

³¹ RDC, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, Op.cit. ; Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux TIC, Op.cit.

³² Expériences françaises/Belgique : France, LOPMI 2023, Op.cit. ; Belgique, Loi 28/11/2000, Op.cit.

³³ Une spécialisation *frontline* désigne une formation ou un domaine d'expertise orienté vers l'intervention directe sur le terrain, au contact immédiat avec les réalités opérationnelles (public, justiciables, menaces ou situations d'urgence), contrairement aux fonctions de soutien ou d'analyse exercées en arrière-plan.

³⁴ Peter Neyroud, Review of Police Leadership and Training, Home Office, 2011, pp.14–15, 49.

³⁵ Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed., Academic Press / Elsevier, 2011 — chap.1 (pp.3–32) ; chap.3 (pp.49–81).

4.2. Prérogatives opérationnelles et cadre procédural

- **Prérogatives** : conduite d'enquêtes numériques, demande d'accès aux données de connexion sous réquisition judiciaire, saisie et examen forensique³⁶ (criminalistique ou informatique légale) de matériels informatiques, coordination avec opérateurs et institutions financières pour le suivi des flux frauduleux³⁷.
- **Garanties procédurales** : toute mesure intrusive (interception, perquisition technique, accès aux données sensibles) doit reposer sur une réquisition motivée du Ministère public ou une autorisation judiciaire, durée limitée et contrôle de proportionnalité afin d'éviter les dérives observées dans certains textes étrangers³⁸.
- **Formation et accréditation** : les OPJ spécialisés doivent suivre une formation pluridisciplinaire (informatique judiciaire, protection des données, droit processuel) et être accrédités selon des standards nationaux, avec recyclage régulier, modèle inspiré des unités belges/fédérales et françaises³⁹.

4.3. Coopération nationale et internationale

Protocoles de coopération entre la DN-Cyber, l'Autorité de régulation du numérique (ARN), l'Agence nationale de cybersécurité et le parquet⁴⁰. Accords bilatéraux et multilatéraux (INTERPOL Cyber, conventions africaines) pour les enquêtes transfrontalières et l'extradition⁴¹ de cyberdélinquants⁴².

V. MESURES PRATIQUES ET FEUILLE DE ROUTE (CALENDRIER OPÉRATIONNEL)

La première phase, couvrant les six premiers mois, consiste en la création administrative de la Direction nationale de la cybersécurité (DN-Cyber) par arrêté ministériel, au recrutement du personnel minimal et à l'équipement de la cellule pilote installée à Kinshasa. Elle inclut également l'élaboration d'instructions opérationnelles précises sur les procédures de réquisition afin d'assurer la cohérence et la légalité des interventions⁴³. La deuxième phase, s'étendant de six à dix-huit mois, est consacrée au renforcement des capacités opérationnelles. Elle prévoit la formation intensive des officiers de police judiciaire (OPJ) ainsi que le déploiement d'une unité de réponse aux incidents informatiques au sein de la Police nationale congolaise (CSIRT-PNC). Elle prévoit aussi la signature de protocoles de coopération avec l'Autorité de régulation des postes, des télécommunications et du numérique (ARN) ainsi qu'avec les opérateurs de réseaux. Enfin, elle prévoit le lancement effectif d'une plateforme nationale de signalement des cyberinfractions⁴⁴. La troisième et dernière phase, prévue entre dix-huit et trente-six mois, marque l'extension du dispositif au niveau provincial, l'ouverture aux échanges et partenariats internationaux, ainsi que la réalisation d'audits indépendants visant à évaluer la conformité du système en matière de protection des données et de respect des droits fondamentaux des citoyens⁴⁵.

³⁶ Le terme forensique (du latin forensis, « relatif au forum » ou « à la justice ») désigne l'application des sciences et des techniques d'investigation à la résolution des questions judiciaires, en particulier dans le cadre des enquêtes pénales. Il renvoie à l'ensemble des méthodes scientifiques telles que l'analyse ADN, la balistique, la toxicologie, l'informatique légale ou la médecine légale utilisées pour collecter, analyser et interpréter des preuves matérielles afin d'éclairer la vérité judiciaire. En droit pénal contemporain, l'approche forensique constitue un maillon essentiel de la police scientifique et technique, permettant d'appuyer les investigations, de renforcer la fiabilité des preuves et d'assurer le respect des droits de la défense par une expertise objective et méthodiquement vérifiable

³⁷ Appui sur articles 126-130 et article 142 de la loi 20/017, Op.cit.. Loi n°20/017 du 25 novembre 2020, Op.cit.

³⁸ Principes repris dans les articles 126-130, Loi n°20/017- critique comparée : Tunisie Décret-loi 2022-54

³⁹ Belgique, Loi du 28 novembre 2000, Op.cit. et France, LOPMI 2023, Op.cit.

⁴⁰ Ordonnance-loi n°23/010, Op.cit. ; Loi n°20/017, Op.cit.

⁴¹ Article 86, Loi organique n°11/013, Op.cit. lié à l'intégration du BCN-INTERPOL à la PNC

⁴² Le terme cyberdélinquant désigne toute personne qui commet, intentionnellement et en violation de la loi, des actes délictueux à l'aide des technologies de l'information et de la communication, notamment par le biais d'Internet, des réseaux sociaux ou d'autres systèmes informatiques. Cette catégorie de délinquant opère dans le cyberspace et se livre à des infractions variées telles que l'accès frauduleux à des systèmes informatiques, le vol de données, l'escroquerie en ligne, la diffusion de fake news, la sextorsion ou encore le cyberharcèlement. Le cyberdélinquant se distingue du cybercriminel principalement par l'ampleur et la gravité de ses actes : si le second commet des crimes d'envergure souvent organisés, le premier agit généralement à titre individuel et sur des infractions de moindre gravité, bien que leurs actions puissent avoir des conséquences considérables sur la sécurité numérique, la vie privée et l'ordre public

⁴³ Se fonder sur Loi organique n°11/013, Op.cit. et Ord-loi 23/010, Op.cit.

⁴⁴ Inspiration : France et Sénégal

⁴⁵ Références : Loi n°20/017, Op.cit., Ordonnance n°23/010, Op.cit.

VI. RISQUES, LIMITES ET GARDE-FOUS DÉMOCRATIQUES

La mise en place d'une police du numérique comporte des risques : instrumentalisation politique, surveillance massive, atteinte au secret des correspondances. Pour y remédier, il faut des garde-fous : contrôle judiciaire effectif pour toute mesure intrusive, transparence des instruments techniques, audits réguliers par une autorité indépendante de protection des données et formation aux droits de l'homme pour tous les enquêteurs. L'expérience tunisienne montre qu'un cadre large sans garanties robustes peut engendrer des critiques sérieuses ; la France et la Belgique soulignent l'importance d'un contrôle parlementaire et judiciaire effectif⁴⁶. Le choix d'un modèle dit « garantiste » n'est jamais anodin : il exprime une orientation fondamentale de l'ordre juridique, celle qui érige la protection des libertés individuelles en priorité face à l'exercice des pouvoirs répressifs de l'État. En d'autres termes, le garantisme postule que la puissance pénale ne doit intervenir qu'en dernier ressort et dans les limites strictement nécessaires à la préservation de l'ordre public. Il en résulte que toute mesure attentatoire aux droits fondamentaux, qu'il s'agisse de la surveillance, des interceptions de communications ou de toute autre forme d'ingérence, doit précisément être encadrée par la loi, soumise à des conditions de légalité, de nécessité et de proportionnalité. Par ailleurs, le justiciable doit toujours disposer de voies de recours effectives, accessibles et adaptées, garantissant un contrôle juridictionnel rigoureux et une transparence démocratique dans la mise en œuvre de ces prérogatives étatiques⁴⁷.

CONCLUSION

La RDC a franchi des étapes législatives importantes (loi n° 20/017 ; ordonnance-loi n°23/010) ; il est maintenant impératif de traduire ces normes en capacités opérationnelles. La création d'une Direction nationale de la cyberpolice intégrée à la PNC, articulée avec l'Agence nationale de cybersécurité et l'Autorité de régulation du numérique est une réponse réaliste et proportionnée. Elle doit être conçue sur la base d'un triptyque : professionnalisation, coopération et garanties juridiques.

BIBLIOGRAPHIE

I. Instruments juridiques

A. Instruments juridiques nationaux (RDC)

- Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de la communication et de l'information, Journal officiel de la RDC, numéro spécial, Kinshasa, 22 septembre 2021.
- Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, Journal officiel de la RDC, numéro spécial, Kinshasa, 11 avril 2023.
- Loi organique n°11/013 du 11 août 2011 définissant l'organisation de la Police nationale congolaise, Journal officiel de la RDC, n°spécial, 57^e année, Kinshasa, 23 août 2011.

B. Instruments juridiques étrangers

- Belgique, Loi du 28 novembre 2000 relative à la criminalité informatique, Moniteur belge, Bruxelles.
- Cameroun, Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité, Journal officiel, Yaoundé.
- Côte d'Ivoire, Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, Journal officiel, Yamoussoukro.
- France, LOI n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI), Journal officiel, France.
- Maroc, Loi n°07-03 du 11 novembre 2003 complétant le Code pénal en matière d'infractions aux systèmes de traitement automatisé des données, Bulletin officiel.
- Sénégal, Loi n°2008-11 du 25 janvier 2008 relative à la cybercriminalité, Journal officiel du Sénégal, Dakar.
- Tunisie, Décret-loi n°2022-54 du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication, Journal officiel, Tunis.

II. Ouvrages

- CASEY, EOGHAN, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3^e éd., Academic Press / Elsevier, 2011.
- DOUZET, Frédéric (et al.), Les guerres de l'information à l'ère numérique, PUF / Cairn, 2022.

⁴⁶ Tunisie, Décret-loi n°2022-54 ; France, LOPMI 2023 ; Belgique, Loi 28/11/2000

⁴⁷ Luigi Ferrajoli, Diritto e ragione. Teoria del garantismo penale, Laterza, 1995 — développement doctrinal sur le garantisme (voir références citées en commentaires doctrinaux)

- FERRAJOLI, Luigi, DIRITTO E RAGIONE. Teoria del garantismo penale, Laterza, 1995.
- NEYROUD, Peter, Review of Police Leadership and Training, Home Office, 2011.

III. Article de revues

- PATCHIN, Justin W. & HINDUJA, Sameer, « Sextortion Among Adolescents: Results From a National Survey of U.S. Youth », *Sexual Abuse: A Journal of Research and Treatment*, vol. 32, n°1, 2019/2020, p. 30-54.