ENCADREMENT NORMATIF DE LA REPRESSION DE LA CYBERCRIMINALITE EN COTE D'IVOIRE

REGULATORY FRAMEWORK FOR THE REPRESSION OF CYBERCRIME IN COTE D'IVOIRE

VEH GOUE ARNAUD LANDRY
Cel. (+225) 0748143718/0102901515
Email : gouelandry@gmail.com

RESUME

Cette étude a pour objectif d'analyser l'effectivité ainsi que les insuffisances du dispositif normatif ivoirien encadrant la répression de la cybercriminalité. Elle examine le processus de construction du droit ivoirien de la cybercriminalité, à travers l'élaboration et l'adaptation des normes juridiques visant à prévenir et à sanctionner les infractions commises dans l'environnement numérique, tout en mettant en lumière les enjeux et les limites de l'application de ce cadre juridique. L'analyse mobilise les apports des théories positiviste du droit, fonctionnelle et critique ou sociologique afin d'apprécier la cohérence interne, la portée et les limites du dispositif normatif, ainsi que ses effets sur les libertés. Dans ce contexte, la transformation numérique impose une adaptation permanente du cadre juridique afin de garantir la protection des droits numériques, de soutenir l'innovation et d'assurer la sécurité dans les espaces virtuels et matériels.

Mots-clés : Droits numériques, cybercriminalité, législations, répression, prévention.

ABSTRACT

This study aims to analyze both the effectiveness and the shortcomings of the Ivorian regulatory framework governing the repression to cybercrime. It examines the process of constructing Ivorian cybercrime law through the development and adaptation of legal norms designed to prevent and punish offenses committed in the digital environment, while highlighting the challenges and limits of applying this legal framework. The analysis draws on contributions from positivist, functional, and critical or sociological legal theories to assess the internal coherence, scope, and limitations of the regulatory system, as well as its effects on freedoms. In this context, digital transformation requires the continuous adaptation of the legal framework to ensure the protection of digital rights, support innovation, and guarantee security in virtual and physical spaces.

Keywords : Digital rights, cybercrime, legislations, repression, prevention**.**

I-INTRODUCTION

L'essor fulgurant des technologies de l'information et de la communication constitue un vecteur majeur d'opportunités pour le continent africain. L'Afrique est aujourd'hui la région du monde où les réseaux Internet et de téléphonie mobile connaissent la croissance la plus rapide, avec une expansion remarquable des services bancaires mobiles (Interpol, 2015). Les mutations engendrées par la révolution numérique, conjuguées à la diffusion rapide de l'accès à Internet, ont profondément remodelé l'environnement économique des entreprises, des citoyens et des

États. Toutefois, cette transformation s'accompagne d'une recrudescence des cyberattaques, devenues une menace mondiale durable, en dépit des dispositifs de sécurisation (Artci, 2024). La Côte d'Ivoire n'échappe pas à cette réalité et se trouve, à l'instar d'autres nations, confrontée à une montée croissante des risques cybernétiques (Artci, 2024). Cependant, cette transition accélérée vers le numérique expose davantage la région aux risques de cyberattaques. La numérisation a engendré une production et une diffusion massive d'informations, issues de sources multiples et presque illimitées. Grâce à son accessibilité et à son architecture décentralisée, Internet favorise l'intensification des échanges interpersonnels et ouvre de vastes perspectives de participation au débat public. Cette évolution comporte à la fois des retombées bénéfiques et des effets indésirables (Koffi, 2022). Les entreprises apparaissent particulièrement exposées aux cyberattaques en raison de l'insuffisance des infrastructures de protection et du déficit de compétences spécialisées. À cela s'ajoute un manque d'information et de sensibilisation aux enjeux de cybersécurité. Ainsi, plus de 90 % des entreprises africaines exerceraient leurs activités sans recourir aux protocoles de cybersécurité requis (Nadéon, 2022). Selon une étude menée en 2022-2023 par Check Point Research sur l'évolution des menaces cybernétiques en Afrique, les organisations africaines ont enregistré, au premier trimestre 2023, le nombre moyen hebdomadaire de cyberattaques le plus élevé au monde. Ces attaques reposaient principalement sur des logiciels malveillants (80 %) et des techniques d'ingénierie sociale (52 %), compromettant des ordinateurs, des serveurs et des équipements réseau dans 85 % des cas. Par ailleurs, 37 % des intrusions réussies résultaient de l'exploitation de vulnérabilités techniques, tandis que l'utilisation frauduleuse d'identifiants a été constatée dans 10 % des incidents (Artci, 2024). L'analyse des rapports d'activité des trois dernières années de l'Agence Nationale des Systèmes de Sécurité et de l'Informatique (ANSSI) de Côte d'Ivoire, montre une hausse continue des plaintes. Celles-ci sont passées de 607 en 2022 à 802 en 2023, puis à 2328 en 2024, soit une augmentation de 283% entre 2022 et 2024 (Anssi, 2024). Elle se justifierait par le basculement de la criminalité traditionnelle dans l'espace numérique, par un usage accru de l'Internet comme outil de commission, l'accroissement du nombre d'utilisateurs des numériques, ainsi que la diversification des services en lignes. Le nombre de personnes physiques victimes de cybercriminalité s'est élevé à 11 563, contre 7 677 en 2023, soit une progression de 50,62 %. Le préjudice financier est estimé à plus de 5 milliards de FCFA entre 2022 et 2024 (Anssi, 2024). S'agissant des personnes morales, 537 entreprises ont été touchées en 2024, contre 458 l'année précédente, ce qui correspond à une hausse de 17,25 %. Ces

données démontrent sans ambiguïté que la cybercriminalité demeure une réalité préoccupante et persistante, nécessitant la mise en œuvre de mesures rigoureuses et coordonnées afin d'endiguer efficacement cette forme de délinquance numérique (Veh, 2025). Il demeure complexe pour les États de concilier la quête de souveraineté numérique avec la garantie effective des droits et libertés des usagers du numérique. À ce jour, d'importants efforts sont entrepris afin de mettre en place un cadre législatif et réglementaire crédible et sécurisant à l'échelle du continent africain, malgré les difficultés liées à son adaptation et à sa mise en œuvre. Cette entreprise est d'autant plus délicate qu'elle s'inscrit dans un environnement technologique en constante évolution, marqué par l'influence d'entreprises hautement technologiques, économiquement puissantes et, pour la plupart, étrangères au continent (Tano-Bian, 2025). En matière d'élaboration et d'harmonisation des normes, la démarche concertée engagée par les États membres de la CEDEAO et de l'UEMOA s'inspire, certes, de la technique européenne, mais demeure empreinte de prudence ; toutefois, certains dispositifs gagneraient à être formulés avec davantage de précision (Tano-Bian, 2015). L'environnement numérique reste traversé, par ailleurs, par de vives préoccupations liées à la censure, à la surveillance et à la protection des données personnelles, autant d'enjeux qui affectent significativement les différents groupes sociaux. Malgré les avancées juridiques enregistrées, une amélioration urgente de l'effectivité des lois relatives à la protection des données et à la liberté d'expression s'impose (LONDA, 2024). La Commission de l'Union Africaine reconnaît cette situation et souligne que « les principaux défis au développement du commerce électronique en Afrique sont liés à des problèmes de sécurité » (UA, 2014). Dans ce contexte, les États s'emploient à définir des cadres juridiques et politiques visant à protéger et à garantir les libertés individuelles face aux cyberattaques et à la cybercriminalité. La loi devient ainsi, dans la plupart des pays, le référentiel central pour réguler l'usage des outils et systèmes informatiques, dans le but de prévenir efficacement les risques (Agnidé & Ali, 2024). L'approche adoptée s'inscrit dans l'esprit de ce que soulignait J.-J. Rousseau : il s'agit de réguler et d'encadrer l'utilisation des technologies de manière libre et responsable, plutôt que de l'interdire (Agnidé & Ali, 2024). Les réponses juridiques à la cybercriminalité présentent de fortes spécificités nationales, la matière pénale relevant de la souveraineté des États et caractérisée par le caractère strictement national des politiques criminelles, en particulier celles liées au droit pénal (Cissé, 2011). La mise en œuvre du dispositif répressif de la cybercriminalité permet d'aborder à la fois l'aspect préventif et l'aspect coercitif. La répression suit ainsi différentes étapes. Concernant le volet

préventif, c'est-à-dire les actions entreprises par les acteurs de la lutte pour éviter la commission d'infractions, plusieurs obstacles demeurent néanmoins (Tano-Bian, 2015). Selon la CEDEAO, plusieurs défis demeurent à surmonter, l'adoption effective de législations par certains États, la formation des acteurs chargés de l'application des lois pénales, ainsi que la modernisation des méthodes et outils de collecte des preuves. L'organisation conclut que la mise en œuvre d'actions communes, tant sur le plan du droit pénal substantiel que procédural, constitue la voie privilégiée pour renforcer la lutte contre la cybercriminalité dans la région ouest-africaine (Koffi, 2022). La sévérité des peines prévues témoigne de la prise de conscience, par l'ensemble des États, de la gravité de la cybercriminalité et des menaces qu'elle fait peser sur les États, les économies, les sociétés et les individus. La diversité des sanctions traduit également la volonté d'adapter les réponses à la complexité des phénomènes cybercriminels (Cissé, 2011). Toutefois, un risque d'incohérence demeure, tant au sein des États qu'entre eux. Ce risque découle notamment du chevauchement entre les sanctions prévues pour les infractions « classiques » dans les codes pénaux et celles issues des textes spécifiquement destinés à lutter contre la cybercriminalité, ainsi que de la multiplication des interventions législatives face à la diversité des cyber infractions (Cissé, 2011). Ainsi, au fil du temps, les enjeux liés à la sécurité se sont intensifiés parallèlement à l'évolution des modes de communication : de l'oralité à l'écriture, puis de l'écriture à l'échange et au traitement des informations via les ordinateurs et les réseaux. De ce fait, les problématiques de sécurité, qui incluaient initialement la protection contre les abus de l'administration envers les administrés, s'étendent aujourd'hui à la protection des données personnelles de l'ensemble des utilisateurs du réseau (Tano-Bian, 2015). La réglementation de la cybercriminalité à l'échelle internationale constitue un enjeu majeur pour lutter efficacement contre ce phénomène transnational (Veh, 2019). De nombreuses conventions et traités internationaux ont été adoptés afin de favoriser la coopération entre les États dans la prévention, la détection, l'investigation et la répression des infractions liées au cyberespace. Ces instruments juridiques jouent un rôle déterminant en facilitant la coopération internationale, en harmonisant les législations et en offrant des mécanismes d'entraide judiciaire. Néanmoins, malgré ces progrès, plusieurs défis subsistent, notamment la diversité des législations nationales, les difficultés liées à l'extraterritorialité des infractions et la complexité des enquêtes transfrontalières (Ghita & Chadi, 2023). En Côte d'Ivoire, les autorités ont multiplié les initiatives à travers des dispositifs juridiques et des structures dédiées à la lutte contre la cybercriminalité. Sur le plan législatif, on relève notamment la loi n°2013-451 du 19

juin 2013 relative à la lutte contre la cybercriminalité, ainsi que la loi n°96-564 du 25 juillet 1996 portant protection de l'œuvre de l'esprit et des droits d'auteur, secteur également impacté par certaines formes de criminalité en ligne (Okou & Dagbé, 2025). Depuis 2013, une opération d'identification des puces des abonnés de téléphonie mobile a été mise en place afin de limiter l'anonymat facilitant la commission d'actes malveillants (Okou & Dagbé, 2025). L'État ivoirien a établi un cadre juridique et réglementaire complet en matière de cybersécurité et de lutte contre la cybercriminalité, comprenant des lois, des décrets et une ordonnance. Ce dispositif est renforcé par l'adhésion à plusieurs conventions internationales favorisant la coopération transfrontalière, ainsi que par la Stratégie Nationale de la Cybersécurité 2021-2025 (Anssi, 2024). Face à l'augmentation des actes de cybercriminalité et à la complexification des cybermenaces, la Côte d'Ivoire a adopté une approche proactive et stratégique. Dans ce cadre, le décret n° 2024-958 du 30 octobre 2024 a institué l'Agence Nationale de la Sécurité des Systèmes d'Information, offrant une réponse structurée, coordonnée et urgente à ces enjeux cruciaux (Anssi, 2024). Malgré des résultats techniques encourageants et un cadre juridique offrant des instruments de prévention, de sécurisation du cyberespace et de répression, l'évolution rapide du numérique et l'apparition constante de services innovants complexifient la situation et génèrent de nouveaux défis en matière de sécurité (Plcc, 2023). Les législations se durcissent progressivement, et l'idée de sanctionner les « voleurs de données » ou les pirates informatiques s'impose de plus en plus (Agnidé & Ali, 2024). Nonobstant l'instauration d'un cadre juridique spécifique destiné à réprimer la cybercriminalité et les réformes qui y ont été apportées, les infractions liées aux technologies de l'information et de la communication restent persistantes et en constante mutation en Côte d'Ivoire. Cette situation soulève des interrogations quant à l'adéquation, à la cohérence et à l'efficacité du dispositif normatif existant face aux évolutions technologiques et à la nature transnationale des infractions. Dès lors, la question centrale de cette étude est de savoir si le cadre juridique ivoirien de répression de la cybercriminalité permet réellement de lutter efficacement contre les infractions numériques, tout en respectant l'état de droit et en garantissant la protection des libertés fondamentales. La présente analyse s'inscrit dans une démarche méthodologique fondée sur une approche juridique à la fois analytique et descriptive des normes relatives à la cybercriminalité. Cette démarche vise à examiner la cohérence interne, la portée ainsi que les limites du cadre normatif encadrant la répression des infractions numériques. À cette fin, elle mobilise les apports de la théorie positiviste du droit, de la théorie fonctionnelle et de l'approche critique ou sociologique,

afin de rendre compte de manière complète et structurée de l'objet d'étude. En effet, selon Hans Kelsen (1934), la théorie pure du droit offre un cadre d'analyse permettant d'examiner la hiérarchie des normes, d'apprécier la validité juridique des règles répressives, d'en vérifier la cohérence interne et d'identifier d'éventuels conflits normatifs. Cette approche apparaît pertinente pour évaluer la conformité des infractions numériques au principe de légalité criminelle, la précision des incriminations en matière de cybercriminalité ainsi que leur compatibilité avec les droits fondamentaux. La théorie fonctionnaliste du droit, développée par Hugues Rabault (2018), permet d'apprécier, par ailleurs, si le cadre juridique atteint son objectif de lutte contre la cybercriminalité, d'en mesurer l'efficacité pratique et d'évaluer son adaptation à la dimension transnationale du phénomène numérique. Cette approche privilégie l'analyse de l'efficacité concrète des normes plutôt que leur seule validité formelle. Enfin, l'approche critique ou sociologique inspirée des travaux de Michel Foucault (1975) contribue à comprendre la manière dont les sociétés construisent les notions de normalité et de déviance, et à analyser les mécanismes de surveillance comme dispositifs de contrôle social. Elle permet d'examiner les enjeux liés à la surveillance numérique, l'équilibre entre impératifs de sécurité et protection des libertés fondamentales, ainsi que les effets du pouvoir étatique dans l'espace numérique, tout en mettant en lumière les limites du cadre normatif et ses impacts sur les libertés. Le présent travail a pour ambition d'analyser, l'effectivité et les insuffisances du dispositif normatif ivoirien encadrant la répression des infractions liées à la cybercriminalité.

II. APPROCHE METHODOLOGIQUE

Elle intègre la description du terrain de recherche, la définition de la population cible et de l'échantillon retenu, les techniques de collecte des données employées, ainsi que les méthodes d'analyse adoptées.

2.1 Terrain d'étude et échantillon d'enquête

La ville d'Abidjan, capitale économique de la Côte d'Ivoire, a été retenue comme cadre d'étude. Elle présente un intérêt particulier en raison de la concentration des principaux acteurs engagés dans la lutte contre la cybercriminalité, notamment l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le Côte d'Ivoire Computer Emergency Response Team (CI-CERT), le Centre de Fusion et d'Analyse de Données (CFAD), ainsi que les juridictions judiciaires compétentes pour connaître des infractions cybercriminelles. Le développement de

l'usage d'Internet y est remarquable. Aucun quartier d'Abidjan n'est en marge de cette dynamique d'inclusion numérique. La ville se caractérise par une forte densité d'usagers et une connectivité Internet étendue. Elle enregistre un nombre important de victimes, tandis que les cyberdélinquants y opèrent en toute discrétion sur l'ensemble du territoire urbain.

2.2 Population d'enquête

L'échantillon est constitué de 85 individus sélectionnés selon une méthode d'échantillonnage raisonné et ciblé. Il comprend 10 victimes, dont les témoignages ont permis de comprendre les démarches entreprises pour porter plainte ainsi que leur vécu des procédures pénales ; 10 cyberdélinquants, dont les expériences ont éclairé les conditions de leur interpellation et leur perception du déroulement des procédures judiciaires ; 10 greffiers, dont la collaboration a contribué à la compréhension du déroulement de la procédure pénale, à la vérification de l'authenticité des actes établis par les magistrats au cours du procès et au respect du formalisme juridictionnel par le juge ; 10 magistrats et substituts du procureur, dont les entretiens ont permis d'analyser les mécanismes procéduraux et les dispositions légales mobilisées pour rendre les décisions de justice après examen des dossiers ; 20 fonctionnaires de police de l'ANSSI, dont l'apport a facilité la compréhension du traitement des plaintes en matière de cybercriminalité, des enquêtes menées conformément au code de procédure pénale pour constater les infractions, en identifier les auteurs et rassembler les preuves ; 5 agents du CFAD et du CI-CERT, dont la contribution a permis d'appréhender les méthodes de collecte, de traitement des données, et d'analyse des informations.

2.3. Techniques de recueil des données

L'analyse documentaire et l'entretien ont constitué les principaux instruments de collecte des données.

2.3.1 Analyse documentaire

L'analyse documentaire consiste en un examen méthodique et approfondi des documents en lien avec le sujet, dans le but d'en tirer des informations pertinentes pour une meilleure compréhension. Elle repose sur l'exploitation des textes législatifs et réglementaires relatifs à la cybercriminalité. Elle intègre l'analyse des instruments juridiques régionaux et internationaux. Cette analyse s'appuie, par ailleurs, sur la doctrine juridique, ouvrages spécialisés, articles scientifiques, rapports institutionnels ainsi que sur la jurisprudence

nationale disponible en matière de cybercriminalité. L'ensemble de ces sources permet, d'une part, de comprendre les fondements juridiques internes de la répression de la cybercriminalité et les réformes récentes intervenues dans ce domaine et, d'autre part, d'identifier les différentes typologies d'infractions ainsi que le régime des sanctions prévues par le droit positif.

2.3.2 Entretiens

Les entretiens constituent une méthode qualitative de collecte des données fondée sur des échanges directs avec les personnes sélectionnées dans le cadre de l'étude. Ils ont été menés sous forme d'entretiens semi-directifs, à l'aide d'un guide préalablement élaboré en fonction des objectifs de la recherche. Cette approche a permis de recueillir des informations détaillées sur les expériences, les pratiques professionnelles, les perceptions et les difficultés rencontrées par les différents acteurs impliqués dans la lutte contre la cybercriminalité. Les entretiens ont ainsi offert la possibilité d'approfondir certains aspects non accessibles par l'analyse documentaire, de confronter les discours aux réalités pratiques et de mieux comprendre le fonctionnement concret des mécanismes de prévention, d'enquête et de répression des infractions cybercriminelles avec les différentes composantes de la population d'enquête.

2.3.3 Méthode d'analyse

Les données collectées font l'objet d'une analyse croisée mobilisant les approches normative, critique, systémique et qualitative. L'analyse normative consiste à identifier les incriminations prévues par la loi, les sanctions applicables ainsi que les mécanismes procéduraux encadrant la répression. L'analyse critique vise, pour sa part, à apprécier l'effectivité des normes en vigueur et à examiner leur conformité aux libertés et droits fondamentaux. L'analyse systémique s'intéresse à l'articulation entre les normes juridiques et les institutions chargées de leur mise en œuvre, en tenant compte des dynamiques institutionnelles et des interactions entre acteurs. Enfin, l'analyse qualitative permet de confronter les discours des enquêtés aux réalités pratiques, afin de comprendre le fonctionnement concret des mécanismes de prévention, d'enquête et de répression des infractions cybercriminelles, ainsi que les jugements de valeur relatifs à ce qui est considéré comme acceptable ou non dans l'espace numérique**.**

III. RESULTATS

Les investigations menées dans le cadre de cette étude mettent en lumière les fondements juridiques de la répression de la cybercriminalité en Côte d'Ivoire, ainsi que les enjeux et les limites liés à l'effectivité du cadre normatif ivoirien.

3.1. Fondements juridiques de la répression de la cybercriminalité en Côte d'Ivoire

La répression de la cybercriminalité en Côte d'Ivoire repose sur un ensemble cohérent de textes nationaux, complétés et adossés aux engagements internationaux.

3.1.1. Construction normative du droit ivoirien de la cybercriminalité

La construction normative du droit ivoirien de la cybercriminalité renvoie au processus d'élaboration, d'adaptation et d'articulation des normes juridiques destinées à encadrer, prévenir et réprimer les infractions commises au moyen des technologies de l'information et de la communication. Elle s'est opérée progressivement, sous l'influence de facteurs internes (essor du numérique, montée des cyberinfractions) et externes (harmonisation internationale).

3.1.1.1 Sources législatives internes

Le cadre juridique ivoirien en matière de cybercriminalité et de sécurité numérique repose sur plusieurs textes fondamentaux. La loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, modifiée en ses articles 17, 33, 58, 60, 62 et 66 par la loi n°2023-593 du 07 juin 2023, constitue le socle de la répression des infractions numériques. Elle définit la cybercriminalité, en son article premier, comme l'ensemble des infractions pénales commises au moyen ou sur un réseau de télécommunication ou un système d'information. Elle incrimine notamment les atteintes aux systèmes informatiques, aux systèmes de cryptologie et aux systèmes automatisés de données, tout en renforçant les sanctions applicables en cas de violation. La loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel établit le régime juridique applicable à la protection des données personnelles. Elle vise à garantir une protection globale de la confidentialité des informations des utilisateurs, ainsi que la sauvegarde de leurs droits et libertés fondamentaux. La loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques encadre le commerce électronique, notamment la formation des contrats par voie électronique. Elle réglemente également l'archivage électronique, la sécurisation des transactions ainsi que l'usage de la cryptologie. Le code pénal ivoirien, issu de la loi n°2019-574 du 26 juin 2019 et modifié par la loi n°2021-893 du 21

décembre 2021, complète ce dispositif. Les modifications apportées en 2021 ont introduit ou adapté certaines infractions afin de prendre en compte les réalités du cyberespace. L'ordonnance n°2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives, prévoit la mise en place, par décret, de référentiels encadrant notamment la sécurité des données échangées par voie électronique. Cette ordonnance a été modifiée par l'ordonnance n°2024-950 du 30 octobre 2024, qui a procédé à la modification des articles 3 et 17, en remplaçant les mentions de l'ARTCI par « l'organisme compétent », et à l'abrogation de l'article 50 de la loi n°2013-546 relative aux transactions électroniques. Ces réformes visent à renforcer la coordination en matière de cybersécurité en confiant la protection des systèmes d'information et des transactions électroniques à un organisme spécialisé. Dans cette dynamique, le décret n°2024-958 du 30 octobre 2024 a institué l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), chargée d'assurer la protection et la sécurisation des infrastructures numériques nationales.

3.1.1.2 Influence des normes régionales et internationales

Les engagements internationaux et africains ont largement contribué à la structuration du cadre normatif ivoirien en matière de cybercriminalité. En tant qu'État partie à plusieurs conventions, la Côte d'Ivoire a intégré l'essentiel des recommandations issues de ces instruments internationaux dans sa législation interne. La Convention sur la cybercriminalité, adoptée à Budapest le 23 novembre 2001 par le Conseil de l'Europe, constitue le principal instrument international de recommandation en matière de répression des infractions informatiques. Par ce texte, les États membres et signataires s'engagent à mettre en œuvre une politique pénale harmonisée visant à protéger la société contre la criminalité dans le cyberespace, à travers l'adoption de lois adaptées et le renforcement de la coopération internationale. Elle identifie quatre grandes catégories d'infractions que les États doivent ériger en infractions dans leur droit interne : les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques ; les infractions informatiques proprement dites ; les infractions liées au contenu ; et les atteintes à la propriété intellectuelle et aux droits connexes. Elle prévoit également un ensemble de pouvoirs et de procédures destinés à faciliter les enquêtes et poursuites pénales, notamment la conservation rapide des données informatiques, la perquisition et la saisie de données stockées, la collecte en temps réel des données de trafic, ainsi que les règles de compétence. Ces mesures sont assorties de garanties procédurales

encadrant leur mise en œuvre. Au-delà des réformes qu'elle a directement inspirées, elle a constitué un véritable point de départ des évolutions législatives engagées par de nombreux États, soucieux d'assurer une protection efficace des personnes, des biens et des réseaux informatiques face aux nouvelles formes de criminalité. Les instruments juridiques africains, par ailleurs, ont également joué un rôle déterminant dans la consolidation du cadre normatif en matière de cybersécurité et de protection des données. La Convention de Malabo du 27 juin 2014 vise à instaurer un cadre juridique harmonisé aux niveaux sous-régional, régional et international en matière de cybersécurité et de protection des données à caractère personnel. Elle définit les engagements des États membres de l'Union africaine dans la perspective de la construction d'une société africaine de l'information sécurisée et respectueuse des droits fondamentaux. La Côte d'Ivoire a ratifié cette convention le 3 avril 2023, marquant ainsi son engagement à aligner sa législation nationale sur les standards africains en la matière. En outre, l'Acte additionnel relatif à la protection des données à caractère personnel dans l'espace CEDEAO, adopté à Abuja le 16 février 2010, encourage les États membres à se doter d'un cadre juridique garantissant la protection de la vie privée et des données professionnelles. Il encadre notamment la collecte, le traitement, la transmission, le stockage et l'utilisation des données à caractère personnel, tout en préservant les exigences liées à l'ordre public. Enfin, la Directive portant lutte contre la cybercriminalité dans l'espace CEDEAO, adoptée les 17 et 19 août 2011 à Abuja, a pour objectif d'harmoniser les législations pénales des États membres de la Communauté Economique des États de l'Afrique de l'Ouest face au phénomène de la cybercriminalité. Elle prévoit l'adaptation du droit pénal matériel ainsi que des règles de procédure pénale afin de permettre une répression efficace des infractions commises dans le cyberespace. L'ensemble de ces conventions a fortement contribué à l'édification et au renforcement du droit positif ivoirien en matière de lutte contre la cybercriminalité. Elles ont servi de fondement et de référence à l'adaptation de la législation nationale, en permettant à la Côte d'Ivoire d'intégrer des normes conformes aux standards internationaux et régionaux, afin d'assurer une répression efficace des infractions commises dans le cyberespace.

3.1.2. Incriminations et sanctions prévues par le cadre juridique

Le dispositif juridique ivoirien en matière de cybercriminalité s'inscrit dans la dynamique des engagements internationaux et africains ratifiés par la Côte d'Ivoire, notamment la Convention de Budapest sur la cybercriminalité et la Convention de Malabo. Au plan interne, la répression

repose principalement sur les Lois n°2013-451 relative à la lutte contre la cybercriminalité ; n°2013-450 relative à la protection des données à caractère personnel ; n°2013-546 relative aux transactions électroniques ainsi que certaines dispositions du Code pénal ivoirien.

3.1.2.1. Typologie des infractions cybercriminelles

Le droit ivoirien érige en infractions plusieurs comportements liés aux technologies de l'information et de la communication. Les infractions pénales pouvant être commises sur ou au moyen d'un système informatique, généralement connecté à un réseau, sont regroupées en trois grandes catégories.

3.1.2.1.1 Infractions spécifiques aux technologies de l'information et de la communication

Ce sont les infractions directement liées au fonctionnement des systèmes informatiques et des réseaux. Elles visent notamment : l'accès frauduleux à un système informatique qui consiste à pénétrer ou à se maintenir, sans autorisation, dans tout ou partie d'un système informatique. L'atteinte à l'intégrité des données ou des systèmes se caractérise par la suppression, la modification, l'altération ou l'introduction frauduleuse de données dans un système informatique. L'entrave au fonctionnement d'un système informatique correspond à toute action visant à perturber volontairement le fonctionnement normal d'un système. La fraude informatique désigne l'obtention d'un avantage patrimonial ou financier par la manipulation frauduleuse de données ou de systèmes informatiques. L'usurpation d'identité numérique consiste à utiliser, de manière frauduleuse, les données d'identification d'une autre personne. La diffusion de contenus illicites renvoie à la propagation, par voie numérique, de fausses informations, d'images à caractère indécent ou attentatoires à la dignité humaine, ainsi que de contenus à caractère raciste ou xénophobe. Les atteintes aux données à caractère personnel regroupent la collecte, le traitement, la conservation ou l'utilisation de données personnelles en violation des dispositions légales applicables. Les atteintes à la propriété intellectuelle en ligne consistent en la violation des droits reconnus aux auteurs, artistes, producteurs ou titulaires de marques, brevets et autres droits protégés, lorsque ces atteintes sont commises par le biais des technologies numériques. Ces infractions portent essentiellement atteinte à la sécurité, à l'intégrité et à la confidentialité des systèmes et des données.

3.1.2.1.2 Infractions liées aux technologies de l'information et de la communication

Cette catégorie regroupe les infractions de droit commun dont la commission est facilitée ou amplifiée par l'usage d'Internet ou des outils numériques. On y retrouve notamment : la pédopornographie et les infractions à caractère pédophile en ligne ; l'incitation au terrorisme ou à la haine raciale sur Internet ; les atteintes aux personnes (menaces, diffamation, harcèlement en ligne) ; les atteintes aux biens. La technologie constitue le vecteur de commission de l'infraction.

3.1.2.1.3 Infractions facilitées par les technologies de l'information et de la communication

Il s'agit d'infractions classiques dont l'exécution est rendue plus aisée par l'environnement numérique, telles que : les escroqueries en ligne (broutage) ; la contrefaçon et les violations des droits de propriété intellectuelle ; et toute autre forme de fraude exploitant les outils numériques. Dans cette hypothèse, les technologies de l'information et de la communication ne créent pas l'infraction en elle-même, mais en facilitent la réalisation et l'ampleur.

3.1.3 Acteurs et actes de procédure pénales

Les règles de procédure pénale ont été adaptées pour tenir compte des spécificités de la cybercriminalité, en aménageant les mécanismes classiques de traitement des infractions et en renforçant le dispositif par l'introduction de nouvelles procédures. L'intégration des infractions numériques dans le Code pénal a ainsi rendu nécessaire une révision de certaines règles procédurales. Des ajustements ont été apportés, notamment en matière de prescription, de preuve et de rédaction des procès-verbaux, pour tenir compte du contexte numérique. Cela inclut, entre autres : la conservation rapide des données informatisées archivées ; la perquisition et la saisie de données informatiques ; l'interception des données électroniques. La conduite des enquêtes et la constatation des infractions relèvent principalement des Officiers et Agents de Police Judiciaire (OPJ et APJ), généralement des fonctionnaires de police ou des gendarmes, qui disposent des prérogatives nécessaires pour appliquer ces procédures adaptées au cyberespace. C'est dans ce contexte qu'a été créée, par le décret n°2024-958 du 30 octobre 2024, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), offrant une réponse structurée, urgente et coordonnée aux enjeux critiques liés à la cybersécurité. Pour remplir efficacement ses missions, l'ANSSI s'est dotée de plusieurs centres techniques

spécialisés, certains étant spécifiquement consacrés à la lutte contre la cybercriminalité ou y apportant une contribution majeure, parmi lesquels : la PLCC : Plateforme de Lutte Contre la Cybercriminalité ; le CI-CERT : Côte d'Ivoire Computer Emergency Response Team ; et le CFAD : Centre de Fusion et d'Analyse de Données.

3.1.3.1 Acteurs

La lutte contre la cybercriminalité est principalement assurée par la PLCC. De 2011 à 2024, la PLCC était issue d'un partenariat entre l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) et la Direction Générale de la Police Nationale (DGPN). Avec le décret n°2024-958 du 30 octobre 2024, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) reprend désormais les missions de la DITT. La PLCC, qui était initialement hébergée au sein de la DITT, devient ainsi un département à part entière de l'ANSSI. La PLCC intervient en fonction de deux axes principaux notamment la prévention et la répression. La PLCC conseille et accompagne le grand public, les entreprises et les victimes afin de réduire les risques liés à la cybercriminalité. Les actions préventives sont menées en collaboration avec la Direction de la Communication et de la Sensibilisation et le Centre de Formation de l'ANSSI d'une part et d'autre part elle exerce l'ensemble des prérogatives de police judiciaire conformément au Code de procédure pénale, au Code pénal et aux textes régissant la cybercriminalité et la protection des données personnelles. Elle reçoit les plaintes, s'auto-saisir, constate les infractions, identifie les suspects et les met à la disposition des Parquets. Pour ses activités d'investigation et de répression, elle collabore étroitement avec le Centre de Fusion et d'Analyse de Données (CFAD). La PLCC travaille également avec plusieurs partenaires internes et externes : Police et Gendarmerie : pour le traitement des plaintes reçues en dehors d'Abidjan ; Services étrangers : pour les plaintes transfrontalières impliquant la Côte d'Ivoire ou pour la localisation de suspects sur leur territoire ; et la Cellule Nationale de Traitement des Informations Financières (CENTIF) pour les enquêtes liées au blanchiment de capitaux d'origine cybercriminelle. La PLCC est structurée autour de plusieurs services particulièrement les services des plaintes et de l'assistance aux victimes ; des Enquêtes spécialisées, incluant les atteintes à la dignité, les fraudes sur transactions électroniques et les investigations techniques; et de la coopération policière internationale, pour assurer la coordination avec les partenaires étrangers et régionaux. Ainsi, la PLCC constitue un pivot central de la politique de prévention

et de répression de la cybercriminalité, combinant expertise technique, enquêtes spécialisées et coopération régionale et internationale.

3.1.3.2 Actes de procédures pénales

L'ANSSI est chargée de recevoir et de traiter les plaintes relatives à la cybercriminalité, en menant ses enquêtes conformément aux dispositions du Code de procédure pénale. Avec ses Officiers et Agents de Police Judiciaire (OPJ et APJ), l'Agence accomplit l'ensemble des actes de police judiciaire nécessaires pour constater les infractions, identifier leurs auteurs et collecter les preuves. Elle procède à des enquêtes de flagrance ou préliminaires ; des auditions de victimes, témoins ou suspects ; la garde à vue de suspects ; des interpellations et arrestations ; la rédaction de procès-verbaux (PV) et de comptes rendus officiels des actes accomplis ; la transmission des dossiers aux autorités judiciaires compétentes, telles que le procureur ou le juge d'instruction. Les experts et agents assermentés de l'ANSSI sont habilités à collecter des preuves auprès de personnes physiques ou morales impliquées dans une infraction, notamment par la saisie de matériel informatique (ordinateurs, serveurs, supports de stockage, etc.) ; la réquisition de données de trafic ou d'identification auprès des fournisseurs de services numériques, d'accès à Internet et des opérateurs de télécommunications, la perquisition de systèmes informatiques dans le respect des règles de procédure pénale ; l'exploitation des journaux de logs et autres traces numériques ; la perquisition et saisie d'objets utiles à l'enquête (documents, équipements, etc.) et les données relatives aux abonnés doivent être conservées par les fournisseurs de service numérique pendant une période de dix ans. L'ANSSI peut intervenir en collaboration avec diverses structures de l'État pour la constatation de faits et la collecte de preuves numériques. Dans ce cadre, elle apporte son expertise aux OPJ, aux auxiliaires, aux services de police judiciaire et aux services de police administrative ; cette assistance est fournie lorsque l'expertise technique de l'ANSSI, en criminalistique numérique et en analyse de données massives, est formellement requise ; toutes les interventions et collaborations se font dans le strict respect des textes législatifs et réglementaires en vigueur.

3.1.4. Régime répressif applicable

La gravité et l'ampleur du phénomène de la cybercriminalité, ainsi que les menaces qu'il fait peser sur l'État, l'économie, la société et les individus, ont conduit la Côte d'Ivoire à adopter une double approche d'une part, une répression rigoureuse et d'autre part, une diversification

des sanctions, qu'elles soient principales, complémentaires ou de sûreté. Le système juridique prévoit ainsi une grande variété de sanctions. Aux peines privatives de liberté s'ajoutent des sanctions pécuniaires en tant que peines principales. L'emprisonnement demeure la réponse pénale de référence, qu'il soit prononcé cumulativement ou alternativement avec une amende. Les infractions liées aux numériques affectent fréquemment des intérêts économiques majeurs et peuvent porter atteinte à des valeurs fondamentales telles que la sûreté de l'État ou la dignité de la personne humaine. Conscients de cette dimension économique et stratégique, le législateur a instauré des sanctions pénales adaptées, caractérisées par des amendes d'un montant singulièrement élevé, destinées à dissuader les auteurs de ces infractions. À ces peines principales s'ajoutent des peines complémentaires, obligatoires ou facultatives, offrant aux juridictions une large marge d'appréciation. Les juridictions disposent ainsi d'un éventail étendu de peines complémentaires leur permettant de sanctionner efficacement les actes de cybercriminalité.

3.1.4.1 Peines principales

Le droit ivoirien prévoit principalement des peines privatives de liberté. L'emprisonnement constitue la sanction pénale de référence en matière de cybercriminalité. Les peines varient selon la gravité des faits et peuvent être aggravées en cas de circonstances particulières (bande organisée, atteinte à la sûreté de l'État, préjudice important) ; des peines pécuniaires (amendes) souvent élevées, elles tiennent compte de la dimension économique des infractions numériques. Elles peuvent être prononcées cumulativement ou alternativement avec l'emprisonnement. Les peines prévues vont d'un (1) à vingt (20) ans d'emprisonnement et de lourdes amendes jusqu'à cent (100) millions F CFA selon la gravité des faits. Outre les peines principales, les juridictions peuvent prononcer diverses sanctions complémentaires, telles que : la confiscation du matériel informatique ayant servi à commettre l'infraction ; la fermeture provisoire ou définitive de sites internet ou d'établissements ; l'interdiction d'exercer certaines activités professionnelles liées aux TIC ; la suspension ou l'interdiction d'accès à un service de communication au public en ligne ; la publication de la décision de condamnation. Ces mesures visent à prévenir la récidive et à neutraliser les moyens ayant servi à la commission de l'infraction.

3.1.4.2. Sanctions administratives et civiles

En complément des sanctions pénales, certaines autorités administratives peuvent infliger notamment des avertissements ou mises en demeure ; des sanctions administratives, notamment des amendes ; des retraits d'autorisation ou de licence. Par ailleurs, les victimes peuvent exercer une action civile afin d'obtenir réparation du préjudice subi, sous forme de dommages et intérêts. En cas de circonstances aggravantes (bande organisée, atteinte à la sécurité de l'État, préjudice grave causé à une victime ou à une institution), les peines sont alourdies.

3.2. Enjeux et limites de l'effectivité du cadre normatif ivoirien

La Côte d'Ivoire s'est dotée d'un cadre juridique structuré pour encadrer et réprimer la cybercriminalité. Toutefois, l'efficacité réelle de ce dispositif dépend non seulement de la qualité des textes adoptés, mais également de leur mise en œuvre concrète.

3.2.1 Enjeux de l'effectivité du cadre normatif ivoirien

Les enjeux se manifestent à plusieurs niveaux, notamment à travers la sécurisation de l'espace numérique, la protection des droits fondamentaux, le renforcement du caractère dissuasif et de la crédibilité de la justice pénale, ainsi que la consolidation de l'intégration régionale et internationale.

3.2.1.1 Sécurisation de l'espace numérique

Dans ce contexte, la protection des systèmes d'information, des données à caractère personnel et des transactions électroniques apparaît comme un défi majeur. La sécurisation de l'espace numérique ne se limite pas uniquement aux solutions logicielles ou au cadre juridique. Elle implique également la mise en place de dispositifs institutionnels et techniques, notamment des unités spécialisées chargées de veiller à la protection physique des infrastructures numériques, telles que les centres de données et les équipements stratégiques. Cette démarche vise à garantir plusieurs principes fondamentaux de la sécurité informatique. Il s'agit notamment de la confidentialité, qui consiste à empêcher l'accès aux données par des personnes non autorisées ; l'intégrité, qui assure que les informations ne sont ni modifiées ni détruites de manière illégitime ; la disponibilité, qui permet aux utilisateurs autorisés d'accéder aux systèmes et aux informations lorsque cela est nécessaire ; l'authentification, qui sert à vérifier l'identité des

utilisateurs ou des systèmes ; et enfin la traçabilité, qui permet de suivre et d'enregistrer les actions effectuées au sein d'un système. Ensemble, ces principes constituent le socle de la sécurité informatique. Grâce à ces mécanismes techniques et organisationnels, il devient possible de renforcer la protection du cyberespace et de passer progressivement d'une simple logique de sécurité informatique à une véritable dynamique de confiance numérique. Cependant, malgré ces dispositifs, plusieurs défis persistent. La fracture numérique, les risques technologiques et informationnels, ainsi que les déséquilibres en matière de cybersécurité favorisent l'extension de la cybercriminalité. Celle-ci tend à se développer au rythme de ces inégalités. Les cyberdélinquants qu'il s'agisse de hackers, de crackers, de script-kiddies, de cyberescrocs ou encore de cyberfraudeurs, disposent de compétences techniques avancées qu'ils exploitent pour attaquer les systèmes informatiques et commettre diverses infractions dans l'espace numérique. Dans un contexte marqué par la digitalisation croissante des activités économiques, administratives et sociales, la sécurisation de l'espace numérique est indispensable. Elle renforcerait la confiance dans les services numériques ; et encouragerait les utilisateurs, les entreprises et les institutions à recourir davantage aux technologies numériques, favorisant ainsi le développement de l'économie numérique et de la société de l'information.

3.2.1.2. Protection des droits fondamentaux

La lutte contre la cybercriminalité ne peut être efficace que si elle s'inscrit dans le respect des droits fondamentaux des individus. La mise en place de dispositifs de cybersécurité et de mécanismes de surveillance du cyberespace doit être conciliée avec la protection des libertés individuelles et des droits garantis par l'État de droit. Dans un environnement numérique où les informations personnelles circulent massivement, il est essentiel de veiller à ce que la collecte, le traitement et la conservation des données soient encadrés par des règles strictes afin d'éviter les abus, les atteintes à la vie privée ou l'exploitation illégale des informations. Elle doit garantir le respect des libertés individuelles, notamment la liberté d'expression et la liberté d'accès à l'information. Les mesures de contrôle ou de régulation du cyberespace ne doivent pas conduire à une restriction excessive de ces libertés, mais plutôt rechercher un équilibre entre la sécurité numérique et la protection des droits des utilisateurs. La protection des droits fondamentaux suppose le respect des garanties procédurales dans le cadre des enquêtes et des poursuites liées

aux infractions numériques. Les autorités compétentes doivent agir conformément aux principes de légalité, de proportionnalité et de transparence, tout en assurant aux personnes concernées le droit à un procès équitable et le respect de la présomption d'innocence. Dans le contexte ivoirien comme dans de nombreux États, l'encadrement juridique de la cybersécurité vise précisément à concilier la répression des actes de cybercriminalité avec la protection des droits fondamentaux des citoyens. Cette approche contribue à renforcer la confiance des utilisateurs dans l'environnement numérique tout en garantissant que la lutte contre les menaces informatiques ne porte pas atteinte aux principes essentiels de l'État de droit.

3.2.1.3. Renforcement du caractère dissuasif et de la crédibilité de la justice pénale

Un dispositif juridique réellement appliqué favorise la confiance des citoyens, des opérateurs économiques et des investisseurs dans l'environnement numérique. La répression de la cybercriminalité doit s'exercer dans le respect des libertés individuelles. Il s'agit de garantir un équilibre entre les impératifs sécuritaires et la protection de la vie privée, la liberté d'expression ainsi que les droits liés à un procès équitable. L'exécution effective des peines, qu'il s'agisse d'emprisonnement, d'amendes ou de sanctions complémentaires, renforce l'effet dissuasif du droit pénal et consolide l'autorité de l'État face aux infractions commises dans le cyberespace. L'effectivité du cadre normatif permet de respecter ses engagements internationaux et de s'inscrire activement dans les mécanismes de coopération judiciaire transfrontalière, indispensables à la lutte contre une criminalité numérique par nature globale. La crédibilité de la justice pénale renvoie à la confiance que les citoyens accordent à l'institution judiciaire dans sa capacité à prévenir, juger et sanctionner efficacement les infractions, y compris celles commises dans le cyberespace. Elle repose sur plusieurs éléments fondamentaux notamment l'application effective de la loi c'est-à-dire que les infractions doivent être poursuivies et sanctionnées conformément aux textes en vigueur, sans impunité ; la célérité des procédures consiste dans le traitement rapide des dossiers pénaux renforçant l'autorité de la justice et affermissant l'effet dissuasif des peines. La compétence technique des acteurs judiciaires notamment les magistrats, les enquêteurs et les experts doivent être avérés et maîtriser les spécificités des infractions numériques. L'équité et le respect des droits de la défense doit être plausible. Car, une justice crédible est une justice impartiale, respectueuse des garanties procédurales. La proportionnalité des sanctions suppose que les peines doivent être adaptées à la gravité des faits afin d'assurer à la fois dissuasion et justice. En matière de cybercriminalité,

la crédibilité de la justice pénale est particulièrement déterminante. Face à des infractions souvent complexes, transnationales et techniquement sophistiquées, la capacité de l'État à identifier les auteurs, à établir les preuves numériques et à prononcer des sanctions effectives conditionne la confiance des citoyens dans l'État de droit et la sécurité de l'espace numérique. Cet arsenal juridique exerce une pression permanente sur les cyberdélinquants, qui s'exposent à des sanctions souvent particulièrement lourdes. Toutefois, il convient de constater qu'il n'existe pas encore de politique publique et pénale véritablement globale, cohérente et pleinement structurée en matière de lutte contre la cybercriminalité. Certaines insuffisances du cadre législatif subsistent, tandis que les données statistiques permettant d'évaluer l'ampleur réelle du phénomène demeurent encore approximatives. Cette situation rend plus difficile l'élaboration et la mise en œuvre de stratégies efficaces et adaptées pour lutter contre les infractions commises dans le cyberespace.

3.2.1.4. Consolidation de l'intégration régionale et internationale.

La lutte contre la cybercriminalité dépasse largement le cadre national en raison de la dimension transfrontalière du cyberespace. Les infractions commises sur Internet peuvent être préparées dans un pays, exécutées dans un autre et produire leurs effets dans plusieurs États simultanément. Dans ce contexte, la Côte d'Ivoire s'inscrit dans une dynamique de coopération régionale et internationale visant à renforcer l'efficacité de la lutte. Au niveau régional, la Côte d'Ivoire participe activement aux initiatives portées par des organisations telles que la CEDEAO et l'Union africaine. Celles-ci encouragent l'harmonisation des législations relatives à la cybersécurité et à la cybercriminalité afin de faciliter la coopération judiciaire entre les États membres et à instaurer un cadre commun pour la prévention et la répression des infractions liées aux technologies de l'information et de la communication. La coopération internationale joue, par ailleurs, un rôle déterminant dans la lutte contre les cybermenaces. La Côte d'Ivoire collabore avec plusieurs organisations et partenaires internationaux afin de renforcer les capacités techniques, juridiques et institutionnelles des acteurs impliqués dans la cybersécurité. Cette coopération permet notamment l'échange d'informations, la formation des professionnels, le partage de bonnes pratiques ainsi que l'assistance dans les enquêtes liées à la cybercriminalité. De plus, l'intégration régionale et internationale favorise la coordination des actions entre les services de police et de gendarmeries, Europol, Interpol, les autorités judiciaires et les institutions spécialisées. Elle facilite également la mise en place de

mécanismes d'entraide judiciaire et d'extradition, indispensables pour poursuivre efficacement les cybercriminels qui opèrent souvent depuis l'étranger.

3.2.2. Limites de l'effectivité du cadre normatif ivoirien

Malgré les efforts réalisés par les autorités ivoiriennes pour mettre en place un cadre juridique destiné à encadrer le cyberespace et à lutter contre la cybercriminalité, l'effectivité de ce dispositif se heurte encore à plusieurs limites.

3.2.2.1 Insuffisances législatives

Tout d'abord, certaines insuffisances législatives persistent. Bien que plusieurs textes aient été adoptés afin de réguler l'usage des technologies de l'information et de la communication, certains aspects de la cybercriminalité évoluent plus rapidement que la législation. Cette situation crée parfois des lacunes juridiques ou des difficultés d'interprétation et d'application des normes existantes. La question de la déclaration des entreprises et de leur autorisation à effectuer des traitements conformément à la loi demeure peu claire, et sa mise en pratique fait l'objet de discussions récurrentes. Le contentieux relatif à la lutte contre la cybercriminalité reste encore limité, de sorte qu'il existe très peu de décisions de justice en la matière, ce qui explique que la jurisprudence demeure encore peu développée dans ce domaine. La montée en puissance de l'intelligence artificielle (IA) et des technologies de traitement des données soulève de nouveaux défis en matière de cybercriminalité et de digitalisation. L'utilisation de l'IA dans divers domaines, tels que les véhicules autonomes, les systèmes de recommandation ou encore les dispositifs médicaux intelligents, entraîne d'importantes implications juridiques à clarifier. Ces technologies présentent également des risques liés à leur utilisation malveillante, singulièrement à travers les attaques automatisées, la manipulation de l'information et les biais algorithmiques, ce qui soulève des interrogations quant à l'adéquation et à l'efficacité de la législation existante. La loi destinée à lutter contre la diffusion de fausses informations est souvent invoquées par les pouvoirs publics comme des instruments de préservation de l'ordre public. Toutefois, l'application soulève la question d'un équilibre délicat entre la protection de la sécurité nationale et la garantie de la liberté d'expression, droit fondamental consacré par le droit international des droits de l'homme et la constitution. Il n'existe pas de législation spécifique relative aux « fake news » ou à la désinformation permettant de distinguer clairement les fausses informations susceptibles de porter préjudice du discours public légitime. Cette

imprécision juridique peut ainsi ouvrir la voie à une utilisation abusive des textes existants, susceptible de restreindre l'exercice du droit à la liberté d'expression. La garantie d'un procès équitable et la possibilité pour les justiciables de faire valoir pleinement leurs droits dans le domaine du numérique demeurent encore en attente. Les avocats spécialisés en la matière sont encore peu nombreux, et les juridictions spécialisées et dédiées aux questions du numérique sont quasi inexistantes.

3.2.2.2 Insuffisances des moyens techniques et matériels

L'une des principales limites réside dans l'insuffisance des moyens techniques et matériels dont disposent les institutions chargées de la lutte contre la cybercriminalité. Les enquêtes en matière de cybercriminalité requièrent des outils technologiques sophistiqués ainsi que des infrastructures adaptées pour assurer la collecte, l'analyse et la conservation des preuves numériques. Toutefois, l'ANSSI, CFAD, CENTIF ne disposent pas encore de structures décentralisées dans les chefs-lieux de région, ce qui limite l'efficacité de son action sur l'ensemble du territoire. Les commissariats de police et les brigades de gendarmerie ne disposent, par ailleurs, pas de compétences techniques spécialisées nécessaires pour traiter efficacement les infractions liées aux technologies de l'information et de la communication et un déficit de connaissances de leurs officiers de police judiciaire dans la procédure pénale en matière de cybercriminalité. Le manque de formation spécialisée de certains acteurs du système judiciaire et des forces de l'ordre constitue également un obstacle à l'efficacité du cadre normatif. Les infractions liées aux technologies de l'information présentent une complexité technique qui exige des compétences spécifiques en matière d'investigation numérique, d'analyse informatique et de traitement des preuves électroniques. Une autre limite importante concerne la faible production de données statistiques fiables sur l'ampleur réelle de la cybercriminalité en Côte d'Ivoire. L'absence d'informations précises et systématisées rend difficile l'évaluation du phénomène et l'élaboration de politiques de sécurité publique adaptées pour y faire face. La persistance de la fracture numérique et le faible niveau de sensibilisation des utilisateurs contribuent, en outre, à fragiliser l'efficacité du dispositif juridique. Une grande partie de la population demeure insuffisamment informée des risques liés à l'usage d'Internet et des bonnes pratiques de sécurité numérique.

3.2.2.3 Dimension transnationale de la cybercriminalité

Elle signifie que les infractions commises dans le cyberespace dépassent les frontières nationales. En effet, les auteurs, les victimes, les serveurs et les infrastructures numériques peuvent être situés dans différents pays, ce qui rend la lutte contre ces infractions particulièrement complexe. Cette situation complique l'application du droit national, dans la mesure où les auteurs peuvent agir depuis l'étranger. Dès lors, la répression efficace de ces actes nécessite une coopération judiciaire et policière renforcée entre les États, afin de faciliter l'identification, la poursuite et la sanction des cyberdélinquants. Ainsi, même si le cadre normatif ivoirien constitue une avancée significative dans la régulation du cyberespace, son efficacité dépend largement du renforcement des capacités institutionnelles, techniques et humaines, ainsi que du développement d'une coopération plus étroite, tant au niveau national qu'international. Par ailleurs, la cybercriminalité s'inscrit dans un espace numérique mondial caractérisé par l'absence de frontières. Les cybercriminels peuvent ainsi mener leurs activités à partir d'un pays, utiliser un serveur situé dans un autre et cibler une victime dans un troisième. À titre d'exemple, un pirate informatique basé en Europe peut s'attaquer à une banque située en Afrique en passant par un serveur localisé en Asie. De plus, la rapidité et l'anonymat qu'offre Internet favorisent ces activités illicites. Les cybercriminels ont recours à des outils tels que les réseaux anonymes, les cryptomonnaies ou encore les VPN, ce qui rend leur identification et leur localisation particulièrement difficiles. En outre, les services numériques tels que le cloud, les réseaux sociaux ou les services de messagerie sont souvent hébergés dans plusieurs États, ce qui complique davantage les enquêtes et les procédures judiciaires. En définitive, la cybercriminalité n'est pas limitée par les frontières physiques, ce qui rend indispensable une coopération internationale renforcée et une harmonisation des législations afin de lutter efficacement contre ce phénomène à l'échelle mondiale.

IV DISCUSSION ET CONCLUSION

4.1 Discussion

Le présent travail analyse l'effectivité ainsi que les limites du cadre normatif ivoirien relatif à la répression de la cybercriminalité. Les recherches réalisées mettent en évidence, d'une part, les fondements juridiques qui structurent la lutte contre la cybercriminalité en Côte d'Ivoire et, d'autre part, les principaux enjeux ainsi que les limites qui entravent l'application effective de

ce dispositif. La répression de la cybercriminalité s'appuie sur un ensemble cohérent de textes nationaux, complétés par des engagements internationaux. Toutefois, l'efficacité de ce dispositif ne dépend pas uniquement de la qualité des normes adoptées, mais également de leur mise en œuvre concrète par les institutions compétentes. Bien que le cadre normatif ivoirien apparaisse relativement complet et globalement conforme aux standards internationaux, son efficacité demeure limitée en raison de difficultés pratiques d'application, d'une insuffisance des moyens institutionnels et des défis liés à la protection des droits fondamentaux dans l'espace numérique. À ce stade de la réflexion, Tano-Bian (2025) souligne que certaines infractions nécessitant des preuves électroniques peinent encore à aboutir à des sanctions judiciaires effectives. Néanmoins, des institutions spécialisées, telles que la Plateforme de Lutte contre la Cybercriminalité en Côte d'Ivoire ou les brigades de lutte contre la cybercriminalité au Sénégal, contribuent à la protection des droits des populations face aux violations liées au numérique. Les lois nationales relatives à la protection des données à caractère personnel, aux transactions électroniques et à la régulation des communications électroniques, par ailleurs, constituent des garanties essentielles pour la protection des droits des individus, à travers l'exigence du consentement (Tano-Bian, 2025). Selon Ghita et Chadi (2023), ces instruments juridiques fournissent le socle normatif de la lutte contre la cybercriminalité en définissant les infractions et les sanctions applicables, tout en établissant des principes de protection des données et des mécanismes de sanction en cas de non-respect. Toutefois, Londa (2024) relève que certaines lois visant à faciliter l'accès des citoyens aux informations détenues par les organismes publics présentent encore certaines limites. Le droit à l'information, qui fait partie intégrante de la liberté d'expression consacrée par la constitution, garantit l'accès aux informations d'intérêt public provenant de diverses sources et confère également aux lanceurs d'alerte la possibilité de divulguer des informations d'importance publique (Ghita & Chadi, 2023). La constitution encadre, en outre, strictement l'enregistrement et le traitement des informations permettant d'identifier les individus et protège les droits des consommateurs dans les transactions commerciales, y compris celles réalisées en ligne. Elle garantit également plusieurs droits numériques fondamentaux, tels que le droit à la vie privée, la liberté d'expression et le droit à un procès équitable. Au niveau international, Ghita et Chadi (2023) soulignent que la coopération et la réglementation internationale constituent des éléments essentiels pour lutter efficacement contre la cybercriminalité, en raison de son caractère transnational. Cependant, Veh (2019) met en évidence l'insuffisance des structures techniques de lutte, notamment des

laboratoires de criminalistique numérique, qui jouent un rôle déterminant dans les enquêtes en matière de criminalité informatique grâce à des équipements spécialisés permettant l'extraction, l'analyse et la préservation des preuves numériques. Au niveau national, ces structures demeurent limitées et fortement concentrées dans la capitale économique, ce qui constitue un obstacle pour une lutte efficace sur l'ensemble du territoire. En outre, bien que les règles de procédure pénale aient introduit des mécanismes adaptés à la spécificité des infractions numériques, tels que la conservation rapide des données informatisées ou l'interception de données informatiques (Cissé, 2011), plusieurs difficultés persistent. Veh (2017) souligne notamment les problèmes liés aux délais de conservation et de prescription des données, d'autant plus que celles-ci sont souvent stockées à l'étranger. Leur accès dans le cadre des enquêtes judiciaires se heurte ainsi à des obstacles juridiques et techniques, aggravés par les dissemblances entre les législations nationales. Enfin, la dimension transnationale de la cybercriminalité engendre de nombreux défis juridiques, notamment les conflits de juridiction pour déterminer l'État compétent, les différences entre les systèmes juridiques nationaux et les difficultés liées à l'extradition lorsque les auteurs des infractions se trouvent à l'étranger.

4.2 Conclusion

L'encadrement normatif de la répression de la cybercriminalité en Côte d'Ivoire traduit la volonté des pouvoirs publics d'adapter le droit aux mutations engendrées par les technologies de l'information et de la communication. À travers l'adoption de textes spécifiques et la mise en place d'institutions compétentes, le législateur ivoirien a cherché à doter le pays d'un dispositif juridique apte à prévenir, détecter et sanctionner les infractions commises dans le cyberespace. Cependant, malgré ces avancées, certains défis persistent, notamment en raison du caractère transnational de la cybercriminalité, des difficultés liées à la collecte des preuves numériques, à la protection des droits fondamentaux et numériques et des divergences entre les législations nationales. Ces contraintes soulignent la nécessité de renforcer la coopération internationale, d'adapter continuellement les normes juridiques et de développer les capacités techniques et institutionnelles des acteurs chargés de la lutte contre la cybercriminalité. Ainsi, l'efficacité de la répression de la cybercriminalité en Côte d'Ivoire dépendra non seulement de la consolidation de son cadre normatif, mais également de l'amélioration de la coopération judiciaire, de la formation des professionnels du droit, des officiers de police judiciaire et renforcement permanent des capacités techniques des spécialistes, des experts et surtout de la

sensibilisation des usagers des technologies numériques. La transformation numérique exige une adaptation constante du cadre normatif afin de préserver les droits numériques, tout en favorisant l'innovation et en garantissant la sécurité dans le cyberespace.

Références bibliographiques

Acte additionnel relatif à la protection des données à caractère personnel dans l'espace CEDEAO adopté à Abuja le 16 février 2010.

Agence National de la Sécurité des Systèmes d'Information. (2024). Rapport sur l'état de la cybercriminalité en Côte d'Ivoire.

Agence National de la Sécurité des Systèmes d'Information. (2023). Rapport sur l'état de la cybercriminalité en Côte d'Ivoire.

Autorité de régulation des Télécommunications/TIC de Côte d'Ivoire (2024). L'état de la cybersécurité en Côte d'Ivoire

Agnidé K. & ALI G. Y. (2023). Cybercriminalité et cybersécurité en Afrique : pourquoi articuler l'action techno-juridique et la responsabilité collective ? Revue des humaines et sociales, Lettre, Langue et Civilisation. ISSN (E) 2958-2814 (P) 3006-306X Numéro 007, Juin 2024. Université Alassane Ouattara. UFR Communication Milieu et Société.

Biosha M. J-M. (2025) Décryptage des menaces sécuritaires à l'ère de la cybercriminalité en Afrique post guerre-froide. MES-RIDS, nO139, vol. 1., Mars – Avril.

Cissé, A. (2011). Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorités de recherche. Centre de recherche pour le développement international.

Convention de Budapest du 23 novembre 2001.

Convention de Malabo du 27 juin 2014.

Décret n° 2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie.

Décret n° 2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique.

Décret n° 2015-78 du 4 février 2015 portant gestion du domaine internet de premier niveau de la Côte d'Ivoire «.ci »

Décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique.

Décret n°2017-193 du 22 mars 2017 portant identification des abonnés des services de télécommunications/TIC ouverts au public et des utilisateurs des cybercafés.

Décret n° 2020-128 du 29 Janvier 2020 portant création, organisation et fonctionne ment du centre de veille et de réponse aux incidents de sécurité informatique (CI-CERT).

Décret n° 2021-911 du 22 décembre 2021 portant adoption du cadre commun d'architecture de référentiel de données. Décret n° 2021-912 du 22 décembre 2021 portant adoption du Cadre Commun d'Urbanisation des Systèmes d'Information de l'État.

Décret n° 2021-913 du 22 décembre 2021 portant adoption du Référentiel Général d'Interopérabilité des Systèmes d'Information. Décret n° 2021-914 du 22 décembre 2021 fixant les règles pour la conception, la réalisation et la gouvernance des projets publics d'infrastructures, d'équipements et de plateformes de services numériques.

Décret n°2021-918 du 22 décembre 2021 instituant un département en charge des systèmes d'information au sein des ministères.

Directive portant lutte contre la cybercriminalité dans l'espace CEDEAO adoptée les 17 et 19 août 2011 à Abuja.

Foucault M. (1975). Surveiller et punir : Naissance de la prison. Les éditions Gallimard

Ghita B. & M. Chadi (2023). La Cybercriminalité dans l'ère numérique : Une étude des défis juridiques et réglementaires. International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 68 No. 1 Aug. 2023, pp. 40-49.
Hans K. (1934). Qu'est-ce que la théorie pure du droit ? Droit et Société. Année 1992 22 pp. 551-568. https://www.persee.fr/doc/dreso_0769-3362_1992_num_22_1_1187. Consulté le 20/01/2026.

Interpol**.** (2015). Soutien aux enquêtes sur la criminalité numérique. Centre de Lutte contre la Criminalité Numérique.

Koffi H. B. I. (2022). Révolution numérique et lutte contre la cybercriminalité en Côte d'Ivoire, revue Échanges, n° 18, juin 2022.

Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, modifiée en ses articles 17, 33, 58, 60, 62 et 66 par la loi n°2023-593 du 07 juin 2023.

Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques.

Londa. (2024). Rapport sur les droits numériques et l'inclusion en Afrique. Copyright © 2024 Paradigm Initiative. 374 Borno Way, Yaba, Lagos, Nigeria Email : media@paradigmhq.org www.paradigmhq.org.

Okou D. E. & Dagbé A, S. (2025). Cybercriminalité en Côte-d'Ivoire : logiques et stratégies des acteurs. Revue Enclume d'Ivoire, Vol 2 N°5 Octobre 2025.

Ordonnance n°2024-950 du 30 octobre 2024 portant modification des articles 3 et 17 de l'ordonnance n°2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives et abrogation de l'article 50 de loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques.

Ordonnance n° 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Plateforme de Lutte contre la Cybercriminalité. (2015). Rapport d'activité.

Plateforme de Lutte contre la Cybercriminalité. (2023). Rapport d'activité.

Rabault H. (2018). La théorie du droit fonctionnaliste de Niklas Luhmann. CAIRN.INFO DROIT & ADMINISTRATION. Date de mise en ligne : 08/10/2019 https://doi.org/10.3917/droit.068.0201, consulté le 20/01/2026.

Tano-Bian J-A., (2025). Les garanties des droits humains à l'ère du numérique en Afrique. Dans Revue juridique et politique en Afrique 2025/2 N° 5, pages 89 à 119 Éditions Centre d'études, de recherche et de prospective en Afrique.

Tano-Bian J-A., (2015). La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'Ouest. Droit. Thèse de Doctorat, Université Sorbonne Paris Cité, Français. ffNNT : 2015USPCB067ff. fftel-01249586f.

Veh G. A. L. (2017). La fraude sur le porte-monnaie électronique en Côte d'Ivoire. Revue Africaine de Criminologie. N° 21 décembre 2017 ISSN 1819-0650.

Veh G. A. L. (2019). La cyberescroquerie à Abidjan. Thèse unique en Criminologie-Non publiée. Abidjan : Université Félix Houphouët-Boigny.

Veh G. A. L. (2025). Rôle causal des victimes dans l'escroquerie sur internet en Côte d'Ivoire. Revue africaine de Criminologie N° 37 Décembre 2025.