M.E.S., Numéro 143, Septembre – Octobre 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, septembre - octobre 2025

DE LA CYBERCRIMINALITE A L'ERE DE L'INTELLIGENCE ARTIFICIELLE MILITAIRE : PERSPECTIVES DE CYBERSECURITE EN DROIT PENAL CONGOLAIS

par

Exaucée TUZOLANA MUKEDIKA

Apprenant au 3ème cycle, Faculté de Droit,
Département de Droit Pénal et Criminologie
Université de Kinshasa

Résumé

Le Droit pénal congolais fait face à des défis majeurs dans la croissance exponentielle de l'Intelligence Artificielle. A mesure que ces technologies se développent, il est crucial que le cadre juridique évolue pour intégrer des régulations qui protègent les droits fondamentaux des citoyens. En effet, l'enjeu consiste à trouver un équilibre entre la protection de ces droits et la Sûreté de l'Etat.

L'utilisation de l'Intelligence Artificielle à usage militaire et de sécurité soulève des questions essentielles sur la sécurité nationale et les relations internationales. Le Droit congolais doit tenir compte des dimensions régionales et internationales dans un climat rude de géopolitique en s'assurant que les pratiques qu'impose cet nouvel outil respectent les normes des droits de l'homme. La République Démocratique du Congo est appelée à mettre en place des mécanismes juridiques adaptés, non seulement à des fins de protection au niveau interne, mais également de contribution à la stabilité internationale tout en promouvant une coopération favorable au maintien de la paix et de la sécurité internationales.

Mots clés : *Intelligence Artificielle, droit pénal congolais, protection, droits fondamentaux, sûreté de l'etat, usage militaire et de sécurité, géopolitique, coopération internationale, stabilité internationale, paix et sécurité internationales.*

Abstract

Congolese criminal law faces major challenges in the exponential growth og artificial intelligence. As these technologies develop, it is crucial that the legal framework evolves to incorporate regulations that protect citizens' fundamental rights. Indeed, the challenge is to find a balance between the protection of these rights and state security.

The use of Artificial Intelligence for military and security purposes raises essential questions about national security and international relations. Congolese law must take into account regional and international dimensions in a harsh geopolitical climate by ensuring that the practices imposed by this new tool respect human rights standards. The Democratic Republic of Congo is called upon to put in place appropriate legal mechanisms not only for internal protection purposes, but also to contribute to international stability while promoting cooperation favorable to the maintenance of international peace and security.

Keywords : *Artificial intelligence, congolese criminal law, protection, fundamental rights, state security, military and security use, geopolitics, international cooperation, international stability, international peace and security.*

INTRODUCTION

L'Internet a été conçu et construit sur un réseau technique : le web. Il a engendré un espace : le numérique. Sur ce nouvel espace, des entreprises ont développé des services, des prestations et des biens, tandis que les personnes y ont trouvé des moyens d'expression nouveaux et profitent des richesses nouvelles. Cela a engendré une économie que certains appellent une « nouvelle économie », tandis que d'autres, allant plus loin, y voient une ère[1]. C'est parallèlement un terrain propice sur lequel les génies du mal vont multiplier leurs tentacules maléfiques à des fins de déstabilisation, à tous les niveaux, des intérêts des personnes tant physiques que morales, jusqu'aux Etats, provoquant notamment des propagandes, des escalades, de la piraterie et de la fuite de données. En effet, au regard de l'ampleur que prennent les nouvelles technologies dans les secteurs militaire et/ou sécuritaire, d'énormes bouleversements sont en gestation notamment, en premier temps, des armes stratégiques, en particulier, dans les domaines d'alerte précoce, de la défense antimissile et de la dissuasion nucléaire ne sont qu'une partie du pouvoir de l'Intelligence Artificielle (dite IA) si bien qu'elle peut trouver des applications dans les systèmes d'information et de commandement stratégique, les systèmes de communication, de navigation, de renseignement et de surveillance ainsi que dans tous les domaines des capacités défensives et offensives dans le cyber espace, dont elle[2] pourrait améliorer l'efficacité[3].

Faute de comprendre ces évolutions, l'Etat laisse la technologie et ses penseurs structurer la société. Insensiblement, le centre de gravité du pouvoir se déplace, puisque la technologie est plus forte que la loi. Il

[1] M.-A. FRISON-ROCHE, « *Internet et espace d'interrégulation* », coll. The Journal of the Regulation, Dalloz, Paris, 2016, p. VII.

[2] Elle est née de l'informatique qui lui fournit les bases techniques qui permettent son développement, tandis que le numérique enveloppe et diffuse ces technologies à l'échelle mondiale.

[3] GROUPE DE TRAVAIL DE LA FONDATION FRIEDRICH-EBERT, « *Les nouvelles technologies militaires et les systèmes d'armes autonomes, L'avenir de la guerre* », in politique de sécurité internationale, Bureau de Paris, novembre 2015, p. 4.

est extrêmement urgent de rénover le pilotage démocratique, de plus en plus prisonnier de la tyrannie du court terme, qui se révèle incapable de penser la révolution NBIC. A cette allure, les pas se pressent pour un oligopole d'une dizaine de sociétés américaines et chinoises contrôlant l'IA, grâce à la maîtrise simultanée de bases de données géantes et de microprocesseurs propriétaires difficilement accessibles aux autres sociétés. C'est l'une des raisons pour laquelle l'Etat devrait se donner les moyens pour des IA qui battent du revers de la main les records dans la détection des dangers notamment dans le domaine de la sécurité. Pour Olivier Sichel[4], l'appétit de pouvoir de certains hommes politiques les poussera à domestiquer l'IA qui est un levier de puissance et la remettre sous le contrôle de l'Etat. Désormais, les gens capables de penser le futur sont en dehors de l'appareil de l'Etat. C'est dramatique, car la science-fiction et les transhumanistes de la *Silicon Valley* ne peuvent rester seuls à imaginer notre futur. La désynchronisation entre nos démocraties et la technologie est devenue mortifère. Si nous voulons résister à la vague des régimes autoritaires et trouver un équilibre harmonieux avec les géants du numérique, il faut réinventer la technologie politique[5]. Il faut maîtriser l'IA, et trouver une sorte de *modus vivendi* avec un voisin envahissant dont on ne sait presque rien puisqu'il devient une boîte noire[6].

Par ailleurs, si certains[7] se positionnent seulement en faveur de l'essor de ces technologies en raison de leurs avantages sur les plans techniques, scientifiques ou économiques ; d'autres[8] se sont fortement opposés à leur propagation en soulevant le spectre d'impacts négatifs particulièrement néfastes pour l'environnement ou la santé humaine. Et, dans la foulée de la réflexion entreprise sur la manière de prendre en compte les différents impacts soulevés par les technologies de rupture, la communauté juridique s'est aussi penchée sur la relation entre l'encadrement normatif que fournissent le Droit et le développement technologique[9]. C'est en ce sens que Sonia Desmoulin-Canselier souligne que les juristes ne sont pas restés indifférents devant les transformations qu'induisent les innovations technoscientifiques pour les institutions juridiques et démocratiques[10]. Pour Clément Durez, les mondes virtuels sociaux représentent un formidable terrain de réflexion pour les juristes[11]. Par conséquent, le législateur congolais est appelé à surgir sur cette scène qui sort

---

[4] Président du think tank, Digital New Deal Foundation cité par L. ALEXANDRE, op.cit. p. 71. Sa réflexion est liée sur la construction d'une IA de confiance, souveraine et respectueuse des valeurs. Dans le magazineCDscope du groupe Caisse des Dépôts (numéro 416, mars-avril 2025), O. SICHEL, directeur général par intérim de la Caisse des Dépôts, évoque les enjeux de souveraineté et de contrôle autour de l'IA. Il insiste sur notamment sur la nécessité de protéger les données, de créer une IA au service de l'intérêt général et de la compétitivité et sur les craintes que l'IA puisse être confisquée par quelques acteurs ou pays. Il souligne aussi le rôle que l'Etat peut devoir jouer pour maitriser les risques et développer des modèles souverains d'IA. Cette perspective peut s'interpréter comme une mise en garde contre un possible appétit de pouvoir politique visant à domestiquer l'IA, pour la contrôler en tant que levier de puissance. Cette édition du magazine CDscope présente en détail cette vision et les enjeux associés à l'IA souveraine et de confiance portée O. SICHEL et la Caisse des Dépôts. (O. SICHEL, « *Pour une IA au service de l'intérêt général* », in CDSCOPE, Caisse des Dépôts, n°416, mars-avril 2025., disponible sur https://www.caissedesdepots.fr/sites/default/files/2025-03/CDscope_416.pdf?utm).

[5] L. ALEXANDRE, op.cit., p.72.

[6] Idem, p.73.

[7] Il s'agit des chercheurs en IA (universitaires, scientifiques), des experts en économie et politiques publiques, des spécialistes industriels et technologiques, des cadres et dirigeants d'entreprises innovantes ; des membres de conseils consultatifs gouvernementaux. Tous mettent en avant les bénéfices liés à la productivité, à l'innovation scientifique, à l'amélioration des processus industriels et à la croissance économique permise par l'IA. (GOUVERNEMENT DU CANADA, « *Ecosystème de l'intelligence artificielle* », in Innovation, Sciences et Développement économique Canada, le 23 mai 2025 (date de modification de l'article)., disponible sur https://ised-isde.canada.ca/site/isde/fr/ecosysteme-lintelligence-artificielle ; BESSON, DOZIAS, FAIVRE et al., « *Les enjeux économiques de l'intelligence artificielle* », in Trésor-Eco, France, publié le 02 avril 2024., disponible sur https://www.tresor.economie.gouv.fr/Articles/2024/04/02/les-enjeux-economiques-de-l-intelligence-artificielle?utm ; AXIOCODE, « *Avantages et inconvénients de l'intelligence artificielle* », publié le 03/07/2019 (modifié le 27/03/ 2025)., disponible sur https://www.axiocode.com/avantages-inconvénients-intelligence-artificielle/).

[8] Il s'agit de T.CADART, président de la Commission IA du CESE (France), des experts et chercheurs de Santé publique France en santé environnementale, des spécialistes en écologie industrielle et éthique des technologies, des chercheur en santé publique spécialisés en impacts environnementaux et experts en robotique médicale. (SANTELOG, « *Intelligence artificielle : l'équilibre nécessaire entre technologie et écologie* », publié le 16/09/2024., disponible sur https://www.santelog.com/actualites/intelligence-artificielle-lequilibre-necessaire-entre-technologie-et-ecologie ; SANTE PUBLIQUE FRANCE, « *L'IA ; synthèse des connaissances et perspectives pour la santé environnementale à santé publique France* », in Santé environnement, juillet 2024., disponible sur https://www.santepubliquefrance.fr/content/download/641355/document_file/748332_spf00005416.pdf?version=1 ; CONSEIL ECONOMIQUE SOCIA ET ENVIRONNEMENTAL (cese), « *Pour une intelligence artificielle au service de l'intérêt général* », in Journal officiel de la République Française, avis, NOR : CESL 1100002X, séance du 14 janvier 2025., disponible sur https://www.lecese.fr/sites/default/files/pdf/Avis/2025/2025_02_IA.pdf?utm).

[9] C.-E. DANIEL, *Les robots et l'Empire du Droit. Forces et limites de la gouvernance par le Droit pour l'encadrement normatif du développement de la robotique interactive*, Thèse de doctorat, Faculté de Droit, Université de SHERBROOKE, Québec, Canada, 2022, pp. 1-2.

[10] S. DESMOULIN-CANSELIER, « *What Exactly Is It All About ? Puzzled Comments from a French Legal Scholar on the NBIC Convergence* », *NanoEthics*, 2012, p. 243, cité par C.-E. DANIEL, idem.

[11] C. DUREZ, « *Mondes virtuels, Droit et jeu* », in Le Droit dans les mondes virtuels, sous la direction de Gérard DELABRE, CRIDS, Bruxelles, Belgique, 2013, p. 9.

tout droit de science-fiction, aux allures d'hécatombes, pour une protection aussi bien des civils, des systèmes d'IA que de la Sûreté de l'Etat[12]. Sur ce, l'on se rend compte qu'aucune recherche portant sur la répression d'une infraction ne peut être menée sans l'étudier dans le Droit pénal, à l'instar de la présente qui analyse les solutions pénales au regard des atteintes commises par et contre l'IA. A ce sujet, l'on peut comprendre le Professeur Nyabirungu mwene Songa lorsqu'il soutient que : « *Partout et dans tous les secteurs où se développe l'activité humaine, le Droit pénal est appelé à intervenir…* ». Ainsi, dans cette quête, il ressort que ce législateur n'a toujours pas ignoré l'évolution des nouvelles technologies. Il a, par ailleurs, pourvu des solutions pénales aux problèmes de cybercriminalité[13]; si bien qu'il a effleuré ou posé des germes[14] des notions faisant appel à l'IA perçue comme la *quatrième révolution industrielle*[15]. Les activités criminelles facilitées par le TIC avec la sophistication qu'accompagne l'IA, deviennent des fléaux modernes capables d'ébranler la sécurité nationale, une atteinte contre les systèmes d'IA peut avoir pour but notamment de modifier les données et/ou des instructions de sorte, pour une arme, de cibler la population civile, par conséquent de commettre des infractions, susciter des tensions entre peuples, des conflits, voir des guerres. Par ailleurs, la problématique de l'utilisation d'armes autonomes considérées comme la *troisième révolution dans la conduite de la guerre*, après la poudre à canon et les armes nucléaires[16], fera l'objet du prochain article, constituent, aujourd'hui, à côté de celles de la responsabilité pénale, des conditions d'exercice au droit à la légitime défense, la preuve et la (les) juridiction (s) compétente (s), des questions fondamentales de société, desquelles dépendent la survie de l'humanité.

Le mépris méthodologique pour les connaissances approximatives est le début de la « *barbarie scientifique contemporaine* »[17]. D'où la nécessité impérieuse de la méthodologie dans la présente étude. En effet, la méthode est un moyen et non une fin ; c'est un instrument devant permettre à l'esprit de s'épanouir, à la réflexion de s'élargir, à l'expression de s'éclairer[18]. Car, d'après Kaplan[19], « *le propre de la méthode est d'aider à comprendre le sens le plus large, non le résultat de la recherche scientifique mais aussi le processus lui-même car tout travail scientifique consiste en une méthodologie afin d'aboutir à une solution* ». Madeleine Grawitz considère que, dans son sens général ou philosophique, la méthode est constituée par l'ensemble d'opérations intellectuelles par lesquelles une discipline cherche à attendre les vérités qu'elle poursuit, les démontre et les vérifie[20]. Toutefois, on le sait, chaque discipline à ses impératifs méthodologiques ; le Droit pénal, qui est principalement abordé ici, étant avant tout une discipline juridique, le juriste pénaliste est donc naturellement censé privilégier la méthode juridique (i). Mais tout au long de la présente recherche scientifique, il sera également fait recours aux méthodes comparative (ii) et sociologique (iii).

i. Méthode juridique

La méthode juridique est celle par laquelle on recourt à un raisonnement objectif et obéit à un système rationnel et logique, elle procède de l'exégèse des textes, de la Constitution et de toutes les autres lois sans la plupart du temps tenir compte des réalités sociologiques sous-jacentes et souvent contraires aux textes[21]. Elle consiste à analyser et à exposer le Droit positif, mais aussi à confronter le fait et le Droit. Elle connaît des « *modalités qui sont les raisonnements de base susceptibles de résoudre juridiquement la question du sens du texte, c'est-*

[12] On est en sûreté lorsque toutes les dispositions sont prises pour qu'aucune infraction ne soit commise. L'Etat, depuis toujours, fait face à deux types de menaces, dont les menaces offensives menées de l'extérieur par des étrangers et celles des insurrections perpétrées de l'intérieur par des nationaux. D'où la « sûreté extérieure » et de « sûreté intérieure ». Jean-Paul DOUCET observe que « la distinction est trop schématique : des menées subversives sont parfois l'œuvre des nationaux stipendiés par l'étranger ; elle n'a été hissé au rang de principe par Lénine et Trotski ». Il conclut que c'est pourquoi « le Nouveau Code pénal français l'a abandonnée et parle de protection des intérêts fondamentaux de la Nation » (J.-P. DOUCET, « *Dictionnaire de droit criminel* », V° Sûreté de l'Etat. https://ledroitcriminel.free.fr/dictionnaire.htm cité par R. de B. MANASI N'KUSU-KALEBA, *Droit pénal spécial. Infractions choisies*, Editions Droit et Société, D.E.S., Kinshasa, Octobre 2023, p. 681.). La perception de A. VITU depuis 1960 rappelle que les prémices de la compréhension de la sûreté de l'Etat était liée aux aspects politiques, diplomatiques et militaires, de sorte que les autres aspects soient mis dans la catégorie secondaire. Alors que l'indépendance, la puissance et la grandeur de l'Etat peuvent être attaquées sur le plan économique, commercial, industriel, scientifique ou financier, notamment par la voie de l'espionnage industriel et économique. Il ne faut donc pas, pour le législateur, ignorer l'importance de ces données nouvelles. (A. VITU, *Commentaire du Juris-classeur*, cité par J.-P. DOUCET, V° Trahison, idem.).

[13] Atteintes aux données du système ou au système lui-même, en passant par les infractions de droit commun facilitées par les technologies de l'information et de la communication.

[14] Notamment l'article 2, point 1 de la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

[15] K. SCHWAB, *La quatrième révolution industrielle*, Dunod, Malakoff, 2017, p. 11.

[16] GROUPE DE TRAVAIL DE LA FONDATION FRIEDRICH-EBERT, « *Les nouvelles technologies militaires et les systèmes d'armes autonomes, L'avenir de la guerre* », op.cit., p. 4.

[17] M. VILLEY, *Leçon d'histoire de la philosophie du Droit*, Dalloz, Paris, 1963, pp. 21-22.

[18] M. A. COHENDET, *Droit public. Méthodes de travail*, 3e édition, Montchrestien, Paris, 1998, p. 12.

[19] Cité par M. GRAWITZ, *Méthodes des sciences sociales*, 11e édition, Dalloz, Paris, 2001, p. 15.

[20] Idem, p. 301.

[21] B. CHANTBOUT, *Droit constitutionnel et science politique*, 8e éd., Paris, 1968, p. 55.

à-dire son interprétation »[22]. Ainsi, sera-t-elle d'un apport important dans l'étude des règles juridiques qui fondent la matrice du Droit pénal du numérique, dans son aspect de l'intelligence artificielle. Toutefois, il sied de relever que le Droit posé applicable au cas d'espèce, la théorie de l'interprétation est complexe et fait intervenir plusieurs considérations, notamment l'exégétique. Cette dernière, en effet, que beaucoup de chercheurs réduisent à l'unique méthode juridique - consistant à faire une interprétation presque littérale ou simplement grammaticale de la règle consiste à analyser les textes législatifs et réglementaires, pour y chercher le véritable esprit de leurs auteurs et ce, en vue d'en cerner l'étendue et les limites qu'ils fixent à leur application[23].

ii. Méthode comparative

La méthode comparative est définie par Reuchelin comme « *la démarche cognitive par laquelle on s'efforce à comprendre un phénomène par la confrontation des situations différentes* »[24]. La comparaison, note avec raison Francis Delperee, est intéressante puisqu'elle permet de voir évoluer dans deux contextes institutionnels, économiques et sociaux différents des institutions qui, au point de départ en tout cas, ont été construites sur le même modèle[25]. La présente étude aborde essentiellement le Droit congolais, quand bien même il sera souvent fait appel aux Droits étrangers (français et belge notamment qui en constituent les sources premières d'inspiration) en parfaite évolution sur le Droit pénal de l'IA. Ainsi, cette méthode permettra-t-elle de déceler les caractéristiques et les particularités, les forces et les faiblesses du Droit pénal congolais à l'ère de l'intelligence artificielle ; puis, de lui proposer, à partir de l'expérience des Droits précités, des pistes des solutions.

iii. Méthode sociologique

La méthode sociologique procède par l'hypothèse approfondie des réalités sociales dans un milieu donné ; elles sont à la fois tributaires des faits et se préoccupent moins de les apprécier que de les expliquer[26]. Cette approche permettra donc de situer la problématique de l'étude, à savoir les défis du Droit pénal congolais à l'ère de l'intelligence artificielle. En effet, comme on peut le constater dans la présente étude, le fossé existant entre la réalité et les textes dans leur application nous téléporte toujours en dehors du Droit pour y trouver des justifications. D'où, le recours dans le cadre ce travail, à la méthode sociologique qui permet d'asseoir une approche holistique sur les questions du Droit pénal dans son interaction d'avec les défis posés par la cybercriminalité à l'ère de l'intelligence artificielle militaire pour des solutions en cybersécurité.

La présente étude s'étable sur deux points, à savoir : du diagnostic des défis lies à la cybercriminalité a l'ère de l'intelligence artificielle militaire ; de la nécessite d'adaptation du droit pénal congolais pour une cybersécurité efficace.

I. DU DIAGNOSTIC DES DEFIS LIES A LA CYBERCRIMINATE A L'ERE DE L'INTELLIGENCE ARTIFICIELLE MILITAIRE

Certains se dirigent vers une définition fonctionnelle de la cybercriminalité, à l'occurrence Romain Ciswicki[27] qui affirme que le terme « *cyber* » renvoie aux nouvelles technologies du numérique, et en particulier l'Internet. La *criminalité,* poursuit-il, est une traduction littérale de l'anglais *criminality,* qui concerne le Droit pénal ou *criminal law* –plutôt que la notion française de criminalité ou de criminologie. Ainsi, argue-t-il qu'il serait plus juste de parler de « *cyberdéliquance* » ou de « *cyberinfraction* », même si le terme couvre bien l'ensemble de comportements prohibés. Il est dès lors possible de considérer que la cybercriminalité concerne l'ensemble d'actes en lien avec les nouvelles technologies, en particulier de l'information et de la communication dont Internet, et prohibés par le Droit pénal. C'est d'ailleurs la définition générale retenue par le gouvernement français : « *toutes les informations tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* »[28]. La cybercriminalité recouvre l'ensemble de

[22] D. MBAU SUKISA, *Contribution à la construction d'un cadre de protection pénale de la Constitution en RDC : Etude Positive et prospective*, Thèse de doctorat, Faculté de Droit, Université de Kinshasa, 2020, p. 27.

[23] A. - J. ARNAUD, *Dictionnaire encyclopédique de théorie et de sociologie du Droit*, cité par J. DJOLI ESENGELI, *Le constitutionnalisme africain entre la gestion des héritages et invention du futur ; L'exemple Congolais*, Thèse de doctorat d'Etat en Droit public, Université de Paris 1 Sorbonne, 2003, p. 25.

[24] M. REUCHLIN, *Les Méthodes en psychologie*, 3e édition, P.U.F., Paris, 1973, p. 25.

[25] Lire dans ce sens, A. KAMUKUNY MUKINAY, *Contribution à l'étude de la fraude en Droit constitutionnel congolais*, Thèse de doctorat en Droit public, Faculté de Droit, Université de Kinshasa, 2007, p. 40.

[26] G. GUIRVITCH, *La vocation actuelle de la sociologie*, Tome I, 3e édition, P.U.F., Paris, 1963, p. 6.

[27] R. CISWICKI, « *La définition fonctionnelle de la notion de cybercriminalité* », in memannuaire sécurité défense, Université de Grenoble-Alpes, 2019, p. 267.

[28] Protéger les internautes, *Rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité*, février 2014, p. 12. Cité par R. CISWICKI, op.cit.

crimes[29] commis à l'encontre ou par le biais des systèmes d'information[30]. Ces infractions renvoient à une large diversité de phénomènes criminels qui vont des escroqueries au harcèlement, en passant par les rançongiciels[31], la compromission d'identifiants, ou encore l'usurpation d'identité[32]. L'IA est utilisée bien de fois à des fins criminelles. Sa définition légale[33] est : « *notion large qui regroupe toutes les infractions commises sur ou au moyen d'un système informatique généralement connecté à un réseau* ». Il faut admettre que les enjeux desquels dépendent les prouesses de l'IA militaire et ceux provoquées par celle-ci, sortent des notions de cybercriminalité classique. En effet, cette dernière diffère de la cybercriminalité inhérente à l'IA militaire ou à usage militaire et de sécurité[34]. En somme, celle-ci rend les menaces plus complexes, ciblées et stratégiques dans le domaine militaire et de sécurité nationale, ce qui représente une évolution et une sophistication indéniables. Il se crée dans cette nouvelle ère, un nouveau mal qui vient, non seulement perturber l'ordre public, mais aussi et surtout le ravager de par la gravité des faits et des conséquences qui en découlent. En termes de défis pénaux, sans que nul n'en disconvienne, la nature anonyme et décentralisée des cyberattaques élague l'aisance dans l'établissement de la responsabilité pénale en ce qu'elle nécessite des prérequis si bien qu'appel peut être fait aux experts patentés, des enquêtes menées par des autorités régulièrement formées en la matière. Il est également fait mention d'une absence de législation congolaise qui consacre l'intelligence artificielle concrètement, pose des règles et obligations, met en lumière des comportements prohibés qui se font suivre des sanctions exemplaires. Par conséquent, empêche une éventuelle coopération du point de vu d'une possible harmonisation en ce qu'il n'existe pas de double incrimination, ni de double punissabilité spécifiques.

Dans le droit fil de cette idée, la réalité impose la prééminence de cet outil au service de l'humanité et exhibe la vitesse vertigineuse à laquelle il évolue obligeant une mise à jour constante des chercheurs qui, désormais, doivent sortir de leurs zones de conforts pour embrasser des horizons inconnus, les étudier, en revenir avec des résultats scientifiquement valides afin de faire échos de ce qui vient, tels des sentinelles, pour des prises de position mûrement réfléchies, des choix légaux responsables au reflet de l'éthique miroir des us et coutumes. A la lumière de ce qui précède, les enjeux sont tels que les Etats se ruent vers l'IA la plus performante, engageant une course vers l'armement le plus sophistiqué alliant technologie et protection d'intérêts, se muant en une identité de Puissance. Aujourd'hui, l'IA est une arme, un moyen, une identité, une dissuasion, bref la supériorité. Pour consolider ces acquis, ils investissent des milliards dans ce domaine. Il se révèle être, au XXI ᵉ siècle, l'investissement le plus rentable en situation de conflits ou de potentiels conflits. Les enjeux géopolitiques basculent frénétiquement vers ce qu'autrefois n'était concevable que dans des films de science-fiction, ce qui soulève des préoccupations en matière de sécurité nationale et de stabilité internationale. Par ailleurs, les Etats doivent faire face à des menaces de cyberattaques qui peuvent paralyser des infrastructures critiques sans engagement militaire direct car la guerre n'implique forcément plus des soldats sur terre, sur la mer ou dans les airs. La défense n'est plus la résultante des opérations tactiques et stratégiques, elle est aussi la dernière carte que l'on réserve quand bien même tout aura disparu. Nous sommes en présence des facteurs nouveaux, à impacts exponentiels au regard desquels le Droit pénal congolais, devrait prévoir un cadre légal puis réfléchir en concert avec les autres Etats sur des Traités et Protocoles qui puissent réguler ce nouveau secteur. Cette course n'exclut aucun pays, la République Démocratique du Congo, non plus. Il serait malvenu de négliger son histoire teintée d'indignation due au fait de la guerre d'agression menée par le gouvernement rwandais depuis près de 30 ans avec un bilan lourdement honteux d'au moins 10 millions

[29] A comprendre dans le sens du droit congolais, comme une infraction, la violation à la loi pénale.

[30] Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

[31] Le rançongiciel (ransomware) est un logiciel malveillant générant une demande de rançon après le chiffrement et/ou l'exfiltration de données.

[32] COMMANDEMENT DU MINISTERE DE L'INTERIEUR DANS LE CYBERESPACE (COMCYBER-MI), op.cit., p. 7.

[33] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

[34] La cybercriminalité liée à l'IA militaire désigne des activités criminelles qui exploitent des technologies d'intelligence artificielle dans le contexte militaire/guerre ou qui ciblent des systèmes militaires ou de défenses, leurs infrastructures et leurs données. Ce qui peut inclure :

1. Attaques cybernétiques exploitant l'IA : des hackers peuvent utiliser des algorithmes d'IA pour optimiser leurs attaques, par exemple en menant des analyses avancées pour identifier les vulnérabilités des systèmes militaires/défenses.
2. Drones autonomes et systèmes d'armement : la cybercriminalité peut également cibler des systèmes autonomes comme des drones armés permettant aux acteurs malveillants de le détourner de leur mission ou de compromettre leur fonctionnement.
3. Espionnage et collecte de données : des acteurs étatiques ou non étatiques peuvent employer l'IA pour infiltrer des réseaux militaires et collecter des informations sensibles entrainant des graves conséquences pour la sécurité nationale.
4. Propagation de fausses informations : l'utilisation de l'IA pour diffuser des propagandes ou de fausses informations sur des événements militaires peut également être considérée comme une forme de cybercriminalité car elle influence les perceptions publiques et déstabilise le psychique du personnel militaires que de leurs opérations. (TW3 PARTNERS, « *L'intelligence artificielle au cœur de la cybersécurité militaire : enjeux, avancées et perspectives stratégiques* », in IA Gen Stratégies et avantages, publié le 06 juin 2025., disponible sur https://tw3partners.fr/fr/ia-cybersecurite-militaire-enjeux/?utm).

de morts[35]. Aussi, de sous-estimer ses potentiels naturels qui feront des amis et frères d'aujourd'hui, des ennemis de demain. L'option de l'acquisition de cette technologie aux prouesses exponentielles pour des intérêts congolais n'est pas un mimétisme aveugle, elle est l'allié qui épargnerait l'effusion de sang causée par des armes dotées d'IA par notamment leur détection et destruction, alors qu'elle offrirait une protection optimale des installations stratégiques de l'armée et des services de renseignement afin de survivre dans cette nouvelle ère.

Revenant au Droit congolais, le législateur[36] marque le début de protection de l'intelligence artificielle si bien qu'elle ne l'est pas expressément mentionnée. En effet, l'IA est considérée comme une technologie de l'information et de la communication (TIC), dans bien des contextes y compris ceux qui touchent à la sécurité des Etats. Il en résulte qu'elle est l'une de ses composantes car elle repose sur des systèmes d'information pour traiter et analyser des données. Les technologies de l'information et de la communication incluent par ailleurs les logiciels et les systèmes qui utilisent des algorithmes d'IA pour extraire des informations ou prendre des décisions.

II. DE LA NECESSITE D'ADAPTATION DU DROIT PENAL CONGOLAIS POUR UNE CYBERSECURITE EFFICACE : DES PERSPECTIVES

Ainsi, en termes de perspectives, je préconise la modification des lois pénales particulières[37] qui devraient inclure les caractères de la cybercriminalité liée à l'IA et l'élaboration des lois spécifiques[38] qui définissent ladite cybercriminalité en tenant compte de tous les contours et la cybersécurité correspondante, en parallèle de ratification des instruments juridiques internationaux[39] dans le but de renforcer la coopération internationale. Pour anticiper et faire face aux risques cyber qui menacent les systèmes d'IA à usage militaire et de sécurité, le législateur congolais, devrait renforcer ses mécanismes de sécurité, au-delà du Titre IV traitant de la cybersécurité, de la cryptologie, de la cybercriminalité et de la fraude[40], en s'inspirant de la méthode EBIOS Risk Manager, développée par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), qui permet d'identifier l'ensemble de risques. Dans ce cadre, plusieurs étapes importantes doivent être suivies[41]. Le législateur congolais devrait encadrer les mesures relatives aux réponses à un incident informatique inhérent à l'IA à usage militaire et sécuritaire. Quand une cyberattaque est détectée, celles qui peuvent être prises sont :

1. Comprendre et caractériser l'attaque et les impacts causés ou susceptibles d'être causés ;
2. Contenir et protéger les systèmes concernés ;
3. Faire cesser l'attaque en désinfectant/réparant, puis en restaurant et en reconstruisant les systèmes concernés.

---

[35] E.-J. LUZOLO BAMBI LESSA, S. MAKAYA KIELA, L. MUBIALA MUTOY et al., *Politique nationale de justice transitionnelle en République Démocratique du Congo. Les options fondamentales*, Centre de recherche sur la Justice Transitionnelle, Presses Universitaires du Congo, Commission interinstitutionnelle d'aide aux victimes et d'appui aux reformes, Kinshasa, 2025, p. 68.

[36] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

[37] Idem.

[38] Faisant référence au domaine militaire et de sécurité contre toutes les activités criminelles touchant à la Sûreté de l'Etat et aux droits fondamentaux.

[39] Les voici :

1. Convention de Budapest sur la cybercriminalité ou Convention sur la cybercriminalité du 1er juillet 2004 ;
2. Convention des Nations Unies sur la cybercriminalité adoptée par l'Assemblée des Nations Unies le 24 décembre 2024 à New York par la résolution 79/243 lors de la 55e séance plénière (une ratification dès sa mise en vigueur) ;
3. Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme ont été adoptés à l'unanimité en 2011 par le Conseil des droits de l'homme.

[40] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

[41]

1. Identifier les sources de risques (attaquants, concurrents) qui pourraient conduire à vouloir porter atteinte à ces données ou ces processus ;
2. Identifier les données et les processus à protéger ainsi que les évènements redoutés susceptibles de leur porter atteinte, leurs impacts et leur gravité ;
3. Imaginer, à un niveau stratégique, par quel chemin ces risques pourraient se concrétiser, nécessitant de bien connaître le système d'information, en l'occurrence les systèmes d'IA de l'armée ou de services de renseignement et de l'ensemble de leur composante comme leur sous-traitants ;
4. Imaginer ensuite comment un attaquant peut conduire son attaque au niveau tactique ;
5. Définir les mesures de sécurité à mettre en place pour corriger les vulnérabilités identifiées et réduire la vraisemblance que ces risques se produisent. (AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION ET LE MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE, *Former à la cybersécurité*, Livret enseignant, France, pp. 34-35.).

L'équipe d'agents affectés à cette tâche joue le rôle de Médecin qui doit intervenir pour sauver un patient malade à l'observation duquel il établit un diagnostic et prescrit des médicaments pour une éradication totale du mal. Elle peut, pour certains cas, recourir à la coopération internationale. Et dans l'hypothèse d'une crise de système d'IA d'origine cyber[42], la réaction de l'armée ou de service de renseignement congolais pourrait être, non seulement technique, mais également opérationnelle et stratégique (coordination interne, avec les partenaires, communication, etc.) afin de permettre une sortie de crise rapide. A l'exemple de la France, des dispositifs de gestion de crises de toutes les origines, notamment cyber[43] pouvant inspirer le législateur congolais. En Droit congolais, ce nouveau champ (TIC à destination militaire ou de défense) sort de toute application légale de ce que l'article 3, point 2[44] exclut les installations de télécommunication et de communication de l'Etat, spécialement celles relevant de la défense nationale et de la Sûreté de l'Etat. L'inclusion de l'IA comme technologie de l'information et de la communication est justifiée[45] par son rôle croissant dans la gestion, l'analyse et l'interprétation des données pour des applications variées. Des considérations éthiques et juridiques pourraient également renforcer cette justification, qui plus est, en ce qui concerne les droits de l'homme et la Sûreté de l'Etat. Ainsi, le législateur congolais devrait aborder la question de la cybercriminalité en lien avec l'IA pour des réponses législatives efficaces dans le domaine de la cybersécurité. De ce fait, le cadre juridique existant devrait évoluer pour traiter des nouvelles menaces posées par l'IA utilisée dans le domaine militaire et de sécurité. De manière pragmatique, les lois pénales particulières qui traitent des menaces traditionnelles comme le piratage, le phishing ou l'accès non autorisé à des systèmes doivent inclurent les spécificités de la cybercriminalité liée à l'IA. Ce complément devrait passer par l'identification des nouvelles atteintes après la reconnaissance de l'IA comme facilitatrice d'activités criminelles et comme moyen efficace de renforcement de la cybersécurité. En cette matière qui exige technicité, une collaboration intersectorielle[46] est recommandée. Quant aux solutions de cybersécurité, elles devraient être intensifiées pour répondre aux défis posés par l'IA. Dans cet ordre d'idées, devraient être retenus :

- le choix sur des systèmes d'alerte avancés pour une utilisation d'IA détectant des comportements anormaux dans les réseaux informatiques, ce qui permet d'identifier rapidement des incidents de la cybercriminalité ;
- evaluation de la sécurité des systèmes d'IA : obliger d'un côté les entreprises à évaluer et à garantir la sécurité de leurs algorithmes d'IA pour s'assurer qu'ils ne peuvent pas être détournés à des fins malveillantes et de l'autre, poser une série d'obligations[47] pour l'Administration et les opérateurs (développeurs, utilisateurs) notamment celle d'appliquer des mesures techniques et non techniques qu'il aura retenues afin d'accroître la protection des systèmes d'IA, à côté d'une liste de comportements prohibés. Pour ce faire, il faudrait :
    - une réglementation à la matière s'appliquant aux entités publiques : Les règles devraient inclure les mesures et recommandations retenues dans la politique nationale[48] de sécurité et de contrôle

[42] On parle de crise « *d'origine cyber* » face à un incident informatique malveillant brutal, soudain, menaçant gravement la stabilité d'un Etat ou d'une organisation. (AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION ET LE MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE, idem, p. 43.).

[43]
- ✓ Le Premier Ministre prépare et coordonne au niveau politique l'action des pouvoirs publics en cas de crise majeure (art. L. 1131-1 du code de la défense français) ;
- ✓ La Cellule interministérielle de crise (CIC), activée par le Premier Ministre, met en œuvre la réponse globale de l'Etat. Elle réunit des représentants de haut niveau de différents Ministères concernés et d'autres entités comme l'Agence Nationale de la Sécurité de système d'information (ANSSI), dans le cas d'une crise d'origine cyber ;
- ✓ Des plans préexistent à certains types de crises afin de préparer la prise de décision des autorités. Le plan spécifique au cyber s'appelle Piranet, mais la cybersécurité fait désormais partie d'autres plans de gestion de crise ;
- ✓ La gestion de crise de l'Etat Français nécessite, par ailleurs, la conduite régulière d'exercices de gestion de crise. (AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION ET LE MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE, pp. 43-44.).

[44] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

[45] L'IA est vue comme une extension des technologies de l'information et de la communication avec les interactions complexes avec les systèmes d'information et informatiques.

[46] Le législateur, pour des choix responsables et des prises de position réfléchies, devrait travailler en concert avec des experts en IA et en cybersécurité pour développer des règles qui protègent à la fois les données et les infrastructures critiques.

[47] Garantir la sécurité et l'intégrité des systèmes, Effectuer des contrôles et des audits réguliers pour s'assurer que les systèmes sont protégés contre les risques externes, Se faire former continuellement, Mettre en place et gérer avec transparence les algorithmes (des obligations spécifiques), les mesures de sensibilisation pour les militaires, agents, développeurs et gouvernants sur les risques encourus et surtout ce que prévoit le Droit pénal des nouvelles technologies notamment. Par ailleurs, il devrait exister des obligations positives pour les personnes physiques et/ou morales qui conçoivent, développent, produisent, testent, vendent ou distribuent des systèmes d'IA.

[48] Il lui revient de définir l'alignement réglementaire et éthique de l'IA à usage militaire et sécuritaire pour une cybersécurité éthiquement congolaise et résiliente. Pour y arriver, il faudrait :

de nouvelles technologies. Elles devraient créer une autorité à compétence nationale en matière de nouvelles technologies à usage militaire et de sécurité sous la tutelle du Ministre de la défense.

- une réglementation applicable aux opérateurs publics et privés les plus critiques : Elle devrait comprendre les règles applicables aux opérateurs d'importance vitale, ceux qui gèrent des installations indispensables à la survie de la Nation ; les règles régionales et/ou internationales pour des directives efficaces de sécurité de systèmes d'IA. En effet, les premières devraient établir les seuils[49] de déclenchement et de repli automatique, consacrer les mécanismes[50] de détection d'anomalies et la mise en place des mécanismes de mise à jour et de réentraînement sûrs au travers des simulations régulières des scénarios de défaillance IA. En somme, le but recherché dans la présente étude est un contenu de lois en la matière qui puisse ressortir l'équilibre, à l'ère de l'intelligence artificielle, entre la nécessité d'une Sûreté de l'Etat garantie et le respect des droits de l'homme sur une base d'actes prohibés et des sanctions pénales dissuasives. L'IA est devenue un levier stratégique en cybersécurité militaire facilitant l'anticipation des menaces, des attaques cyber sophistiquées et la protection des infrastructures critiques militaires. Les enjeux des vulnérabilités exploitées par des hackers qui utilisent des algorithmes d'IA pour optimiser leurs attaques[51]. Les risques liés à l'IA militaire comme les fuites de données, le potentiel de deepfakes pour manipuler l'opinion et les enjeux de sécurité autour des systèmes autonomes et des attaques cyber[52]. Le Ministère des Armées souligne que la désinformation est devenue une arme de guerre, avec des campagnes utilisant des deepfakes et autres manipulations IA pour déstabiliser[53] les régimes politiques, la stabilité internationale. La première étape étant, au niveau interne, la reconnaissance juridique des systèmes d'intelligence artificielle, en général, et ceux à usage militaire et sécuritaire, en particulier. Au niveau international, je propose la ratification des instruments internationaux portant lutte contre la cybercriminalité, à savoir : la Convention de Budapest sur la cybercriminalité, la Convention des Nations Unies sur la cybercriminalité. Aussi, celle des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme. Le but étant l'accroissement et le renforcement de la coopération internationale dans un monde pour lequel les frontières ne résistent plus à la criminalité et dans lequel la protection universelle des droits humains constitue un horizon commun.

CONCLUSION

La portée de cet article se place dans la capacité du Droit pénal congolais à s'adapter aux nouveaux intérêts et menaces liés au développement de l'intelligence artificielle à usage militaire et sécuritaire. En effet, le voyage entrepris a été celui de démontrer son intérêt pour les technologies de l'information et de la communication. Une course de survie qui appelle à des mutations multiples et diversifiées invitant le législateur congolais à l'initiation aux prescrits de cette nouvelle ère pour des contenus de lois plus structurés, réfléchis et responsables. Pour ne pas être en retard dans un monde qui ne cesse de se réinventer et participer activement sur la scène internationale comme acteur de décision de ce qui devrait être, ce qui devrait se faire, ce qui devrait être retenu. Notre histoire ne nous permet pas de rester spectatrice et de subir les dictats des autres. Il n'existe pas de hiérarchie. Seules les insuffisances l'imposent.

L'Intelligence artificielle est un langage à apprendre, un moyen à posséder, une identité à revêtir, une arme à porter conséquemment et un outil à utiliser à son aise pour ses intérêts contre toute menace. Elle est la nouvelle compétence, le nouvel allié à encadrer juridiquement pour un équilibre entre la protection des droits de l'homme, la Sûreté de l'Etat et la stabilité internationale. Celle-ci étant la résultante d'une coopération internationale transparente, fluide et rigoureuse dans le respect des instruments internationaux pour garantir la paix et la sécurité internationales dans le climat rude des équations géopolitiques. Cette impulsion nait de

a. Concilier performance algorithmique, sécurité et transparence ;
b. Anticiper les risques par une gouvernance proactive et pluridisciplinaire ;
c. Renforcer la confiance la confiance numérique par des IA sûres, explicables et auditées.

[49] Le seuil dépend de la vision de l'éthique du pays et de l'armée (politique nationale), par conséquent, le degré d'autonomie d'un matériel acceptée par cette politique est déterminant pour l'établissement des différents seuils en présence.

[50] En ce compris I. Machine learning supervisé (1.Précision élevée (si les données sont bien labellisées) et 2. Difficulté à obtenir des labels fiables) ; II. Machine learning non-supervisé (1.Applicable à grande échelle et 2. Risque de faux positifs selon les seuils définis) ; III. Apprentissage semi-supervisé ; IV. Apprentissage par renforcement ; V. Méthodes basées sur l'analyse comportementale (UEBA) et VI. Détection par séries temporelles (Time Series Anomaly Detection).

[51] TW3 PARTNERS, op.cit.

[52] P. RIVIERE, « *IA et renseignement militaire : qui observe qui ?* », in le connecteur, disponible sur https://leconnecteur.org/ia-et-renseignement-militaire-qui-observe-qui/

[53] MINISTERE DES ARMEES, « *La désinformation, une arme de guerre* », publié le 01 mars 2025., disponible sur https://www.defense.gouv.fr/actualites/desinformation-arme-guerre

l'intérieur vers l'extérieur. Ainsi, le législateur congolais est appelé à évoluer au rythme de la société, adapter ses lois et aux pouvoirs publics de prendre conscience des nouveaux défis. La réponse à l'avancée technologique en matière d'IA militaire et de cybersécurité exige des solutions intégrées et collaboratives, basées sur une approche préventive et proactive.

BIBLIOGRAPHIE

I. Textes juridiques

A. Textes juridiques internationaux

- Convention sur la cybercriminalité ou Convention de Budapest du 1er juillet 2004.
- Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme ont été adoptés à l'unanimité en 2011 par le Conseil des droits de l'homme.
- Convention des Nations Unies sur la cybercriminalité adoptée par l'Assemblée des Nations Unies le 24 décembre 2024 à New York par la résolution 79/243 lors de la 55e séance plénière (pas encore entrée en vigueur).

B. Textes juridiques nationaux

- Décret du 30 juin 1940 tel que modifié et complété à ce jour portant Code pénal.
- Loi n°20/017 du 25 novembre 2020 relative aux Télécommunications et aux Technologies de l'Information et de la Communication.

II. Doctrine et travaux académiques

- BEAUGRAND A., *Intelligence artificielle et opérations de maintien de l'ordre : Enjeux et perspectives d'une rupture technologique*, Mémoire de Master 2, Droit public, parcours Sécurité et défense, Université Panthéon-Assas-Paris II, année académique 2019-2020.
- CHANTBOUT B., *Droit constitutionnel et science politique*, 8e éd., Paris, 1968.
- CISWICKI R., « *La définition fonctionnelle de la notion de cybercriminalité* », in memannuaire sécurité défense, Université de Grenoble-Alpes, 2019.
- COHENDET M. A., *Droit public. Méthodes de travail*, 3e édition, Montchrestien, Paris, 1998.
- CONSTANT J., *Traité élémentaire de Droit pénal*, Tome II, Imprimeries Nationales, Liège, 1966.
- DANIEL C.-E., *Les robots et l'Empire du Droit. Forces et limites de la gouvernance par le Droit pour l'encadrement normatif du développement de la robotique interactive*, Thèse de doctorat, Faculté de Droit, Université de SHERBROOKE, Québec, Canada, 2022.
- DESMOULIN-CANSELIER S., *What Exactly Is It All About ? Puzzled Comments from a French Legal Scholar on the NBIC Convergence*, NanoEthics, 2012.
- DJOLI ESENGELI J., *Le constitutionnalisme africain entre la gestion des héritages et invention du futur ; L'exemple Congolais*, Thèse de doctorat d'Etat en Droit public, Université de Paris 1 Sorbonne, 2003.
- DUREZ C., « *Mondes virtuels, Droit et jeu* », in Le Droit dans les mondes virtuels, sous la direction de DELABRE G., CRIDS, Bruxelles, Belgique, 2013.
- FRISON-ROCHE M.-A., *Internet et espace d'interrégulation*, coll. The Journal of the Regulation, Dalloz, Paris, 2016.
- GRAWITZ M., *Méthodes des sciences sociales*, 11e édition, Dalloz, Paris, 2001.
- GROUPE DE TRAVAIL DE LA FONDATION FRIEDRICH-EBERT, « *Les nouvelles technologies militaires et les systèmes d'armes autonomes, L'avenir de la guerre* », in politique de sécurité internationale, Bureau de Paris, novembre 2015.
- GUIRVITCH G., *La vocation actuelle de la sociologie*, Tome I, 3e édition, P.U.F., Paris, 1963.
- KAMUKUNY MUKINAY A., *Contribution à l'étude de la fraude en Droit constitutionnel congolais*, Thèse de doctorat en Droit public, Faculté de Droit, Université de Kinshasa, 2007.
- LUZOLO BAMBI LESSA E.-J., MAKAYA KIELA S., MUBIALA MUTOY L. et al., *Politique nationale de justice transitionnelle en République Démocratique du Congo. Les options fondamentales*, Centre de recherche sur la Justice Transitionnelle, Presses Universitaires du Congo, Commission interinstitutionnelle d'aide aux victimes et d'appui aux reformes, Kinshasa, 2025.
- MANASI N'KUSU-KALEBA R. de B., *Droit pénal spécial congolais*, Editions Droit et Société-D.E.S-, Kinshasa, 2023.
- MANASI N'KUSU-KALEBA R. de B., *Droit pénal spécial. Infractions choisies*, Editions Droit et Société, D.E.S., Kinshasa, Octobre 2023.
- MBAU SUKISA D., *Contribution à la construction d'un cadre de protection pénale de la Constitution en RDC : Etude Positive et prospective*, Thèse de doctorat, Faculté de Droit, Université de Kinshasa, 2020.
- NYABIRUNGU mwene SONGA R., *Traité de droit pénal général congolais*, 2e éd., E.U.A., 2007.
- REUCHLIN M., *Les Méthodes en psychologie*, 3e édition, P.U.F., Paris, 1973.
- SCHWAB K., *La quatrième révolution industrielle*, Dunod, Malakoff, 2017.
- VILLEY M., *Leçon d'histoire de la philosophie du Droit*, Dalloz, Paris, 1963.

III. Webographie

- AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI), « *Panorama de la cybermenace* », Paris, 2024., disponible sur www.cyber.gouv.fr www.cyber.gouv.fr/publications
- AXIOCODE, « *Avantages et inconvénients de l'intelligence artificielle* », publié le 03/07/2019 (modifié le 27/03/ 2025)., disponible sur https://www.axiocode.com/avantages-inconvénients-intelligence-artificielle/
- BESSON, DOZIAS, FAIVRE et al., « *Les enjeux économiques de l'intelligence artificielle* », in Trésor-Eco, France, publié le 02 avril 2024., disponible sur https://www.tresor.economie.gouv.fr/Articles/2024/04/02/les-enjeux-economiques-de-l-intelligence-artificielle?utm
- COMMANDEMENT DU MINISTERE DE L'INTERIEUR DANS LE CYBERESPACE (COMCYBER-MI), « *Rapport annuel sur la cybercriminalité 2024* », 2024, p. 48., disponible sur rapport-ccmi@gendarmerie.interieur.gouv.fr
- CONSEIL DE L'EUROPE, « *Etat des signatures et ratifications du Traité 185*», Portail du Conseil de l'Europe, disponible sur http://conventions.coe.int (consulté le 14 mai 2025).
- CONSEIL ECONOMIQUE SOCIAL ET ENVIRONNEMENTAL (cese), « *Pour une intelligence artificielle au service de l'intérêt général* », in Journal officiel de la République Française, avis, NOR : CESL 1100002X, séance du 14 janvier 2025., disponible sur https://www.lecese.fr/sites/default/files/pdf/Avis/2025/2025_02_IA.pdf?utm
- DOUCET J.-P., « *Dictionnaire de droit criminel* », V° Sûreté de l'Etat. Disponible sur https://ledroitcriminel.free.fr/dictionnaire.htm
- GOUVERNEMENT DU CANADA, « *Ecosystème de l'intelligence artificielle* », in Innovation, Sciences et Développement économique Canada, le 23 mai 2025 (date de modification de l'article)., disponible sur https://ised-isde.canada.ca/site/isde/fr/ecosysteme-lintelligence-artificielle
- MINISTERE DES ARMEES, « *La désinformation, une arme de guerre* », publié le 01 mars 2025., disponible sur https://www.defense.gouv.fr/actualites/desinformation-arme-guerre
- RIVIERE P., « *IA et renseignement militaire : qui observe qui ?* », in le connecteur, disponible sur https://leconnecteur.org/ia-et-renseignement-militaire-qui-observe-qui/
- SANTELOG, « *Intelligence artificielle : l'équilibre nécessaire entre technologie et écologie* », publié le 16/09/2024., disponible sur https://www.santelog.com/actualites/intelligence-artificielle-lequilibre-necessaire-entre-technologie-et-ecologie
- SICHEL O., « *Pour une IA au service de l'intérêt général* », in CDSCOPE, Caisse des Dépôts, n°416, mars-avril 2025., disponible sur https://www.caissedesdepots.fr/sites/default/files/2025-03/CDscope_416.pdf?utm
- TW3 PARTNERS, « *L'intelligence artificielle au cœur de la cybersécurité militaire : enjeux, avancées et perspectives stratégiques* », in IA Gen Stratégies et avantages, publié le 06 juin 2025., disponible sur https://tw3partners.fr/fr/ia-cybersecurite-militaire-enjeux/?utm
- UN HUMAN RIGHTS COUNCIL, « *Principes directeurs relatifs aux entreprises et aux droits de l'homme* », vidéo publiée le 22 novembre 2024, disponible sur https://www.youtube.com/watch?v=pM6040*qH5I
- UNITED NATIONS, « *Convention against cybercrime* », Office on Drugs and Crime, disponible sur https://www.unodc.org/unodc/fr/cybercrime/convention/home.html