REVUE DE L'U.KA

Volume 12, n. 23 (juin 2024)

Finances, Droit et Ethique

Université Notre-Dame du Kasayi
KANANGA

Mesures de répression de la cybercriminalité en droit congolais Analyse de l'ordonnance-loi portant code du numérique

Charles Daniel TSHIBUABUA TSHIBOBA
Assistant à l'Université Notre-Dame du Kasayi (U.KA)

Résumé

La question de la « *cybercriminalité* » ou de la délinquance électronique se pose avec d'autant plus d'acuité que les mass medias sont devenus incontournables dans la société de l'information. La présente étude analyse l'Ordonnance-Loi n°23/010 du 13 mars 2023 portant code du numérique notamment la répression de la cybercriminalité en RDC.

Mots-clés : Code du numérique, répression, société de l'information, cybercriminalité, pénal.

Summary

The question of "cybercrime" or electronic delinquency arises with all the more acuteness as the mass media have become essential in the information society. This study analyzes Ordinance-Law No. 23/010 of March 13, 2023 relating to the digital code, in particular the repression of cybercrime in the DRC.

Keywords: digital code, repression, Cybercrime, information society, criminal.

Introduction

L'ère du numérique, à l'aube du 3e millénaire, est prédominée par l'évolution grandissante des Technologies de l'Information et de la Communication (TIC) qui s'innovent toujours plus et touchent toutes les couches de la vie sociale. A cette époque de digitalisation, les techniques de numérisation et de connexion à l'internet ont changé la manière d'être, de vivre et de connaitre des individus[1].

1 K. NDUKUMA ADJAYI, *Droit de l'économie numérique : E-Commerce et dérégulation européenne, française, internationale, africaine et congolaise des télécoms*, Paris, l'Harmattan, 2019, p. 21.

Ayant le don de l'ubiquité, le numérique affranchit les objets culturels et les contraintes de l'existence physique, en leur permettant d'être répliqués à l'identique et à l'infini sans restriction de temps ni de lieu[2], entrainant ainsi de profonds bouleversements dans les catégorisations juridiques traditionnelles.

Au cours de deux dernières décennies, la navigation sur internet et l'utilisation des services en ligne à partir d'appareils informatiques, sont devenues des activités courantes très répandues dans le monde avec pour conséquences que de plus en plus de personnes sont victimes d'arnaqueurs[3]. Les moyens utilisés par ces cybermalfaiteurs sont de plus en plus sophistiqués et ingénieux.

Comme Jean Carbonnier l'affirmait : « l'évolution des mœurs et des techniques donne naissance à des nouvelles formes de délinquance »[4]. De même, la révolution numérique a engendré, outre quelques avancées positives, des retombées négatives, parmi lesquelles figure en bonne place une criminalité[5] particulière appelée « cybercriminalité », charroyée par les premières lueurs de la société de l'information et qui n'épargne personne en RDC.

Les attaques dont a été victime le système informatique de la Commission électorale nationale indépendante (CENI) congolaise attribuées aux hackers russes, en décembre 2023, en confirment l'expansion[6].

En sus, certaines enquêtes de victimisation de la cybercriminalité ont effectivement démontré que la prévalence de cette criminalité est non moins négligeable et est en hausse constante[7]. Le phénomène est donc préoccupant car il prend de l'ampleur et les conséquences pour les

2 M. DALLE, *Réflexion sur l'éducation des internautes au respect du droit d'auteur*, dans *colloque diffusion*, Paris, Ed. Amiens, 2014, p. 87.

3 Citons les fraudes informatiques, les vols d'identités ou des données à caractère personnel, etc.

4 J. CARBONNIER, *Sociologie juridique*, Paris. PUF, 1978, p. 401.

5 M. QUEMENER, *Cybercriminalité : Aspects stratégiques et juridiques*, *dans Revue de la défense et sécurité collective*, mai 2008, p. 23.

6 Le Président de la CENI, Denis Kadima Kazadi a confirmé les propos tenus par le Vice Premier Ministre congolais en charge de la défense, Jean-Pierre Mbemba Gombo, affirmant que le site informatique de la centrale électorale a fait l'objet de 3244 attaques de la part des hackers russes. En ligne sur www.actualité.cd , RDC : La CENI confirme les menaces de piratage de son site, consulté le 12/02/2023.

7 *La prévention de la Cybercriminalité : résultat d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière*, en ligne sur www.papyrus.bib.umontreal.ca, consulté le 22 avril 2024.

individus, les industries, l'économie et les gouvernements sont de plus en plus considérables et couteuses[8].

Consciente des dangers qui la guettent et des enjeux suscités par l'avènement de la cybercriminalité, la RDC a entrepris, dès octobre 2002, un vaste chantier juridique de mise en place des textes législatifs et réglementaires pour réguler le développement des TIC en vue de protéger les personnes, les biens et les institutions contre le phénomène cybercriminel[9]. Ces réformes ont débouché sur l'Ordonnance-Loi n°23/010 du 13 mars 2023 portant Code du Numérique[10]. Pour rappel, le projet de ladite ordonnance-loi a été validé par le Gouvernement Congolais en octobre 2022 puis jugé recevable par l'Assemblée Nationale en décembre de la même année[11]. Ce code a apporté d'innombrables innovations dans le droit pénal congolais et marqué une nouvelle ère dans la répression des cybercrimes sur le territoire virtuel congolais, mieux le cyberespace.

A la différence des législations antérieures[12], cette loi procède d'une appréhension globale du contexte numérique congolais et des phénomènes cybercriminels. Les rédacteurs ont, en effet, élaboré des véritables Cybermesures de répression du fléau de la cybercriminalité articulées autour du commerce électronique, de la signature électronique, des plateformes numériques, de la protection des données à caractère personnel, de la cybersécurité ainsi que de la lutte contre la cybercriminalité[13].

Dans cette étude, il sera question d'une analyse panoramique des cybernormes de lutte contre la cybercriminalité telles que codifiées dans la présente Ordonnance-Loi tout en démontrant ses mérites et limites dans la répression de la cybercriminalité en RDC.

---

8 C. COUTOU, *La prévention de la cybercriminalité : résultat d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière,* Mémoire de DEA, Université de Montréal, août 2019.

9 Ce vaste chantier juridique débute en octobre 2002 avec l'Ordonnance-Loi n°013/2002 du 16 octobre 2002 relative aux télécoms, remplacée par la loi n°20/017 du 25 novembre 2020 sur les télécoms.

10 *Dans JO de la RDC*, numéro spécial (mars 2023).

11 *RDC : Présentation de l'Ordonnance-Loi portant code du numérique*, en ligne sur www.cio-mag.com, consulté le 6 mars 2024.

12 K. NDUKUMA ADJAYI*, Cybercriminalité, faire du neuf avec du vieux*, Tribune ; en ligne sur www.zooméco.net, consulté le 12/02/2024.

13 Les différents axes de la nouvelle ordonnance-loi sur le numérique ont été présentés par le Ministre national du numérique, Monsieur Désiré-Casimir KOLONGELE EBERANDE. En ligne sur www.actualité.cd, *RDC : EBERANDE KOLONGELE dévoile les avantages du code du numérique*, consulté le 12/02/2024.

1. Apercu du champ d'application et des innovations du code du numérique

Doté de 5 Livres en plus du livre préliminaire, 22 Titres repartis en 50 chapitres et 390 articles, le code du numérique est un véritable levier juridique de transformation digitale de la RDC. Il se positionne aussi comme un instrument de développement et de diversification de l'économie nationale.

En effet, comprendre le contexte de justification de cet instrument juridique n'est pas un fait anodin. Le code du numérique fait suite à l'évolution des mœurs et des habitudes devenues répréhensibles ; car les mœurs en évoluant contraignent le droit à évoluer.

Ce code vient donc réglementer le secteur du numérique en mettant l'accent sur la lutte contre les fausses informations, la diffamation, le cyberharcelement, les arnaques et autres abus qui violent la vie privée des personnes[14]. Ce texte établit donc un encadrement juridique complet de l'économie numérique et il convient d'en étudier le champ d'application et les innovations. .

1.1. Du champ d'application

La législation congolaise du numérique est constituée du code sous examen, des dispositions légales et réglementaires édictées pour son application. Ainsi, nous examinerons l'application de ce code sur le plan matériel et spatial.

1.1.1. Sur le plan matériel

Fort de ses attributs, le chapitre premier du code du numérique consacré uniquement à l'objet et au champ d'application, dispose à son article 1er que les prescriptions de ce code s'appliquent :

- ✓ Aux activités numériques ;
- ✓ Aux écrits, outils électroniques et prestataires des services de confiance ;
- ✓ Aux contenus numériques ;
- ✓ A la sécurité et à la protection pénale des systèmes informatiques[15]

14 A. KABASELE MUKENGE, *La révolution numérique, dans Revue de l'UKA*, vol.10, n. 20, (décembre 2022), p. 9.

15 Article 1er du code du numérique congolais, *dans JO de la RDC*, n° spécial (mars 2023).

Aussi, ce code fixe-t-il le régime fiscal, parafiscal, douanier et de change applicable aux activités et services numériques en RDC.

Cependant, l'article 4 du même code exclut de son champ d'application les activités suivantes :

- Les activités et services numériques exercés pour le besoin de la sécurité publique et de la défense nationale ;
- La réglementation et la régulation des télécommunications [16] ;
- La réglementation et la régulation du secteur de l'audiovisuel et ce, nonobstant les biens immatériels et comportant des éléments immatériels. Ces dernières activités sont régies par des règles particulières compte tenu de leurs susceptibilités.

1.1.2. Sur le plan spatial

L'article 3 de ce code dispose que ses dispositions s'appliquent pour autant que les activités et services numériques s'exercent en RDC par toute personne physique ou morale, quelques soient son statut juridique, sa nationalité ou celle de son capital social.

De la sorte, nous pouvons déduire que les prescriptions du code du numérique s'appliquent lorsque le système informatique ou le réseau de communication électronique est installé en RDC.

En sus, le code du numérique a posé le jalon du principe de l'extraterritorialité qu'il instaure à son article 3 précité. C'est dire en filigrane que ce code sera d'application lorsque les activités numériques sont à destination du territoire virtuel de la RDC. C'est à dire, du moment où par les faisceaux d'indice un système informatique dirige ses activités ou ses services vers le territoire national au point que ces derniers sont accessibles au niveau de la RDC.

Il s'agit d'une avancée significative qui tient compte de l'extraterritorialité du numérique qui ne peut, en principe, se cantonner sur un espace géographique donné[17]. En d'autres termes, le code congolais du numérique est d'application à partir du moment où les activités d'un système informatique ou d'un réseau électronique[18], bien que situé à l'étranger, sont destinées au public se trouvant sur le territoire de la RDC. Toutefois, comme nous le verrons dans la seconde partie de l'étude, cette intention noble et louable appelle des défis cruciaux,

16 La réglementation et la régulation des activités de télécommunications en RDC est assurée par la loi n°20/17 du 25/11/2020 relative aux télécoms et TIC.

17 *Code du numérique : que retenir pour les entreprises* ?. En ligne sur www.avocat.cd, consulté le 06/03/2024.

18 Par réseau électronique il faut considérer le serveur, l'hébergement, le stockage des données, le site internet,…

notamment la coopération policière et judiciaire internationale ainsi que les moyens adéquats.

Outre les domaines d'application du code du numérique, précisons que ce texte a apporté d'innombrables innovations sur le plan technologique.

2. Des innovations du code du numérique

Parmi ces innovations, nous pouvons citer :

- ✓ La réglementation des plateformes numériques ;
- ✓ La dématérialisation des éléments de preuves (admission du principe de la validité juridique de l'écrit électronique et la preuve électronique).
- ✓ La détermination des principes et condition d'identification électronique (nbp16 notamment avec l'utilisation des données personnelles par des procédés électroniques.)
- ✓ L'insertion du principe d'obligation de stocker et loger en RDC chacune des catégories des données pour assurer la souveraineté numérique du pays ;
- ✓ La sécurisation du système informatique contre les cyberattaques ;
- ✓ La détermination des infractions dans le domaine du numérique[19].

Aussi, l'ancien Ministre congolais ayant le numérique dans ses attributions, Monsieur Désiré Casimir Kolongele Eberande, a ajouté parmi les innovations apportées par le texte : la reconnaissance des droits intellectuels et industriels aux logiciels et applications ainsi que leurs matériels préparatoires comme œuvres d'esprit légalement protégées[20].

Par ailleurs, au-delà des innovations décrites plus haut sur le plan matériel, le code du numérique a également apporté du nouveau sur le plan institutionnel notamment la création de :

- ▪ L'Autorité de Régulation du Numérique (ARN) ;
- ▪ L'Autorité Nationale de certification (ANCE) ;
- ▪ L'Agence Nationale de Cybercriminalité ;
- ▪ Le Conseil National du Numérique (CNN) ;
- ▪ L'Autorité de protection des données (APD)[21].

Ces différentes institutions sont créées pour encourager l'éclosion de l'économie numérique et réprimer par la même occasion les faits de cybercriminalité tout en consacrant des obligations de cybersécurité aux

19 A. KABASELE MUKENGE, *art.cit.,* p. 9.

20 En RDC, un nouveau code du numérique pour favoriser le développement et la diversification de l'économie, en ligne sur www.financialafrik.com, consulté le 07/03/2024.

21 Art. 5 et 262 du code du numérique.

opérateurs du secteur. C'est pourquoi l'analyse des dispositions pénales de ce texte s'avère être indispensable.

2.1. Mérites et limites des cybermesures du code du numérique dans la répression de la cybercriminalité en RDC

A n'en point douter, la cybercriminalité est un fait de la société postmoderne. C'est un fléau du tout numérique et du tout connecté pour notre société contemporaine[22].

De l'aperçu définitionnel, la cybercriminalité est l'ensemble de différents délits et infractions susceptibles d'être réalisés ou favorisés par l'usage de la technologie[23]. La dimension réseau qu'introduit internet dans le crime informatique, autorise, via la commission à distance d'un délit, une certaine ubiquité criminelle[24].

Par ricochet, il y'a quelques années, la répression de la cybercriminalité échappait au juge congolais dans bien des mesures compte tenu de l'archaïsme et l'inadaptabilité de l'arsenal juridique en la matière.

En effet, le cyberespace peut être un moyen de commission des infractions de droit commun comme les injures, la diffamation, l'incitation à la haine,… Dans ce cas, le droit commun peut s'y appliquer avec l'adaptation sommaire.

Mais, face aux infractions qui ne se conçoivent que dans le cyberespace, le droit congolais était quasiment en retard ; d'où la nécessité d'une nouvelle réglementation telle que la loi sur les TIC et le code du numérique, sujet de la présente étude.

Ainsi, le code sous examen est une réponse bien réfléchie et sur mesure afin de combler le vide juridique dans le secteur du numérique. Il convient d'en apprécier les mérites et d'en évaluer les limites.

2.1.1. Mérites du code du numérique congolais : modernisation des normes de répression de la cybercriminalité

La RDC s'est dotée d'un code destiné à réguler le secteur numérique du pays. Au livre 4e de cette loi, plusieurs mesures ont été adoptées pour lutter contre la cybercriminalité. Dans ce 4e livre qui traite de la sécurité et de la protection pénale des systèmes informatiques, l'on retrouve des

22 K. NDUKUMA ADJAYI, *op.cit.*, p. 18.

23 S.H. GHERNAOUI, *La cybercriminalité comme facteur de déstabilisation des processus de régulation*, p.4, cité par G. NZE BOLEILANGA, *Le traitement judiciaire de la cybercriminalité en droit congolais*, dans *Revue les analyses juridiques*, n°46, (avril 2022), p. 7.

24 G. NZE BOLEILANGA, *art.cit.*, p. 7.

règles applicables à la cybersécurité, aux modalités de lutte contre la cybercriminalité ainsi qu'à l'utilisation de la cryptologie en RDC[25].

Ce livre fixe également les règles spécifiques de procédures et de compétence de juridiction, en plus de plusieurs crimes électroniques parmi lesquels la fraude informatique, l'usurpation d'identité, la tromperie, la fraude à la carte bancaire, la diffusion du contenu tribaliste, raciste et xénophobe ; la pornographie infantile, le harcèlement par le biais de communication électronique, négation, minimisation grossière, incitation à la commission d'actes terroristes, divulgations des détails d'une enquête, cyberespionage, enregistrement des images relatives à la commission des infractions, atteintes aux droits d'auteurs et à la propriété intellectuelle[26].

Faute de ne pas examiner toutes les incriminations contenues dans ce code, nous allons pouvoir en analyser quelques-unes en deux points dans un aperçu synoptique. Il s'agit de la modernisation des incriminations pénales et l'amélioration de la procédure pénale contre la cybercriminalité.

2.1.1.1. La modernisation des incriminations pénales : adoption des nouvelles infractions spécifiques aux TIC et adaptation des infractions classiques aux TIC

En vue de garantir l'effectivité de la modernisation du droit pénal classique, la technique de la modernisation des qualifications du droit pénal traditionnel a eu pour objectif principal de remédier aux situations latentes de vide juridique et d'inadaptation juridique qui caractérisait l'arsenal pénal classique.

En effet, les grands axes de l'ordonnance-loi du 13 mars 2023 se sont articulés autour de la protection pénale des systèmes informatiques et des données informatiques, de la répression des abus de dispositifs et des infractions informatiques.

a. La protection pénale des systèmes informatiques

Le code du numérique a élaboré des cybermesures comblant ainsi les carences législatives et règlementaires pour paralyser le développement des paradis numériques en RDC[27]. Le législateur congolais a donc

25 Art. 271 du code du numérique.

26 *RDC : Quel est le contenu du code du numérique*. En ligne sur www.infoactualité.cd, consulté le 8 mars 2024.

27 Sur ce spectre des paradis informatiques, V. M. TSHIOBANE, *Le paradis pénal du cyberespace*, sur www.osiris.sn/article html; cité par P. ASSANE TOURE, *La cybertratégie de la répression de la cybercriminalité au Sénégal : présentation de la loi n°2008-11 du 25/02/2008 portant sur la cybercriminalité, conférence sur la coopération contre a criminalité*, Strasbourg, France, 23-25 mars 2010, p. 3.

disposé d'une définition à la notion de système informatique avant d'en détailler les sortes d'atteintes aux systèmes informatiques.

En effet, selon l'article 2.78 de la loi portant code du numérique, le système informatique est défini comme « un dispositif composé des procédures, matériels et des logiciels permettant l'échange, le stockage ou le traitement automatisé des données ». Cette définition se rapproche de celle donnée par la loi sénégalaise du 25 janvier 2008 relative à la cybercriminalité à son article 431-7 et celle donnée à cette notion par la Convention de Budapest sur la cybercriminalité du 23 novembre 2001[28].

La jurisprudence comparée avait même déjà assimilé un ordinateur pris isolément à un système informatique au sens de la loi[29]. De même, il a été jugé qu'un terminal[30] de paiement électronique constitue un système informatique[31]. C'est pourquoi le législateur de 2023 a érigé en valeurs pénalement protégées la confidentialité et l'intégrité des systèmes informatiques.

b. Les atteintes aux systèmes informatiques

1° Les atteintes à la confidentialité des systèmes informatiques

Ces infractions sont prévues à la 2e section du chapitre 2 du 4e livre. Il s'agit de l'accès et le maintien illégal dans un système informatique. L'article 332 du code du numérique incrimine le piratage informatique en disposant que quiconque accède ou se maintient dans l'ensemble ou partie d'un système informatique avec une intention frauduleuse sera puni. C'est une infraction continue.

2° Les atteintes aux données et à l'intégrité du système informatique

– *Les atteintes aux données d'un système informatique*

Elles sont instituées en infractions aux articles 334 et suivant du code du numérique qui dispose : « est puni d'une servitude pénale de cinq à dix ans et d'une amende de cinq millions des francs congolais, celui qui intercepte, divulgue, altère ou détourne intentionnellement et sans droit par des moyens techniques, des données lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système

28 Article 1.a de la Convention sur la cybercriminalité de Budapest du 23 novembre 2001.
29 SV. TRHC Dakar, n°4241/09 du 18 septembre 2009, jugement inédit ; cité par P. ASSANE TOURE, *op. cit.*, p. 3.
30 Un terminal peut être une carte SIM d'un opérateur de télécommunication ou une clé USB.
31 TRHC Dakar, 2e ch. Corr. 12/01/2010, affaire Fulgence BAHI, jugement inédit, cité par P. ASSANE TOURE, *art. cit.*, p. 3.

informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant des telles données ».

Cette disposition protège les données informatiques dans un système contre les changements frauduleux d'état. Aussi, l'article 335 punit celui qui transfère sans autorisation de la personne concernée, des données à caractère personnel d'un système informatique ou d'un autre moyen de stockage des données vers un autre.

Il en découle que les transferts des données personnelles d'un individu, via les plateformes électroniques notamment whatsapp, Facebook, tiktok, … sans son autorisation sont donc prohibés sous peine de l'article précité.

L'on considère comme données à caractère personnel ou données personnelles, le nom d'un individu, son numéro d'identification, son numéro d'assurance sociale, d'assurance maladie, son numéro de permis de conduire, l'adresse du domicile, le numéro de téléphone et l'âge. On y inclut également des images jugées privées[32].

Cependant, l'alinéa 4 de cette disposition exclut 4 cas exceptionnels qui ne tombent pas dans cette incrimination : les interceptions réalisées conformément à un mandat de justice ; la communication envoyée par ou destinée à une personne qui a consenti à l'interception ; l'interception réalisée par une personne morale légalement autorisée pour le besoin de la sécurité publique ou de la défense nationale ; l'interception réalisée par une personne morale ou physique autorisée légalement.

En outre, l'article 336 punit toute personne qui, intentionnellement et sans droit, endommage … altère ou supprime des données ; et si l'infraction est commise dans le but de nuire à une personne, la peine sera très sévère.

– *Les atteintes à l'intégrité du système informatique*

Prévue à l'article 337 du code sous examen, cette disposition vise à sanctionner quiconque, sans droit, provoque ou tente de provoquer l'interruption de fonctionnement d'un système informatique.

Il sied de préciser que cette incrimination tend à protéger les systèmes informatiques contre les infections informatiques et logiciels malveillants qui sont programmés et destinés à détruire les éléments indispensables à leur fonctionnement normal[33].

32 C-D. TSHIBUABUA TSHIBOBA, *La protection des consommateurs des services de télécommunications en RDC.* Mémoire de licence en droit, Université Notre-Dame du Kasayi, 2020, p. 24, inédit.

33 Il s'agit de la protection contre les virus informatiques.

c. Les infractions informatiques

L'on peut ranger dans ce point les infractions visant la falsification des données informatiques ou le faux en informatique et la fraude informatique.

1° Falsification des données informatiques ou faux en informatique

Selon l'article 339 du code sous analyse, le faux en informatique consiste en l'introduction sans droit, dans un système informatique ou réseau de communication électronique, en modifiant ou en effaçant les données stockées, traitées ou transmises par un système informatique ou réseau de télécommunication engendrant des données contrefaites.

L'alinéa 2e de cette disposition punit également l'usage des données informatiques falsifiées. Cette infraction protège l'authenticité des données informatisées au regard du droit commun[34].

2° La fraude informatique

Elle consiste en l'introduction dans un système informatique, modifiant, altérant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, la perturbation du fonctionnement normal d'un système informatique ou des données y contenues.

L'article 340 punit quiconque aura, intentionnellement et sans droit, causé et cherché à causer, un préjudice à autrui avec l'intention de se procurer un avantage illégal pour soi-même ou pour autrui par la commission des actes suscités. L'on peut ranger dans cette même catégorie l'infraction de la fraude des cartes bancaires, prévue à l'article 353 de la loi sur le numérique. Dans cette optique, il a été jugé que le fait pour une personne d'utiliser une carte de paiement falsifiée, en accédant aux terminaux de paiement électronique d'une banque …[35], constitue l'infraction prévue à l'article précité.

d. La répression des autres abus

Loin de nous l'idée de faire du droit pénal spécial en analysant toutes les incriminations prévues dans le code du numérique, nous allons traiter dans ce point de quelques infractions particulières , notamment : les abus de dispositifs, l'usurpation d'identité et les infractions liées au contenu.

34 L'article 124 du code pénal congolais punit le faux en écriture ainsi que son usage.
35 TRHC Dakar, 2e Ch. Corr. 21 janvier 2010, affaire Fulgence, jugement inédit.

1° Les abus de dispositifs et l'usurpation d'identité

– *Les abus de dispositifs*

D'après l'article 338, les abus de dispositifs consistent à produire, vendre, importer, détenir, diffuser, offrir, céder ou mettre à disposition un équipement électronique, principalement conçu pour permettre la commission d'une ou de plusieurs infractions au regard du code du numérique, notamment contre les systèmes des données.

– *L'usurpation d'identité*

Au regard de l'article 351, toute personne qui usurpe, par l'hameçonnage, phishing ou tout autre moyen, intentionnellement et sans droit, par le biais d'un système informatique, l'identité d'autrui, une ou plusieurs données permettant de s'attribuer faussement et de manière illicite, l'identité d'autrui dans le but de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts, sera punie d'une servitude pénale d'un à cinq ans.

2° Les infractions se rapportant au contenu

Au-delà des autres incriminations qu'on ne saura toutes citer ici, les infractions se rapportant au contenu concernent principalement la diffusion du contenu tribaliste, raciste ou xénophobe par le biais d'un système électronique, la pornographie infantile et le harcèlement par le biais des communications électroniques.

- *La diffusion du contenu tribaliste, raciste et xénophobe par le biais d'un système informatique*

Non seulement l'article 356 du code du numérique réprime le fait de créer, diffuser et mettre à la disposition du public, au moyen du système informatique, des contenus de message, images, vidéos ou toute représentation d'idée faisant apologie du tribalisme et du racisme , mais encore faut-il préciser qu'il punit même le simple fait de télécharger des tels contenus.

– *La pornographie infantile*

Considérant les dispositions de l'article 357 du même code, la production et la distribution, la vente, possession d'un matériel pornographique mettant en scène les enfants, c'est-à-dire des mineurs, par le biais d'un système informatique, est sévèrement sanctionnée.

Cette approche, pourtant très extensive, vise à protéger les enfants mineurs, exposés au fléau de la pédopornographie[36].

36 L'on se rappellera les vidéos obscènes des élèves d'une école de Kinshasa, vidéos

La pornographie mettant en scène les mineurs est apparue initialement comme infraction autonome avec la réforme de 2006 du code pénal congolais ordinaire à son article 174m[37] réprimant quiconque aura fait toute représentation par quelques moyens que ce soit d'un mineur s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels des mineurs à des fins principalement sexuelles[38], avant d'être reprise par la loi portant protection de l'enfant qui en modifie uniquement la peine[39].

L'insistance du législateur dans l'incrimination de la pédopornographie dans tous les textes légaux suscités laisse croire donc son soutien indéfectible tendant à protéger efficacement les mineurs contre cet abus.

– *Le harcèlement par le biais d'une communication électronique*

Si les articles 358 et 359 punissent quiconque initie une communication électronique et harcèle ou provoque la détresse émotionnelle chez une personne…, l'article 360 du même code, par ailleurs, sanctionne quiconque relaie une fausse information contre une personne par le biais des réseaux sociaux, des systèmes informatiques ou de toute forme de support électronique.

A en croire cette disposition, toute fausse information concernant une personne qui sera publiée par les medias sociaux et autres plateformes sociales ou réseaux sociaux tels que Facebook, x (ex Twitter), whatsapp, instagram, telegram …, expose son auteur aux poursuites judiciaires.

Comme on peut le remarquer, en modernisant ses instruments juridiques, le législateur congolais met un terme, sinon des gardes fous, à la jungle sociale dans le secteur du numérique avec les différentes incriminations contenues dans ce code. Dans cette optique, la modernisation des incriminations a également conditionné celle d'une procédure pénale contre la cybercriminalité.

---

devenues virales sur les réseaux sociaux.

37 Article 174m de la Loi n°06/018 du 20 juillet 2006 modifiant et complétant le Décret du 30 janvier 1940 portant code pénal congolais.

38 G-D. KASONGO LUKOJI, *Manuel de droit congolais de protection des mineurs*, Kinshasa, éd. Kongo, 2022, p. 370-371.

39 Article 179 de la Loi n°09/001 du 10 janvier 2009 portant protection de l'enfant.

2.1.1.2. L'amélioration de la procédure pénale contre la cybercriminalité en RDC

Raymond de Bouillon Manasi N'kusu et Kodjo Ndukuma Adjayi décrivaient, il y'a quelques années, l'inadaptation du droit pénal congolais en le qualifiant de déficitaire et de vétuste en matière de répression de la cybercriminalité[40].

En adoptant le code du numérique, le législateur congolais sonne une nouvelle ère dans son arsenal juridique. Les nouvelles normes font naître une nouvelle procédure criminelle adaptée. Dans ce contexte, l'adaptation des outils de la procédure classique a permis de consacrer la perquisition et la saisie informatique tout en admettant la preuve électronique en matière criminelle.

a. Consécration de la perquisition et la saisie informatique

Signalons ici que la perquisition et la saisie telles que prévues par la loi aux articles 22, 23, 24, et 25 du code de procédure pénale congolais et les articles 320 à 323 du code du numérique, ont étendu les prérogatives du magistrat instructeur en l'habilitant à procéder à des perquisitions dans un système informatique ou à partir de celui-ci lorsque les données concernées peuvent concourir à l'établissement de la vérité.

En revanche, si les données stockées sont utiles à la manifestation de la vérité, mais que la saisie du support ne parait pas souhaitable, l'article 321 permet au magistrat instructeur à copier sur les supports de stockage informatiques pouvant être saisis et placés scellés[41]. Elles peuvent être de plus en plus rendues inaccessibles ou retirées du système informatique en question sur décision du juge.

b. Admission de la preuve électronique en matière pénale.

Par-delà le principe de la liberté de la preuve en matière pénale, l'article 95 du code du numérique a établi la possibilité d'admettre la preuve électronique en matière criminelle.

La lecture croisée des articles 94 et 95 du code précité permet d'affirmer la même valeur de l'écrit juridique que l'écrit physique sous réserve qu'il soit établi dans les conditions de nature à en garantir

40 R-B MANASI N'KUSU, *Etude critique du système congolais de répression de la cybercriminalité : panorama, annales de la faculté de droit*, UNIKIN, Kinshasa, éd. Droit et Société, juin 2013, p.105 et 126.

41 T. VERBIEST et E. WERRY, *Le droit de l'internet et la société de l'information. Droit européens français et belge*, Bruxelles, éd .Larcier, 2001, p. 34-35.

l'intégrité conformément à la conservation des archives pour être vraiment valable. C'est dans ce cadre que l'encadrement juridique de la preuve électronique en matière pénale s'imposait compte tenu du caractère volatile et du don de l'ubiquité du numérique[42].

Au regard de tout ce qui précède, le code du numérique s'avère complémentaire quant à la procédure pénale à suivre en matière de cybercriminalité. Il suffit, pour s'en convaincre, de considérer l'article 319 qui dispose : « les infractions à la législation du numérique sont constatées dans les procès-verbaux établis conformément au code de procédure pénale ». Ce qui signifie visiblement qu'en ce qui concerne les règles de la constatation des infractions à la législation du numérique ainsi que la détermination de la juridiction compétente, l'on recourt au droit commun, en gardant quelques particularités.

2.2. Limites du code du numérique : défis de l'applicabilité effective des cybermesures contre la cybercriminalité

Dans le contexte actuel de la prolifération des médias sociaux et réseaux sociaux, parfois sans assise connue au pays, il est important de s'interroger de quelle manière l'application du nouveau code sera effective.

A cet égard, les limites de ce code, coulées en forme de difficultés et/ou contraintes de l'applicabilité s'aiguisent sur le plan opérationnel ainsi que sur le plan technique et institutionnel.

2.2.1. Sur le plan opérationnel : risque de restriction des libertés fondamentales

La promulgation du code du numérique et sa publication au Journal officiel ainsi que sa présentation officielle par le Ministre ayant dans ses attributions le numérique, furent des moments émouvants pour la population congolaise avant qu'elle ne s'aperçoive du danger des restrictions des libertés fondamentales.

En effet, cette loi est observée comme un instrument destiné à réduire au silence ceux qui veulent dénoncer les informations sur les médias sociaux. Pour s'en rendre compte, il suffit de lire les dispositions de l'article 360 : « quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sociaux, systèmes informatiques ou toute forme de support électronique, sera puni… »

42 M. DALLE, *op. cit.*, p. 87.

Ainsi, dans un contexte où les réseaux sociaux sont inondés par des comptes fictifs, des comptes pirates et l'insuffisance d'une réglementation efficace ; on le voit, l'internet, pour le différencier des autres moyens de communication comme les journaux et la radio-tv qui sont plus en vogue, représente autant un défi avec la désinformation qu'une opportunité[43], qu'il est important de procéder à la réécriture de cette disposition légale pour éviter que des innocents, dont les comptes peuvent êtres piratés ne subissent d'une peine en lieu et place de leurs bourreaux.

2.2.2. Sur le plan technique et institutionnel

Certes, la régulation du secteur du numérique, en général, et la répression des infractions contre le numérique en particulier, exige une expertise, une logistique et des compétences ainsi que des infrastructures numériques adéquates.

Sans se voiler la face, l'état actuel démontre que ces préalables à l'application effective de ce code sont encore loin d'être réunis. En sus, le code du numérique prévoit la création de plusieurs institutions du secteur du numérique, notamment l'Autorité de Régulation du Numérique (ARN) ; l'Autorité Nationale de certification (ANCE) ; l'Agence Nationale de Cybercriminalité ; le Conseil National du Numérique (CNN) ; et l'Autorité de protection des données (APD). Une année après, depuis le 13 mars 2023, aucune d'entre ces institutions n'est encore installée. La création urgente de ces institutions telles que prévues par cet instrument juridique est donc impérative pour rendre effective l'application du code du numérique.

Conclusion

Après ce tour d'horizon sur les notions essentielles du numérique, il est plausible de préciser que cette étude a porté sur l'analyse synoptique de l'Ordonnance-Loi n°23/010 du 13 mars 2023 portant code du numérique dans ses mesures de répression de la cybercriminalité en RDC. L'analyse s'est penchée sur la présentation de l'objet et du champ d'application de cet instrument juridique tout en démontrant ses mérites et limites dans la lutte contre le fléau de la cybercriminalité.

43 F. MUISANZA KATEWU, *La désinformation et ses applications aux conflits internationaux via les médias : comment une Afrique en quête de démocratie peut s'en protéger* ?, Paris, l'Harmattan , 2017, p. 49.

Il va s'en dire que ce texte est un véritable levier de développement du secteur du numérique, mieux de l'économie numérique en RDC, mais aussi un outil de dissuasion de la commission des cybercrimes par les cyberdélinquants dans le cyberespace.

Le code du numérique a apporté de grandes innovations dans l'arsenal juridique congolais sur le plan pénal en secrétant un véritable cyber droit pénal congolais, régulateur de la société congolaise de l'information. En revanche, toute innovation normative ne passe jamais sans se heurter à certains défis pouvant saper son application effective. Ainsi, outre les mérites de ce nouveau code dans la répression de la cybercriminalité ; il y'a lieu d'édicter les mesures d'application et mettre en place les différentes institutions qu'il prévoit.

Aussi, faut-il renforcer les capacités et équiper les acteurs intervenants dans l'application du code du numérique au-delà de la vulgarisation et de la sensibilisation qu'il requiert. Toutefois, la nature planétaire de la cybercriminalité exige une mobilisation de la communauté internationale contre ce phénomène international.

De ce fait, l'internationalisation du traitement de la cybercriminalité, gage d'une bonne harmonisation de la répression, doit également passer par l'adhésion de la RDC à la Convention de Budapest du 23 novembre 2001[44] et la ratification de la Convention sur la cybersécurité et la protection des données à caractère personnel ; adoptée en 2014 et dont l'entrée en vigueur est imminente[45].

En définitive, l'adhésion de la RDC à ces Traités le placera dans le concert des nations de manière à contribuer efficacement à l'organisation d'une bonne répression de la cybercriminalité qui constitue une menace pour la sécurité et la protection des mass medias dans le cyberespace congolais.

44 La Convention du Conseil de l'Europe sur la Cybercriminalité, dite « Convention de Budapest, conclue en 2001 et entrée en vigueur en 2004, est un instrument important de portée internationale dans ce secteur.

45 Cette Convention a été adoptée par une déclaration des Chefs d'Etat et de Gouvernement de l'Union Africaine. A ce jour, seuls le Sénégal, la Guinée et le Congo-Brazza sont déjà membres en attendant son entrée en vigueur au seuil de sept ratifications.