

La répression de la propagation de fausses informations sur Internet en République Démocratique du Congo

Par Billy Muzambakani Kisula*

Résumé

La propagation des fausses informations sur Internet constitue un défi majeur pour la République démocratique du Congo (RDC), où l'essor du numérique bouleverse les rapports sociaux et politiques. Ces « fake news » fragilisent la confiance des citoyens envers les institutions, alimentent les tensions communautaires et menacent la stabilité nationale. La problématique centrale de cette étude est de comprendre comment le droit congolais est passé d'une absence d'incrimination spécifique à une répression légale et organisée de ce phénomène.

Les résultats montrent que la réforme intervenue avec la promulgation du Code du numérique (ordonnance-loi n°23/010 du 13 mars 2023) marque une rupture normative et traduit la volonté de l'État congolais de moderniser son droit pénal face aux défis technologiques. La conclusion souligne que la répression des fausses informations illustre une transition vers une régulation cohérente du cyberspace, inscrivant la RDC dans une dynamique internationale de lutte contre la cybercriminalité, tout en posant la question de l'équilibre entre liberté d'expression et responsabilité numérique.

Abstract

The spread of misinformation on the Internet poses a major challenge for the Democratic Republic of the Congo (DRC), where the digital revolution is transforming social and political relations. This “fake news” erodes citizens' trust in institutions, fuels communal tensions, and threatens national stability. The central issue addressed in this study is to understand how Congolese law has evolved from a lack of specific criminal provisions to a legal and organized crackdown on this phenomenon.

The results show that the reform brought about by the enactment of the Digital Code marks a normative break and reflects the Congolese state's commitment to modernizing its criminal law in response to technological challenges. The conclusion emphasizes that the crackdown on disinformation illustrates a transition toward coherent regulation of cyberspace, aligning the DRC with international efforts to combat cybercrime, while raising the question of the balance between freedom of expression and digital accountability.

* Doctorant en droit à l'Université de Kinshasa, Assistant à la Faculté de droit et Assistant Principal du Recteur de l'Université de Kikwit (RDC), E-mail : billmuzambakani@gmail.com.

Introduction

Le monde est dominé à l'ère actuelle par l'avancée significative de l'informatique et devant une telle évolution aucune nation ne reste indifférente, car il n'est plus à démontrer la place qu'occupe l'information dans notre société. La découverte de l'Internet qui remonte à plusieurs décennies¹ a impacté et continue d'impacter la vie quotidienne des nations. L'Internet se trouve être l'outil le plus exploité dans la communication et facilite les échanges de manière rapide et fiable. Son utilisation touche les couches des populations même les plus reculées de la planète et contribue ainsi à faciliter la connectivité. Toutefois, le recours aux outils numériques constitue une arme à double tranchante, faite de perspectives positives mais aussi de risques et menaces pesant sur l'activité des Etats, des Entreprises et sur la vie quotidienne des citoyens qui sont aussi très souvent des internautes.²

En 1972, le Doyen Jean Carbonnier affirmait déjà que « l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance ».³ En effet, les réseaux numériques offrent des possibilités nouvelles d'échanges et de diffusion des connaissances, mais ils recèlent aussi bien des risques de dérives préjudiciables au respect des droits de la personne humaine et suscitent l'apparition de nouvelles formes de délinquance et de criminalité (immatérielle) regroupées sous le terme de cybercriminalité dont la répression constitue le champ de la présente recherche. La cybercriminalité est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau Internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité humaine. Ainsi Colin Rose souligne que « la cybercriminalité est la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires ».⁴ Abondant dans le même sens, Mukadi Musuyi estime « qu'il ne serait pas exagéré de la qualifier de SIDA numérique ou informatique ».⁵

Dès lors, la sécurisation des infrastructures d'information est devenue une préoccupation majeure des acteurs publics et privés qui mettent en place des parades technologiques et prennent des mesures pour lutter contre les contenus illicites ou préjudiciables sur Internet, pour protéger les droits de la propriété intellectuelle, les données à caractère personnel et renforcer la sécurité des transactions électroniques, etc. Et face aux maux que cause l'Internet, il est impératif que la lutte contre ce fléau puisse faire l'objet d'une politique pénale définie. D'où la nécessité d'un cadre légal, gage d'une répression significative de toutes les infractions commises sur Internet. Faisant ainsi partie de la cybercriminalité qui demeure difficile à conceptualiser, car il ne fait l'objet d'aucune définition légale ou

1 S. Elzein, L'Indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie in *M-c.Piati (ed.) : Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, Lyon 2001, p. 153.

2 Myriam Quemener, *Cyber menaces, entreprises et internautes*, Paris 2008, p. 86.

3 Jean Carbonnier, *Sociologie juridique*, Paris 1978, p. 9.

4 Colin Rose, cité par Mohammed Chawki, *Essai sur la notion de cybercriminalité*, Paris, 2006, p. 2.

5 Mukadi Musuyi, « Cybercriminalité, le SIDA informatique », Kinshasa, 2008, p. 9.

réglementaire.⁶ Elle s'inscrit dans cette perspective où les formes de la criminalité et de la délinquance passant de l'espace physique au domaine virtuel, changent de nature ainsi que d'expression. Phénomène protéiforme aux contours flou, bien que l'internet joue un rôle salubre à l'ère actuelle, une législation qui réglementerait les comportements des internautes ou usagers de cet outil est d'une grande nécessité pour réprimer et remettre chacun à son aise et ses droits qui lui sont garantis par les textes juridiques tant nationaux qu'internationaux.

Il s'observe qu'en République démocratique du Congo comme sous d'autres cieux, la prolifération des comportements déviants et délinquants tels que des sextapes, des insultes, de fausses informations sur internet, etc. Malheureusement, les auteurs de ces comportements répréhensibles ne sont pas généralement inquiétés par la justice. Quant aux victimes, elles sont de fois dans l'impossibilité de prouver l'identité des auteurs; et même si elles s'y efforcent, la valeur des éléments probants est trop faible pour permettre le déclenchement d'une procédure judiciaire. Devant toutes ces réalités quotidiennes, les droits et libertés de citoyens se trouvent être mis à rude épreuve.

D'où la nécessité de cette réflexion axée sur la répression des fausses informations sur internet en République démocratique du Congo. Cette étude qui part du constat sus évoqué examine la question en se basant sur la l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique en République démocratique du Congo. Dans un premier volet, il sera question d'examiner cette répression avant l'avènement de ce cadre légal et ensuite comment cette loi réprime la propagation de fausses informations sur internet. Mais avant d'y arriver, la définition de concepts clés constituera le préalable et les perspectives marqueront la fin de notre réflexion.

A. Décryptage des concepts opératoires

Définir les concepts dans le cadre de cette démarche est impérative dans la mesure où il faut donner les lignes de compréhension de chacun de ces mots pour éviter toute sorte d'acceptions erronées.

Il sera question de concepts suivants : répression, propagation, fausses information et internet.

1. La répression

Selon le dictionnaire le Littré, le terme répression vient du latin « *repressum, reprimere* » et se rattache à l'action de réprimer, qui signifie le fait d'empêcher de mal faire par la menace ou le châtement⁷. Au sens juridique du terme, le mot répression tire son origine de la définition du droit pénal et de son importance dans les rapports qui régissent les

6 Raymond Gassin, « Le droit pénal de l'informatique », CHRONIQUE 1, Volume 1, N°5, 1986, p. 35.

7 Dictionnaire le Littré : définition du mot répression et du verbe réprimer.

individus dans la société. Et donc la répression est perçue comme une réponse de la société à un mal qualifié de trouble à l'ordre établi. De ce fait, la répression renvoie directement à un individu dans ces rapports avec la communauté. Ce que le contemporain Jean-Jacques Rousseau a préconisé dans sa théorie du contrat social où il soutient que face au comportement qui sort de l'ordinaire, une réponse à l'acte posé par son auteur doit lui être réservée⁸. D'où justement l'idée de répression; on réprime le mal par le mal, ce qui nous renvoie à ce qu'on a appelé sous la Rome antique, « le code d'Hammourabi » exprimé par la maxime « œil pour œil, dent pour dent ». Devant cette théorie qualifiée de la défense sociale, la répression trouve sa justification par le fait qu'elle est une réponse, c'est-à-dire le fait de sanctionner un individu par un châtement ou une punition.

II. La propagation

Le concept propagation, tire son étymologie du latin « *propagationem*, de *propagere* » qui signifie action de propager, c'est-à-dire multiplier, répandre, étendre, faire croître⁹. D'après cette acception, parler de la propagation renvoie à un fait existant dont on répercute l'écho, ce qui créerait la propension vers l'information propagée. La propagation nécessite en premier lieu une information à l'aide d'un canal médiatique disponible et accessible par un grand public sans lequel, ladite information ne serait jamais disponible et donc à la portée d'une telle ou telle autre communauté.

III. L'Internet

Le mot « Internet » est composé du préfixe « inter » qui renvoie au lien entre deux éléments et le mot « net » mot anglais qui signifie « réseaux ». L'internet est donc défini comme un lien entre deux ou plusieurs réseaux informatiques, un réseau des réseaux.

Il s'agit en effet, du réseau informatique le plus prestigieux dans le monde et regroupe une multitude de réseaux régionaux, gouvernementaux et commerciaux. Tous ces réseaux discutent entre eux par le biais du même protocole de communication à savoir TCP/IP (transmission control protocol over internet protocol). La connexion est effectuée par l'utilisation de lignes téléphoniques. Contrairement aux appels téléphoniques traditionnels qui transmettent l'information par le circuit de communication, l'internet transmet l'information par le « paquet commutation ».

IV. La fausse information

Une information est comprise comme un élément de connaissance exprimé sous forme écrite, visuelle, sonore ou numérique, susceptible d'être représenté à l'aide de conventions

8 Raphaël Nyabirungu Mwene Songa, Traité de droit pénal congolais, Tome II, Kinshasa 2007, p. 17.

9 Dictionnaire le Littré : définition du mot propagation.

pour être utilisé, conservé, traité ou communiqué.¹⁰ Elle est aussi synonyme d'une donnée, c'est-à-dire une information ou ensemble d'informations susceptibles d'être stocké, traité ou analysé au sein d'un système informatique ou d'un réseau de communication électronique.¹¹ Une information peut être envoyée sous forme d'un message électronique, c'est-à-dire information envoyée ou transmise à travers un système informatique ou d'un réseau de communication électronique¹², mais aussi sous forme de courrier électronique, c'est-à-dire tout message sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.¹³

Par ailleurs, l'adjectif « fausse » placé devant le vocable information signifie l'altération, la supposition ou la dégradation¹⁴ d'une information. Cette altération est qualifiée de falsification informatique ou de fraude informatique, entendue comme l'introduction, l'effacement ou la suppression des données informatiques qui engendre les données non authentiques d'une part et fausses d'autre part dans l'intention qu'elles soient prises en compte.¹⁵

Les fausses informations ont une portée juridique très large et doivent être comprises aussi comme de fausses déclarations ou dénonciations, ce qui s'apparente aux infractions de droit commun à savoir : les dénonciations calomnieuses, les diffamations, les imputations dommageables et les injures publiques.

B. Analyse chronologie de la répression de la propagation de fausses informations en RDC

L'analyse de la répression de la propagation de fausses informations en RDC est à présenter en deux temps, d'abord avant la promulgation et l'entrée en vigueur du Code du numérique et ensuite après l'avènement de ce dernier.

1. Avant le code du numérique

Parler de la répression revient à recenser les textes juridiques qui incriminaient ce fait d'une part et la sanction y rattachée d'autre part. C'est ainsi qu'il sera question de passer en revue les textes légaux qui incriminaient ces faits avant l'avènement de l'ordonnance-loi

10 Art 4 point 49 de la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

11 Article 2 point 28 de l'Ordonnance-loi n°23/010 du 13 Mars 2023 portant code du numérique.

12 Note (11) point 51.

13 Article 1^{er} de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

14 Dictionnaire le Littré, définition de l'adjectif Faux, Fausse.

15 Lire utilement les articles 7 et 8 de la convention sur la cybercriminalité dite convention de Budapest.

n°23/010 du 13 mars 2023 portant code du numérique en République démocratique du Congo.

1. Le décret du 30 janvier 1940 portant code pénal congolais

Le code pénal congolais malgré son ancienneté était tout en usage face aux infractions perpétrées grâce à l'internet, qualifiées de la cybercriminalité. Cet instrument juridique remontant de l'époque coloniale n'est pas totalement dépassé, plusieurs de ses incriminations restent applicables à la cybercriminalité. Bien que le digital défie l'Etat de droit.

Le code pénal congolais servait d'actualité pour la répression de plusieurs comportements cybercriminels. Il était resté efficace particulièrement pour les infractions classiques qui trouvent en l'internet ou aux technologies d'information et de la communication¹⁶ de véritables moyens de commission. Il faut noter également que la cybercriminalité ne correspond pas à une infraction précise, elle n'est ni futuriste à l'idée, ni surréaliste à l'envie, elle n'est pas aussi récente dans son analyse que l'intellection profane entend faire croire. Vue sous l'angle de nouvelle forme de délinquance, elle s'accompagne largement d'un sentiment d'impunité et du mythe de violation juridique. S'il faut recourir aux conclusions de la magistrate française Myriam Quiminer, elle soutient que la cybercriminalité englobe trois catégories d'activités répréhensibles entre autres : les infractions anciennes de droit commun pour lesquelles l'internet est le moyen facile de leur perpétration telles que les escroqueries, injures publiques et diffamations perpétrées en ligne; les infractions informatiques au sens strict pour lesquelles l'informatique est la cible ou l'objet comme le piratage (hacking) et l'accès illicite aux bases des données; et les infractions dont la condition d'existence est la divulgation d'informations liées à la vie intime ou à la sphère privée sur le support électronique grand public comme la revanche pornographie (l'enregistrement des conversations téléphoniques privées à l'insu de l'interlocuteur en vue de leur diffusion publique¹⁷). C'est sur base de cette approche génésique que nous sommes d'avis avec Kodjo Ndukuma et soutenons que la cybercriminalité au Congo a des rudiments et des réponses dans nos lois pénales.

Comme sus évoqué, le code pénal congolais ne réprimait pas la propagation de fausses informations sur internet comme une infraction distincte des infractions d'imputation dommageables, diffamation, injures publiques, outrages aux bonnes mœurs etc. Dans la pratique judiciaire, cette infraction qui manquait une incrimination précise était poursuivie comme d'autres infractions et il faut également souligner qu'il se posait un problème de preuves, l'on ne savait pas prouver la perpétration de ces infractions sur internet étant donné que l'auteur pouvait utiliser un pseudonyme pour se dissimuler et les éléments probants étaient de faible intensité pour asseoir la conviction du juge et l'OMP qui sont liés par la preuve

16 Kodjo Ndukuma, « La cybercriminalité, Paris 2020, p. 3.

17 Kodjo Ndukuma, note 17, p. 3.

traditionnelle, c'est-à-dire l'écrit. Et donc, il existait une sorte d'impunité des auteurs d'infractions cybernétiques.

En effet, punir la propagation de fausses informations comme l'on punit la diffamation et autres était une analogie non permise en droit sur base du principe « *nullum crimen, nulla poena, sine lege* », car on ne pouvait pas se baser sur la définition légale de la diffamation pour punir la propagation de fausses informations en dépit de leur similitude. L'article 74 du code pénal définit l'imputation dommageable comme « *le fait d'imputer méchamment et publiquement à une personne un fait précis qui est de nature à porter atteinte à l'honneur ou à la considération de cette personne ou à l'exposer au mépris du public* ». Une analogie avec l'infraction d'injure publique prévue à l'article 75 qui nécessite un public – la publicité en demeurant le socle d'après les circonstances et les lieux – n'était pas aussi appropriée. Toutes ces trois infractions ne sont donc pas à confondre, car il est de principe qu'il n'y a pas d'infraction sans loi, ni de sanction sans loi et donc on ne pouvait pas fonder une répression sur base d'une interprétation analogique de la loi car, la loi pénale est de stricte interprétation.

En dehors du code pénal, il a existé aussi d'autres textes légaux qui reconnaissaient au moins l'existence du cyberspace sans pour autant réprimer *expressis verbis* l'infraction de propagation de fausses informations sur internet en République démocratique du Congo.

2. La loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

Tout comme l'ordonnance n°87-243 du 22 juillet 1987 sur l'activité informatique au Congo qui préconisait déjà à cette époque, des peines d'amende contre les usages informatiques qui seraient subversifs aux bonnes mœurs et la loi cadre n°13/2002 du 16 octobre 2002 sur les télécommunications qui prévoyait des délits et des peines face à la levée de secrets de correspondance par la voie des ondes et protégeait les données nominatives et autres à caractère personnel dans les réseaux téléphoniques, la loi de 2020 n'avait toujours pas comblé de défaillances, en l'absence des dispositions antérieures pouvant assurer la protection de la vie privée de la personne humaine et ses données à caractère personnel face aux multiples dangers résultant du développement des technologies de l'information et de la communication. Avec cette loi, il y a la mise en place des mécanismes relatifs à la protection des données à caractère personnel. En outre, elle ne définissait et ne réprimait que des fraudes et infractions liées à l'utilisation des technologies et de la communication, ce qu'il faut lire en son titre III qui traite de la protection de la vie privée et des données à caractère personnel des utilisateurs des réseaux et des services de télécommunication et des technologies de l'information et de la communication¹⁸.

18 Cette loi en dehors de définir les mécanismes de protection de la vie privée a préconisé la répression de certaines infractions liées à la cybercriminalité.

Il sied de noter que même après la promulgation de cette loi, le secteur cybercriminel n'était toujours pas suffisamment règlementé, car cette loi avait elle aussi de failles et d'insuffisances mais aussi et surtout n'a pas pris en compte la répression de la propagation de fausses informations sur internet en République démocratique du Congo.

Il a fallu attendre l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique en RDC pour voir une évolution remarquable.

II. L'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique en RDC.

Face aux limites du dispositif légal actuel dans la répression de la cybercriminalité (voir supra), cette loi est la réponse convenable, car malgré l'existence des dispositions pénales, ces dernières étaient confrontées à la question d'éléments de preuves. Devant ce véritable terrain d'insultes sur les réseaux sociaux et du fait que tout le monde se permet de raconter selon son aise tout sur internet de surcroît même la vie privée des gens sans être gêné ni par la loi encore moins pas la justice. D'où le droit qui a vocation de résoudre les problèmes juridiques dans la société bien que dans le domaine informatique ou cybernétique, une multitude de problèmes est restée sans solutions juridiques ou du moins avec des solutions imparfaites et insuffisantes.

« Le développement du numérique, avec les nombreuses innovations technologiques a révolutionné l'humanité et modifie en profondeur notre façon de penser, de produire, d'échanger et de consommer les biens et services ainsi que nos us et pratiques », disait Cashemir Eberande Kolongele, alors ministre congolais en charge du Numérique. Le numérique, a-t-il rajouté, confronte les pays à des nouveaux enjeux et défis nécessite, par conséquent, l'adoption d'un environnement juridique adapté en mesure de maîtriser et de contrôler les activités et services souvent entre les mains des puissantes entités privées établies à l'étranger et échappant au contrôle de la plupart d'Etats.

Le code du numérique est exactement ce texte qui manquait à l'arsenal juridique numérique congolais pour créer un équilibre entre d'une part, les principes de liberté dans le cyberspace, notamment la liberté d'expression, d'information, de réunion et d'opinion, d'entreprendre, et d'autre part, la protection de la vie privée, la sécurité des échanges, la croissance économique, le progrès social et le renforcement de la gouvernance. Non seulement que ce code réprime la propagation de fausses informations sur internet, mais il prend également en compte, sur le plan juridique, les enjeux concernant le renforcement de la législation se rapportant à la protection des données à caractère personnel, qui oblige les responsables de traitement à veiller à la sécurité des données collectées et à reconnaître aux personnes dont les données sont collectées et traitées l'exercice des droits liées à leurs données personnelles, et consacre notamment :

- Le droit à la portabilité des données et à l'oubli, la possibilité d'introduire une réclamation auprès d'une autorité indépendante de contrôle de données à l'encontre du responsable de traitement ou du sous-traitant;

- La validité juridique de l'écrit électronique et de la preuve électronique ainsi que l'admission des outils qui les accompagnent, notamment l'identification digitale, la signature électronique et le cachet électronique;
- La responsabilité des fournisseurs de services numériques, notamment les fournisseurs de services de confiance qui permettent de garantir les échanges d'informations dans l'espace cybernétique.

Avec le nouveau code du numérique, insulter, diffamer ou calomnier puis relayer sur le net, ont des conséquences réelles sur le plan de la rigueur de la loi. En outre, ce code consacre le respect de la vie privée à travers notamment toutes les dispositions sur la protection de personnes et la détermination des incriminations et des peines qui leur sont applicables.

1. Définition légale de l'infraction de propagation de fausses informations sur internet.

Le législateur congolais définit la propagation de fausses informations sur internet comme « le fait d'initier ou relayer une fausse information contre une personne par le biais des réseaux sociaux, des systèmes informatiques, des réseaux de communication de ou toute forme de support électronique ». En droit français, on parle de la diffusion de fausse nouvelle qui consiste à publier, diffuser ou reproduire, par n'importe quel moyen des informations fausses, des pièces fabriquées, falsifiées voire mensongères et basées sur la mauvaise foi du moment que celles-ci ont été reconnues comme de nature à troubler l'ordre public.¹⁹

Il ressort de la définition de cette infraction les éléments constitutifs suivants :

- L'élément légal : ici, il est question du texte juridique sans lequel cette infraction ne peut exister. La propagation de fausses informations sur internet est définie et réprimée à l'article 360 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique.
- L'élément matériel : il s'agit du comportement réprimé par la loi. Généralement, l'infraction sera constituée, si le comportement a produit un résultat visé par le texte. Mais parfois, l'infraction sera constituée alors même que le comportement n'a pas produit le résultat redouté. Dans le cas de la propagation de fausses informations sur internet, il s'agit du fait d'initier ou de relayer une fausse information contre une personne par les biais des réseaux sociaux, des systèmes informatiques, des réseaux de communication électronique ou toute forme de support électronique. Il faut d'abord qu'il s'agisse d'une

19 Article 27 de la loi française du 29 juillet 1881 sur la liberté de la presse : paragraphe 2 : délits contre la chose publique, modifiée par l'ordonnance n°2000-916 du 19 septembre 2000-art «3(V) journal officiel français du 22 septembre 2000 en vigueur depuis le 1^{er} janvier 2002; cette infraction est punie d'une amende 45.000 euros et les mêmes faits sont punis de 135.000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation, disponible sur <https://www.legifrance.gouv.fr>, consulté le 22/04/2023.

information. Et cette information propagée via les réseaux sociaux doit être fausse au départ contre une personne²⁰.

- L'élément moral ou intentionnel : il s'agit de l'attitude psychologique de l'auteur du comportement réprimé par la loi. Selon les infractions, l'auteur peut avoir agi avec l'intention ou par imprudence. Pour ce qui est de la propagation de fausses informations, il s'agit du fait d'initier ou relayer une fausse information sur les réseaux. Ici la nuance est à deux volets : l'on peut être poursuivi soit comme auteur par le fait qu'on a initié une fausse information et on l'a relayée ensuite, soit comme co-auteur par le simple fait de relayer une information qui s'avère fausse sur les réseaux; c'est dans cette deuxième hypothèque que l'on se retrouve dans le cas d'imprudence.

2. La répression de l'infraction propagation de fausses informations sur internet pour les personnes physiques.

Réprimer suppose la sanction et comme il était difficile de retenir que dans le passé, cette infraction n'avait pas été réprimée faute d'un texte juridique qui incriminait ce fait tel qu'il en est le cas dans le code du numérique. D'où justement la raison d'être de cette recherche. Il est question ici de détailler la manière dont cette infraction est réprimée en République démocratique du Congo.

Comme nous l'avons indiqué ci-haut, le principe de la légalité de délits et de peines veut à ce qu'un fait doit être défini comme fait infractionnel par la loi et que cette loi doit en déterminer la sanction éventuellement applicable. Dans le cas d'espèce, le législateur définit la propagation de fausses informations et prévoit ainsi la sanction à l'article 360 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique d'une peine de servitude pénale d'un à six mois et d'une amende de cinq cent mille à un million de francs congolais ou l'une de ces peines seulement. Cette répression est significative dans la lutte contre la cybercriminalité en RDC. Ainsi, désormais, insulter, calomnier ou diffamer une personne sur les réseaux ne restera plus impuni.

3. La répression de l'infraction propagation de fausses informations sur internet pour la personne morale.

Il est très important de spécifier la répression de cette infraction que pourrait aussi commettre la personne morale de même qu'elle serait victime comme il en est question pour les personnes physiques. La question principale restera de savoir comment poursuivre une personne morale qui serait auteure de cette infraction d'une part et dans quelle mesure la personne morale peut réagir pour intenter une action en justice lorsqu'elle est victime de propagation de fausses informations sur internet.

20 Ici l'accent est mis sur le fait que l'auteur peut être soit l'initiateur ou soit le canal par lequel, une fausse information passe pour être propagé.

Le principe selon lequel “la personne morale ne peut délinquer” (*societas deliquere non potest*) connaît une limite en matière économique au regard de certaines sanctions spécifiques qui leur sont applicables à l’instar de la fermeture de l’établissement et le retrait de l’autorisation d’exercer, etc. Il en va de même pour la réparation du dommage que peut subir une personne morale à la suite de propagation de fausses informations sur internet dont elle serait victime. Dans le cadre de la loi portant code du numérique en RDC, la question de la responsabilité pénale de la personne morale est résolue à la lumière des articles 308 à 314.

Le législateur congolais punit la personne morale au regard de sa spécificité par l’une de sanctions suivantes :

- La servitude pénale;
- L’amende;
- La confiscation spéciale;
- La dissolution;
- La fermeture définitive ou pour une durée de cinq ans;
- L’exclusion définitive des marchés publics ou pour une durée de deux à cinq ans;
- L’interdiction définitive ou pour une durée de deux à cinq ans;
- La confiscation de l’outil qui a servi à commettre l’infraction et du produit de l’infraction.

Il faut préciser que le code du numérique punit une catégorie de personnes morales à savoir : les personnes morales de droit privé lorsque les infractions sont commises pour leur compte par l’un de leurs représentants, les dirigeants des personnes morales de droit privé lorsqu’ils commettent des infractions liées à la cybercriminalité dans les mêmes circonstances et dans l’exercice de leurs fonctions. Pour les agents de l’Etat ou fonctionnaires publics œuvrant pour l’Etat, les provinces, les entités territoriales décentralisées, les autorités administratives indépendantes et les établissements publics, leur responsabilité pénale est individuelle lorsqu’ils commettent des infractions dans le cas sus évoqué.

Conclusion

La problématique de la répression des fausses informations en République démocratique du Congo révèle longtemps un vide juridique qui favorisait l’impunité numérique et fragilisait la confiance des citoyens envers les institutions. Les textes anciens, tels que le Code pénal de 1940 et la loi de 2020 sur les télécommunications, ne prévoyaient pas d’incrimination spécifique, laissant les juges démunis face à une criminalité immatérielle en expansion.

L’adoption du Code du numérique en 2023 marque une évolution normative décisive. En érigeant la propagation de fausses informations en infraction autonome assortie de sanctions pénales et financières, ce texte modernise le droit congolais et dote la justice d’outils adaptés aux réalités technologiques. Il renforce la valeur probante des écrits électroniques et la protection des données personnelles, contribuant ainsi à une meilleure gouvernance numérique.

Cependant, des défis persistent : la preuve numérique reste fragile et l'équilibre entre liberté d'expression et responsabilité demeure délicat. Des pistes de réflexion s'imposent, notamment la formation des magistrats, la sensibilisation des internautes et la coopération internationale pour consolider la lutte contre les cybermenaces.