

« La protection des données personnelles en RDC face à l'émergence du numérique »

Alkain KALALA NSAMBI

Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, chercheur en Droit des affaires, Droit International, Droit Judiciaire¹ et en Droit Numérique.

MOTS-CLES

« La protection des données personnelles, l'émergence technologique, le numérique, le code du numérique, la réglementation spécifique, la protection de la vie privée, l'Intelligence Artificielle »

RESUME

L'émergence rapide du numérique en République Démocratique du Congo a ouvert de nouvelles perspectives économiques et sociales, mais elle a également soulevé des défis majeurs en matière de protection des données personnelles.

Alors que de plus en plus de services et de transactions se numérisent, la nécessité de protéger la vie privée des citoyens congolais est devenue une préoccupation centrale ; il est très crucial de noter que dans le contexte numérique mondial, la question relative aux données personnelles constitue un enjeu majeur de souveraineté étatique² et d'intérêt économique³.

Cette émergence de la technologie dans le monde est une véritable expansion des nouveaux systèmes techniques du numérique et de l'électronique, la protection des données personnelles à l'ère du numérique comporte plusieurs difficultés en droit congolais.

Cet article se doit de relever intégralement l'analyse et l'application des lois relatives à la protection des données en République Démocratique du Congo.

¹ <https://www.leganet.cd/Doctrine.textes/DJud/double%20degre%20nsambi%202022.pdf>

² Pour en savoir plus, Lire BELLANGER Pierre, *La souveraineté numérique*, stock, 2014. GUEHAM Farid, *vers la souveraineté numérique : pour une nouvelle gouvernance de l'internet*, Fondation pour l'innovation politique.

³ V. TOLEDANO Joelle, *GAFA : Reprenons le pouvoir*, Odile Jacob 2020.

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

Actuellement, la RDC ne dispose pas de loi spécifique et exhaustive dédiée à la protection des données personnelles, à l'instar du Règlement Général sur la Protection des Données (RGPD) en Europe.

Le cadre juridique existant est dispersé et fragmenté, ce qui le rend insuffisant pour encadrer efficacement les pratiques de collecte, de traitement et de stockage des données dans l'environnement numérique.

Les dispositions existantes se retrouvent dans des textes généraux tels que la loi relative aux télécommunications et aux technologies de l'information et de la communication (TIC), qui aborde la question de la confidentialité des communications.

Cependant, ces articles ne couvrent pas la diversité des enjeux modernes, comme le consentement, le droit à l'oubli, ou les transferts de données transfrontaliers.

L'absence d'une autorité de régulation indépendante et dotée de pouvoirs de sanction est également un point faible. Le contrôle et la surveillance de l'application des rares dispositions existantes sont complexes, laissant souvent les citoyens sans recours en cas de violation de leurs droits les plus légitimes.

ABSTRACT

The rapid emergence of digital technology in the Democratic Republic of Congo has opened up new economic and social opportunities, but it has also raised major challenges regarding the protection of personal data. As more and more services and transactions become digitized, the need to protect the privacy of Congolese citizens has become a central concern.

This emergence of technology in the world is a true expansion of new digital and electronic technical systems, and personal data protection in the digital age faces several difficulties under Congolese law. This article aims to fully address the analysis and application of laws related to data protection in the Democratic Republic of Congo.

Currently, the DRC does not have a specific and comprehensive law dedicated to the protection of personal data, similar to the General Data Protection Regulation (GDPR) in Europe. The existing legal framework is scattered and fragmented, making it insufficient to effectively regulate the practices of data collection, processing, and storage in the digital environment.

Existing provisions can be found in general texts such as the Law on Telecommunications and Information and Communication Technologies (ICT), which addresses the issue of communication confidentiality. However, these articles do not cover the diversity of modern challenges, such as consent, the right to be forgotten, or cross-border data transfers.

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

INTRODUCTION

L'avènement de l'ère numérique a engendré une transformation sans précédent de nos sociétés, et la République Démocratique du Congo (RDC) n'y fait pas exception. L'accès croissant à Internet, l'essor des services en ligne et la multiplication des plateformes numériques ont ouvert de vastes opportunités économiques et sociales.

Cependant, cette révolution technologique s'accompagne d'un défi majeur : celui de la protection des données personnelles, comme c'est le cas avec l'absence de contrôle juridictionnel et réglementaire, une fois les données transférées vers un pays tiers, la RDC perd en grande partie son contrôle sur leur gestion et leur utilisation⁴, ce qui a pour conséquence que les autorités nationales ne disposent généralement d'aucun pouvoir de surveillance ou des sanctions à l'égard des entités étrangères qui traitent ces données.

Cela peut poser un problème en cas d'atteinte aux droits des citoyens congolais, notamment lorsque les mécanismes de recours sont limités ou inexistants⁵.

Dans un monde où chaque clic, chaque transaction et chaque interaction en ligne génère des informations, les données personnelles sont devenues une ressource précieuse, souvent qualifiée de « nouvel or noir⁶ ».

En RDC, le manque de cadre juridique et institutionnel spécifique expose la vie privée des citoyens à de nombreux risques. En l'absence d'une loi exhaustive dédiée à la protection des données, et d'une autorité de régulation indépendante, les informations sensibles des Congolais sont collectées, traitées et stockées sans garanties suffisantes.

Si le pétrole a dominé les débats économiques du 20ème siècle, les données sont qualifiées d'or noir du 21ème siècle dans le sens où les données personnelles transitant sur Internet sont devenues des richesses capitales qui viennent accompagner le développement de nos sociétés, symbole de la numérisation et de la dématérialisation de nos sociétés, l'exploitation de ces datas a effectivement pris une importance

⁴ Brozeck Kandolo wa Kandolo, « Les transfert des données personnelles hors de la RD Congo », Journal CODES Africa- Numéro 2- Vol 1. Mars 2025

⁵ *Idem*

⁶ <https://pro.orange.fr/lemag/les-donnees-l-ornoirdu21emesiecleCNT0000019pH8b.html#:~:> Source consulté le 26 Septembre 2025 ; à 9H'05

capitale aussi bien pour les administrations et organisations publiques que pour les entreprises privées qui ne peuvent plus passer à côté de ce carburant numérique⁷.

Cette situation est d'autant plus préoccupante que les acteurs du numérique, qu'ils soient nationaux ou internationaux, opèrent sur un marché en pleine expansion. L'exploitation non encadrée de ces données peut conduire à des abus, des cyber attaques, des fuites d'informations, voire une utilisation à des fins illégitimes, compromettant ainsi les droits fondamentaux des individus.

Cet article se propose d'analyser en profondeur les enjeux de la protection des données personnelles en RDC. Il mettra en lumière les lacunes du cadre juridique actuel, les risques encourus par les citoyens et les entreprises, et esquissera des pistes de réflexion pour la mise en place d'une législation moderne et efficace.

L'objectif est de démontrer que la protection de la vie privée n'est pas un frein à l'innovation, mais bien une condition essentielle pour bâtir une économie numérique sûre et de confiance, où les droits fondamentaux sont respectés.

PROBLEMATIQUE

Comment le cadre juridique actuel de la RDC assure-t-il la protection des données personnelles face aux défis et opportunités de l'ère du numérique ?

Face à cette problématique, nous pensons que le cadre juridique actuel de la République Démocratique du Congo est manifestement inadapté pour assurer une protection efficace des données personnelles à l'ère du numérique. L'absence d'une loi spécifique et exhaustive, telle que le RGPD en Europe⁸, est la problématique centrale.

Les dispositions existantes sont dispersées dans des textes généraux comme la loi sur les télécommunications, qui ne couvrent pas la complexité des défis modernes, en l'occurrence : le consentement explicite, le droit à l'oubli ou les transferts de données transfrontaliers.

Face à l'émergence des services numériques et des transactions en ligne, cette lacune juridique crée une situation de vide législatif, exposant les citoyens à des risques majeurs notamment: l'utilisation abusive de leurs informations par les entreprises, fuites de données et profilage intrusif⁹.

⁷ *Idem*

⁸ Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016, RGPD, source : journal officiel de l'UE

⁹ <https://www.cnil.fr/fr/profilage-et-decision-entierement-automatisee#:~:text=Le%20profilage>, source consulté le 26 septembre 2025, à 11H : 33

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

Les opportunités économiques et sociales offertes par le numérique se heurtent ainsi à un environnement de défiance et d'insécurité pour les consommateurs. Il est impératif que la RDC se dote d'une législation moderne et d'une autorité de régulation totalement indépendante ou renforcer intégralement l'Autorité de Régulation des Postes, de l'Information de la télécommunication (ARPTIC) remplaçant l'Autorité de Régulation du Numérique (ARN)¹⁰ prévue par le code du numérique pour garantir un développement numérique responsable et respectueux des droits fondamentaux.

I. : LE CADRE JURIDIQUE EXISTANT DE LA PROTECTION DES DONNEES PERSONNELLES EN RDC

Le cadre juridique de la protection des données personnelles en République Démocratique du Congo (RDC) a connu des avancées significatives ces dernières années. Il est principalement régi par l'Ordonnance-Loi n° 23/010 du 13 mars 2023 portant Code du Numérique :

C'est le texte le plus important et le plus récent en la matière, il vise à combler les lacunes des législations précédentes en matière de protection des données personnelles.

Ce code aborde des aspects cruciaux tels que : les principes liés au traitement des données¹¹, les droits des personnes concernées comme le droit à la confidentialité, le droit au consentement pour le traitement des données, l'interdiction des traitements de données particulières, des sanctions pénales en cas de non-respect des dispositions, avec des amendes et des peines de prison pour les contrevenants.

Ensuite il y a la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, notons qu'avant le Code du Numérique, cette loi contenait déjà des dispositions relatives à la protection des données à caractère personnel.

Elle posait notamment le principe de la garantie du secret des correspondances et proscrivait toute atteinte à ce secret, sauf dans des cas d'intérêt public prévus par la loi, cette loi prévoit que toute personne a droit au secret des correspondances émises par voie de télécommunications et des technologies de l'information et de la communication ; le secret des correspondances est levé sur réquisition du ministère public ou sur autorisation des Cours et Tribunaux dans le cadre de l'instruction judiciaire¹².

Cependant, elle était considérée comme moins exhaustive et ne détaillait pas suffisamment les aspects liés au traitement, au consentement, ou aux transferts de données.

¹⁰ Brozeck Kandolo wa Kandolo « *régulation du numérique en RDC, l'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données* » Droit-Numérique.cd - Dossier N°4 Octobre 2024.

¹¹ Art 184 de l'Ordonnance-Loi n° 23/010 du 13 mars 2023 portant Code du Numérique

¹² Art 126 la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

I.1. LES FONDEMENTS CONSTITUTIONNELS ET LEGISLATIFS DISPERSÉS

La base juridique sur la protection des données personnelles en République Démocratique du Congo est tout d'abord consacré fondamentalement par la constitution qui prévoit en son article 31 que « Toute personne a droit au respect de sa vie privée et au secret de la correspondance, de la télécommunication ou de toute autre forme de communication. Il ne peut être porté atteinte à ce droit que dans les cas prévus par la loi¹³. »

Cette disposition constitutionnelle confirme en effet la licéité d'une protection rigoureuse devant toute entrave ou manquement aux données personnelles en RDC, il est impérieux de noter que la société numérique prend de plus en plus de l'ampleur et les victimes sont nombreuses car la sécurité numérique congolaise a encore des imperfections sur le plan juridique et électronique nonobstant les récentes réformes en matière de protection des données avec l'intervention du code du numérique.

Sur le plan législatif, avec l'intervention du code du numérique ; le législateur congolais a réglementé en spécifiant l'application de loi en matière de protection des données personnelles au niveau de l'article 183 du code du numérique qui dispose que les catégories suivantes sont considérées comme données personnelles. Il s'agit notamment de :

- des données d'identification personnelle notamment : prénom, nom, post-nom, date et lieu de naissance, âge, état civil, numéro d'identification nationale, document officiel d'identité en cours de validité et toute autre donnée biométrique notamment photographie, enregistrement sonore, image, empreintes digitales et iris.
- des données de correspondance : coordonnées téléphoniques, adresses physique, postale et électronique ;
- des données professionnelles : statut, emploi occupé, employeur, rémunération ;
- des données de facturation et de paiement : montant et historique des factures, état de paiement, relances, soldes de paiement, date de prélèvement ;
- des coordonnées bancaires : code banque, numéro de compte et de la carte bancaire, nom/adresse/coordonnées de la banque, références de transactions ;
- des données sur des personnes morales de droit public ou privé faisant apparaître les données personnelles ;
- des données sur la situation familiale ;
- des données concernant des décisions de justice¹⁴.

¹³ Art 31 de la Constitution du 18 février 2006 modifiée et complétée par la loi n°11/002 du 20 janvier 2011

¹⁴ Art 183 Ordonnance loi N°23/10 du 13 Mars 2023 portant le code du numérique.

La République Démocratique du Congo a clairement affiché sa volonté de se doter d'un cadre juridique moderne pour la protection des données personnelles, l'adoption du Code du Numérique en 2023 marque une avancée significative et c'est une preuve que le législateur congolais a la volonté d'une réelle et effective protection des données des citoyens congolais, mais la gestion et le suivi de la sécurité numérique de cette matière font encore apparaître des points faibles indéniables, ainsi que des défis persistants en matière de mise en œuvre de cette loi spécifique.

Par ailleurs, le socle de la protection des données en RDC repose sur des bases constitutionnelles solides, en l'occurrence l'article 31 de la Constitution du 18 février 2006, qui garantit le droit au respect de la vie privée et au secret des communications qui sont particulièrement pertinents et importants. Il pose en effet ; le principe fondamental selon lequel toute atteinte à la vie privée doit être expressément prévue par la loi.

Cette disposition est essentielle, car elle établit une obligation de légalité et de proportionnalité, empêchant l'arbitraire et offrant une protection intrinsèque aux citoyens congolais.

1.1 La Constitution du 18 Février 2006

Dans cette partie de la recherche, il est question de comprendre le fondement constitutionnelle sur la notion de la protection des données principalement en analysant de l'article 31, c'est-à-dire comprendre ce qu'on entend par le droit au respect de la vie privée, aux correspondances ou à toute forme de communication.

1.2 La protection de la vie privée et du secret de la correspondance.

La protection de la vie privée est entendue en droit numérique comme l'ensemble des droits et des mécanismes juridique, techniques et organisationnels visant à garantir à un individu la maîtrise de ses données à caractère personnel et de sa sphère intime face aux collectes, traitements, stockages et diffusion par des tiers, notamment dans l'environnement numérique, elle englobe le droit à l'autodétermination informationnelle , le droit à l'oubli, le respect de la correspondance privée, de l'image, de l'honneur et de la réputation en ligne, et la nécessité d'un consentement éclairé pour toute utilisation des données personnelles¹⁵.

L'article 192 du code du numérique renchérit en disposant que « Le traitement des données personnelles n'est licite que dans la mesure où la personne concernée a consenti au traitement de ses données à caractère personnel ou si le traitement est nécessaire à l'exécution d'une obligation légale à

¹⁵ Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016, RGPD, source : journal officiel de l'UE, p. 1 -88
 Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

laquelle le responsable du traitement est soumis. Le traitement de données personnelles se fait dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques¹⁶. »

La notion de consentement est d'une importance capitale et déterminante dans les processus de traitement et de protection des données personnelles, et il existe déjà un organe régulateur et protecteur de cette matière appelé L'ARPTIC, historiquement chargée de la régulation des télécommunications¹⁷, a vu son périmètre d'action s'élargir avec la réforme de 2020¹⁸ et le décret de 2023¹⁹, qui lui ont conféré de nouvelles compétences dans le domaine numérique.

Cependant, l'arrêté de 2024²⁰ a encore accentué cette évolution en lui assignant des missions additionnelles. La question centrale est désormais de savoir si l'ARPTIC dispose des ressources adéquates pour répondre à ces nouvelles responsabilités.

Sur le plan juridique, le principe de légalité²¹ impose à l'ARPTIC d'agir dans le cadre défini par la loi et par l'arrêté qui lui confère ses nouvelles responsabilités. Cela implique qu'elle doit être dotée des ressources nécessaires pour respecter les exigences de cette législation²².

S'agissant de la communication, notons que les nouvelles technologies de l'information et de la communication (NTIC) prennent chaque jour plus d'importance et posent de nombreuses problématiques juridiques²³.

Cette révolution transcende les branches du droit existantes pour s'appliquer à des domaines multiples et variés : administration électronique, services publics, cybercriminalité et cyber défense, enjeux de propriété intellectuelle, droit des marques et droits d'auteurs, sécurité des réseaux de télécommunication sont autant de secteurs sensibles aux nouvelles technologies et dans lesquels les juristes sont très attendus.

¹⁶ Art 192 de l'Ordonnance loi N°23/10 du 13 Mars 2023 portant le code du numérique.

¹⁷ Lire J. PANZA et B. KANDOLO, « L'histoire du numérique et ses défis réglementaires en République démocratique du Congo », op. cit.

¹⁸ La loi sur les télécoms et TIC 2020

¹⁹ Décret portant la création de l'ARPTIC de 2023

²⁰ Arrêté ministériel de 2024, portant harmonisation des modalités de mise en œuvre des régimes du code du numérique et de la loi sur les télécoms et TIC.

²¹ Le principe de légalité impose que toute action ou décision prise par une autorité publique doit être conforme à la loi. Cela signifie que l'ARPTIC ne peut agir que dans le cadre des pouvoirs qui lui sont conférés par la législation et les arrêtés qui définissent ses missions et compétences. Pour en savoir plus sur ce principe juridique lire, J. GOURDOU, « Principe de légalité - Fiche LexisNexis 360 », Fiches pratiques [Lexis 360 Intelligence], 2018, disponible sur <https://univ-pau.hal.science/hal-02447543> (Consulté le 5 octobre 2024).

²² Brozeck Kandolo wa Kandolo « régulation du numérique en RDC, l'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données » Droit-Numérique.cd - Dossier N°4 Octobre 2024. p.11-12

²³ Catherine Barreau et Najoua Djerad « DROIT ET NUMÉRIQUE » Actes du Colloque international 20 et 21 novembre 2017, p.21-22

1.3 Limites de cette protection face aux défis numériques spécifiques.

Plusieurs éléments spécifiques démontrent les limites de la protection des données personnelles des usagers du numérique en RDC, d'une part ; le transfert de données personnelles hors de la RDC, bien que facilitant la circulation de l'information et l'accès aux services numériques mondiaux, comporte des risques pour la confidentialité, la sécurité et la souveraineté des données. Ces données, une fois transférées, peuvent être soumises à des régimes juridiques étrangers, parfois moins protecteurs des droits des individus.

Les multinationales opérant en RDC participent également à ces transferts en rapatriant les données personnelles collectées localement vers leurs sièges sociaux situés à l'étranger²⁴. Or cette pratique soulève dans la plupart des cas des interrogations quant à la protection des données personnelles de citoyens congolais, notamment lorsque celle-ci sont envoyées vers des Etats dont la législation en matière de protection des données personnelles est moins rigoureuses²⁵.

La question de la transparence dans la gestion de ces transferts devient ainsi cruciale, notamment en ce qui concerne le consentement des personnes concernées, la traçabilité des flux de données et les garanties offertes par les pays de destination²⁶ ; et d'autres part c'est l'absence de contrôle juridictionnel et réglementaire, une fois les données transférées vers un pays tiers, la RDC perd en grande partie son contrôle sur leur gestion et leur utilisation.

Les autorités nationales ne disposent généralement d'aucun pouvoir de surveillance ou de sanction à l'égard des entités étrangères qui traitent ces données. Cela peut poser un problème en cas d'atteinte aux droits des citoyens congolais, notamment lorsque les mécanismes de recours sont limités ou inexistant²⁷.

I.2 LA LOI SUR LES TELECOMMUNICATIONS ET LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC) :

La loi sur les télécommunications et les technologies de l'information et de la communication apporte plusieurs innovations, en l'occurrence : la prise en compte des nouvelles

²⁴ Dernier rapport disponible de l'Agence Nationale pour la Promotion des Investissements (ANAPI) sur le volume des Investissements Directs Étrangers (IDE), classant parmi les trois principaux investisseurs étrangers la Chine, le Royaume-Uni et les Pays-Bas. Pour consulter le rapport, voir : [\[https://www.investindrc.cd/fr/spip.php?article14\]](https://www.investindrc.cd/fr/spip.php?article14)

²⁵ Brozeck Kandolo wa Kandolo, « Les transfert des données personnelles hors de la RD Congo », Journal CODES Africa- Numéro 2-Vol 1. Mars 2025

²⁶ CODES AFRICA « *Le guide des pionniers du numérique* » LE TRANSFERT DES DONNÉES PERSONNELLES HORS DE LA RDC. MARCH 2025 /VOL 1. p. 3

²⁷ Idem, p. 3

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

technologies de l'information et de la communication ; la révision des définitions technico-juridiques et le complément de la notion des télécommunications avec celle des technologies de l'information et de la communication, mieux adaptée à un contexte de convergence des réseaux et des services ; la redéfinition du régime de l'exploitant public en retirant toute idée de monopole et en ouvrant à la concurrence toutes les activités du secteur ; la généralisation, à l'exception du régime de l'exploitant public, à tous les exploitants du secteur des régimes applicables aux activités des télécommunications et des technologies de l'information et de la communication, qui sont fondés uniquement sur la nature des réseaux et services²⁸, la protection de la vie privée et des données à caractère personnel des utilisateurs de réseaux et de services des télécommunications et des technologies de l'information et de la communication²⁹.

2.1 Identification des dispositions pertinentes

La divulgation des données personnelles sans consentement préalable peut avoir des conséquences juridiques énormes, c'est-à-dire que le traitement de chaque information surtout personnelle doit se faire en toute légalité en observant scrupuleusement la loi sur le numérique, car au niveau de la sécurisation et la protection des données ; le responsable de traitement est tenu de prendre toutes les dispositions pour protéger les données et empêcher qu'elles soient détournées, réutilisées à des fins non prévues, afin de respecter l'intégrité et la confidentialité des données³⁰.

Il est important de relever les dispositions pertinentes relatives à la confidentialité de la communication et de la protection des abonnés ou utilisateurs.

En effet, le code du numérique prévoit les dispositions relatives à la cyber sécurité définie comme l'ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain et procédural ou autre permettant d'atteindre les objectifs de sécurité des systèmes informatiques et des réseaux de communication électronique et de garantir la disponibilité, l'intégrité, la confidentialité, l'authenticité ou la traçabilité des données stockées, traitées ou transmises et des services connexes³¹.

²⁸ *Exposé des motifs de la loi n° 20/017 du 25 Novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.*

²⁹ *Art 126 de la loi n° 20/017 du 25 Novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.*

³⁰ YENDE R. Grevisse, MADAWA K. Zéphyrin, MBAKWIRAVYO M. Osée, KASIMWANDE K. William, KAKULE L. Thierry et 6MAHASANO M. Emmanuel. « De la protection des données à caractère personnel des internautes en RDC » GSJ: Volume 8, Issue 5, May 2020, p.1889

³¹ *Art 2-25 de l'Ordonnance-Loi n° 23/010 du 13 mars 2023 portant Code du Numérique*
Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

2.2 Autres textes juridiques pertinents

Le code pénal (infractions liées à l'atteinte à la vie privée, cybercriminalité). L'article 153 de la loi n° 20/017 du 25 Novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication est très explicite au sujet de la cybercriminalité dans une perspective communicationnelle en RDC, cette disposition énumère ce qu'on entend par la cybercriminalité en ces termes : la cybercriminalité est constituée par l'un des faits énumérés ci-après :

- La pornographie infantile ;
- Le racisme ;
- La xénophobie ;
- Les atteintes portées notamment :
 - a) aux activités des prestataires de services de communication ouverts aux publics par voie électronique ;
 - b) à la publicité par voie électronique ;
 - c) à la prospection directe.)
- Les atteintes aux biens liés aux technologies de l'information et de la communication ;
- Les atteintes par tout moyen de diffusion publique ; les atteintes à la défense nationale ;
- Les atteintes à la confidentialité des systèmes informatiques ;
- Les atteintes à l'intégrité des systèmes informatiques ; les atteintes à la disponibilité des systèmes informatiques ; les atteintes aux données informatiques en général ; les atteintes spécifiques des données à caractère personnel.

2.3 La législation spécifique

Cette partie sera consacrée spécifiquement à l'analyse du cadre juridique existant en matière de protection des données personnelles et ses limites, car il sied de noter qu'en République Démocratique du Congo il y a déjà une législation spéciale (le code du numérique) en matière de protection des données personnelles.

Les États précurseurs en matière de protection des données personnelles, notamment les pays européens, ont d'abord adopté le principe de la libre circulation des données à caractère personnel au sein de l'Union européenne, tout en encadrant strictement les flux transfrontaliers de données vers des pays tiers ou des organisations internationales³².

³² Lire BENSOUSSAN Alain, Règlement européen sur la protection des données, Bruylant, 2017 ; PRÉVOST Stéphane et ROYER Erwan, Le RGPD, Dalloz, 2018.

Il est impérieux de noter que la maîtrise des données confère en effet un pouvoir stratégique considérable, influençant aussi bien les politiques publiques que les dynamiques économiques et sécuritaires³³.

Dans cette optique, le renforcement du système numérique et la mise en place d'une législation spécifique seraient une réponse favorable à l'efficacité et la sécurité des données à caractère personnel en RDC.

Malgré l'adoption de la loi relative aux communications électroniques et certaines dispositions éparses relatives à la vie privée dans la Constitution de la RDC en l'occurrence l'article 31.

Cependant la RDC ne dispose pas encore d'une loi-cadre moderne, complète et autonome spécifiquement dédiée à la protection des données à caractère personnel, cette absence entraîne des conséquences juridiques et pratiques majeures notamment le non-respect des données personnelles sur les réseaux sociaux.

L'absence d'une loi spécifique freine l'effectivité de la protection des droits fondamentaux, elle rend difficile la régulation des pratiques numériques, l'encadrement des plateformes en ligne, et la responsabilisation des entreprises technologiques.

En RDC, la protection des données personnelles reste encore embryonnaire, en raison du manque d'une législation dédiée et cohérente. Cette situation crée un vide juridique qui expose les citoyens à des abus sans réel moyen de recours³⁴.

Cette situation crée clairement la vulnérabilité des citoyens, le risque d'abus, l'impact sur l'e-gouvernement et l'e-commerce ou commerce électronique. Les citoyens congolais deviennent de plus en plus vulnérables face aux abus des acteurs publics et privés en subissant la collecte illégale de données, la surveillance abusive, ou l'exploitation commerciale sans consentement.

L'absence de loi claire fragilise également les initiatives d'e-gouvernement ou le gouvernement électronique, de digitalisation des services de l'État, et les ambitions de développement de l'e-commerce.

³³ On dit même que la donnée est le pétrole – « l'or noir » – de demain, une expression souvent attribuée au mathématicien et entrepreneur britannique Clive Humby. Voir ARTHUR Charles, « Tech giants may be huge, but nothing matches big data », The Guardian, 23 août 2013, [en ligne] <https://www.theguardian.com/technology/2013/aug/23/tech-giants-data> [consulté le 20 Septembre 2025].

³⁴ Dr. Mbuyi Kankonde, *Revue Congolaise de Droit Numérique*, 2022.

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

II. LES DEFIS JURIDIQUES ET TECHNOLOGIQUES POSES PAR L'ÉMERGENCE DU NUMERIQUE EN RDC

L'émergence du numérique en RDC s'accompagne d'une prolifération de plateformes technologiques, parmi lesquelles les réseaux sociaux (Facebook, TikTok, WhatsApp et autres), les services d'e-commerce (M-Pesa, Orange Money, airtel money), Ces plateformes sont de véritables canaux de collecte massive de données à caractère personnel³⁵, en effet, constitue une donnée à caractère personnel « toute information relative à une personne identifiée ou identifiable par un numéro d'identification, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.³⁶»

II.1 Diversité des données collectées (identitaires, comportementales, de localisation, financières).

Les données collectées sont souvent très variées : Données identitaires (nom, prénom, numéro de téléphone, adresse e-mail), données comportementales (clics, préférences, historique d'achat), données de géolocalisation (via GPS), données financières (via paiements mobiles et cartes bancaires³⁷),

II.2 Question de la territorialité du droit face aux données traitées à l'étranger.

La majorité des données des citoyens congolais transitent et sont traitées, stockées à l'étranger, notamment sur des serveurs situés en Europe, en Chine, en Asie ou en Amérique du Nord. Cela pose un défi de territorialité juridique, et un problème de droit se pose : Comment appliquer le droit congolais à des entreprises ou serveurs hors territoire national ? à ce propos le traitement des données à caractère personnel est défini comme « toute opération ou ensemble d'opérations effectuées à l'aide des procédés automatisés ou non et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la conservation, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission ou toute autre forme de la mise à la disposition, le rapprochement ou l'interconnexion ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel³⁸.

³⁵ Loi n° 22/063 du 15 septembre 2022 relative à la protection des données à caractère personnel

³⁶ *Idem*, Art 4

³⁷ Georges Mukuna, « La protection des données à caractère personnel en République Démocratique du Congo, » éd. Larcier Afrique, 2023

³⁸ Art 1-95 de la loi n° 20/017 du 25 Novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

Par exemple, une plateforme comme Facebook, en l'absence d'une représentation locale, échappe de fait à toute responsabilité juridique directe en RDC, malgré l'utilisation massive des données personnelles congolaises,

III.3 Intelligence artificielle, Big Data, objets connectés : défis en termes de consentement, d'anonymisation et de traçabilité.

L'avènement des technologies de l'intelligence artificielle et du Big Data en RDC impose une nouvelle approche juridique, car le consentement classique perd de sa pertinence face à la collecte massive et automatisée des données. La législation congolaise doit évoluer vers un modèle qui intègre les principes de transparence, d'accountability et de responsabilité renforcée des acteurs numériques³⁹.

Le premier et le plus fondamental des défis réside dans la désuétude du consentement classique. Face à la collecte massive, automatisée et souvent opaque des données par des algorithmes d'IA, le principe de l'«accord libre, spécifique, éclairé et univoque» devient une fiction juridique. L'utilisateur est incapable d'anticiper la diversité des traitements futurs et des recoupements de données que permettent ces technologies, rendant le consentement inefficace comme garantie réelle de l'autonomie individuelle.

Cette insuffisance du modèle basé sur l'individu appelle à une transition impérative vers un nouveau paradigme de conformité, centré sur le responsable de traitement. La législation congolaise doit évoluer pour intégrer pleinement les principes de transparence et d'Accountability (obligation de rendre compte). Il ne suffit plus d'avoir des règles ; les acteurs numériques doivent être contraints de démontrer de manière proactive et documentée le respect de ces règles, notamment par le biais de l'intégration de la protection des données dès la conception (Privacy by Design).

L'anonymisation de traitement ultérieur, bien que prévue par le code du numérique⁴⁰, reste un concept fragile dans un contexte où les techniques de recoupement des données deviennent de plus en plus sophistiquées. La protection des données personnelles ne peut se limiter à des prescriptions formelles sans un contrôle technique accru⁴¹.

II.4 Cyber sécurité : menaces de piratage, fuites de données, usurpation d'identité.

³⁹ Dr. Jean-Marc Lumbala, Professeur en droit numérique, Université de Kinshasa, *Revue Congolaise de Droit et Technologie*, 2021.

⁴⁰ Art 204 de l'Ordonnance loi N°23/10 du 13 Mars 2023 portant le code du numérique

⁴¹ Me Béatrice Mbuyi, Avocate spécialisée en droit des technologies, Colloque sur la protection des données en RDC, 2022.

Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

La RDC fait face à une multiplication des cybers attaques qui mettent en péril non seulement la sécurité des données, mais aussi la stabilité économique et sociale. L'adoption d'un cadre juridique intégré, combinant sanctions pénales et mesures préventives, est une urgence nationale⁴².

PERSPECTIVES ET RECOMMANDATIONS POUR UNE PROTECTION EFFICACE DES DONNEES PERSONNELLES EN RDC

Pour renforcer le cadre juridique congolais et protéger efficacement les données personnelles, plusieurs pistes peuvent être envisagées :

Le renforcement de l'ARPTIC et garantir son indépendance, doter cette autorité de moyens techniques et financiers suffisants, et renforcer ses pouvoirs de sanction.

L'adoption de textes complémentaires : développer des lois spécifiques sur l'intelligence artificielle, la cyber sécurité en intégrant des principes de responsabilité et d'éthique numérique.

Campagnes de sensibilisation : informer les citoyens et les entreprises sur leurs droits et obligations en matière de données personnelles, en formant également les acteurs judiciaires comme les magistrats, les forces de l'ordre et les Avocats dans les questions numériques.

L'harmonisation régionale et internationale : s'inspirer des standards internationaux (RGPD, recommandations de l'union internationale des communications) pour faciliter la coopération transfrontalière et l'intégration économique.

Promotion de solutions techniques : encourager l'utilisation de technologies respectueuses de la vie privée, comme le chiffrement et l'anonymisation avancée

⁴² Prof. André Mwamba, Expert en cybersécurité et droit, Journée Nationale de la Cybersécurité en RDC, 2020.
Alkain KALALA NSAMBI Licencié en Droit privé et Judiciaire de l'Université de Lubumbashi (Bac+5) équivalent de Master, Consultant et chercheur en Droit.

CONCLUSION

L'analyse de la protection des données personnelles en République Démocratique du Congo révèle un paradoxe stimulant. Face à l'irrépressible émergence technologique qui transforme l'administration, le commerce et les interactions sociales, la RDC a posé un jalon juridique fondamental : la promulgation du Code du Numérique. Cet instrument législatif témoigne d'une prise de conscience étatique quant aux enjeux soulevés par la collecte, le traitement et la circulation massifs d'informations à caractère personnel dans l'environnement numérique.

Le Code du Numérique constitue la pierre angulaire de la réglementation spécifique congolaise en la matière, cherchant à aligner le droit national sur les standards internationaux de protection.

Il introduit des concepts clés, tels que le consentement, le droit à l'oubli, et les obligations des responsables de traitement, offrant ainsi une base légale pour garantir aux citoyens le contrôle de leur sphère privée. Cette avancée est d'autant plus cruciale que l'économie numérique, moteur de croissance potentiel, ne peut se développer sainement sans la confiance des utilisateurs et la sécurité juridique des transactions.

Toutefois, l'existence d'un cadre normatif n'est qu'une première étape. La véritable protection des données personnelles dépend de sa mise en œuvre effective. Les défis sont considérables : ils incluent l'insuffisance des mécanismes de contrôle et de sanction, le déficit de sensibilisation du public et des acteurs économiques aux nouvelles exigences légales, et la nécessité de renforcer les capacités techniques et humaines des institutions chargées de l'application de la loi. L'absence d'une autorité de régulation des données dédiée, dotée de l'autonomie et des moyens nécessaires, représente un point de vulnérabilité majeur.

En définitive, si la RDC, par son Code du Numérique, a résolument embrassé le défi de la protection des données personnelles face à l'essor du numérique, le chemin vers une cyber-souveraineté juridique pleine et entière reste à parcourir.

L'urgence est désormais de passer de la proclamation normative à la concrétisation opérationnelle, en investissant dans l'éducation numérique, la structure de gouvernance et le renforcement des capacités de contrôle. C'est à cette seule condition que le citoyen congolais pourra jouir pleinement des opportunités de l'ère numérique sans sacrifier son droit fondamental à la protection de sa vie privée.

Le succès de la transition numérique de la RDC sera intrinsèquement lié à sa capacité à sécuriser ce nouveau trésor qu'est la donnée personnelle.