Augmentation des cyberattaques en RDC : Quelle réglementation pour lutter contre ce fléau ?

N. DJUMA SOSTHENE,

Apprenti Délégué à la protection des données chez Conforama France
Étudiant en Master 2 Droit des données, des administrations numériques et des gouvernements ouverts à Université Panthéon-Sorbonne Paris 1
Mastère spécialisé en droit de la propriété intellectuelle et du numérique à l'Institut supérieur du droit à Paris

1 - Plusieurs pays à travers le monde sont confrontés aux cybermenaces[1]. La République démocratique du Congo, à l'instar de nombreux autres pays africains, subit fréquemment des cyberattaques dans le système informatique de l'administration. Selon la dernière édition du rapport Security Navigator d'Orange Cyberdefense, les cyberattaques pourraient engendrer une perte de 10 % du PIB pour le continent africain, avec une augmentation de 70 % des cas d'extorsion en 2023. Ces chiffres pourraient néanmoins être en deçà de la réalité.[2] Dans la plupart des situations, il y a une difficulté notable quant à l'identification des personnes derrière ces attaques informatiques.

2 - Face à ces menaces numériques croissantes, une réponse juridique renforcée s'impose pour maintenir l'ordre dans l'usage des outils informatiques et déterminer la responsabilité des auteurs qui se livrent à des actes de cyberattaque. Afin de mieux comprendre la gestion juridique des cyberattaques, il faudra tout d'abord parler du fléau des cyberattaques en RDC (A), faire une analyse de la législation congolaise sur les cyberattaques (B).

A. Fléau des cyberattaques en RDC

3 - Il est essentiel d'évaluer l'ampleur et l'impact des cyberattaques sur les systèmes informatiques en République Démocratique du Congo, en mettant particulièrement l'accent sur les institutions publiques (2). Cependant, avant cette analyse, il convient d'établir une distinction entre cyberattaque et cybercriminalité (1).

1. Différence entre cyberattaque et cybercriminalité

4 - Le concept de cyberattaque est défini par l'article 4 de la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication en République Démocratique du Congo (RDC). Selon cette loi, une cyberattaque se caractérise par des « actes malveillants de piratage informatique dans le cyberespace », englobant des activités telles que la désinformation, l'espionnage électronique, la modification clandestine des données sensibles ou la perturbation des infrastructures critiques d'un pays. Cette définition, bien que détaillée, reste dans une perspective essentiellement fonctionnelle et opérationnelle.

Par contraste, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France propose une définition qui met l'accent sur la nature coordonnée des attaques : une cyberattaque est un « ensemble coordonné d'actions menées dans le cyberespace visant des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité ». Cette définition souligne la dimension organisée et structurée des cyberattaques, ainsi que leur impact sur les trois aspects fondamentaux de la sécurité de l'information : la disponibilité, l'intégrité, et la confidentialité.[3]

5 - En comparaison, le terme cybercriminalité se réfère à l'ensemble des infractions commises via le cyberespace, incluant des activités illégales telles que le vol de données personnelles, la diffusion de logiciels malveillants, le sabotage, et l'espionnage industriel. La cybercriminalité est donc une catégorie plus large qui englobe diverses formes de délits numériques. Tandis qu'une cyberattaque est un acte spécifique, souvent ciblé, visant à compromettre la sécurité d'un système ou d'une infrastructure, la cybercriminalité est le champ d'application de ces actes, dans un cadre plus général de criminalité.

[1] CARTE. (s. d.). *Carte des cybermenaces en temps réel*. Kaspersky. Disponible en ligne : https://cybermap.kaspersky.com/fr

[2] En Afrique, la menace cyber enfle au rythme de la digitalisation. (s. d.). *Les Échos*. Disponible en ligne : https://www.lesechos.fr/thema/articles/en-afrique-la-menace-cyber-enfle-au-rythme-de-la-digitalisation-2085287

[3] Glossaire. (s. d.). *Agence nationale de la sécurité des systèmes d'information*. Disponible en ligne https://cyber.gouv.fr/glossaire

2. Étude de Cas : Deux Cyberattaques réalisées contre des Institutions Publiques

6 - En janvier 2021, le site de la Société Nationale d'Électricité (SNEL) a été la cible d'une cyberattaque, le rendant inaccessible. Cet acte a été attribué à des Congolais mécontents des interruptions intempestives de l'électricité. Les auteurs de cette cyberattaque promettaient de passer à un niveau supérieur en piratant également les turbines et les centrales électriques. Cela a suscité la réaction notamment de Dominique MIGISHA[4], Coordonnateur de l'Agence pour le Développement du Numérique, qui a déclaré : « *Le piratage en cours du site de la SNEL est à condamner et il faut poursuivre les auteurs. C'est clair que la RDC doit rapidement se doter d'une structure pour encadrer le développement du Numérique (Normes, textes légaux, protection des données, sécurité, etc.)*. »

À travers sa réaction, deux éléments essentiels ressortent. Premièrement, Dominique MIGISHA mettait en lumière l'absence partielle de textes législatifs spécifiques régissant la protection et la sécurité des données. Et deuxièmement, un appel d'urgence à la mise en place d'un cadre juridique clair pour de telles infractions. S'il faut le rappeler, en droit pénal et comme le souligne l'article 17 alinéa 2 de la Constitution[5] de la RDC révisée en 2011 : « Nul ne peut être poursuivi, arrêté, détenu ou condamné qu'en vertu de la loi et dans les formes qu'elle prescrit. ». Ce texte pose un principe essentiel du droit pénal, celui de légalité des délits et des peines qui dispose qu'on ne peut être condamné pénalement qu'en vertu d'un texte pénal précis et clair (en latin, Nullum crimen, nulla pœna sine lege, c'est-à-dire « [il n'y a] aucun crime, aucune peine, sans loi »). En 2021, le Code du numérique dont nous parlerons en large ultérieurement n'existait pas encore. Il y avait cependant un Plan National du Numérique « Horizon 2025 ».[6]

7 - En décembre 2023, pendant la période électorale, la Commission Électorale Nationale Indépendante (CENI) a annoncé avoir été la cible de plusieurs tentatives d'intrusion informatique.[7] Denis KADIMA, président de la CENI, avait informé que l'institution avait enregistré 3.244 cyberattaques la veille des élections. Ces tentatives ont été repoussées à l'aide d'un système de sécurité informatique adéquat. Selon certaines révélations, l'un des candidats à la course présidentielle aurait tenté de pirater le serveur de la CENI via une organisation russe.[8] L'objectif derrière une cyberattaque étant généralement la volonté de rendre les informations du système d'information indisponibles, de violer leur intégrité (comme la falsification des résultats de vote) ou à compromettre leur confidentialité.

B. Analyse de la législation congolaise sur les cyberattaques

8 - À l'ère numérique, les cyberattaques sont devenues une menace omniprésente, touchant les individus, les entreprises et les gouvernements à travers le monde. En République Démocratique du Congo, comme dans beaucoup d'autres pays, la montée en puissance de ces cybermenaces a conduit à la nécessité de développer des cadres juridiques adaptés pour les contrer efficacement (2). Cela marque un tournant significatif par rapport à la période antérieure, marquée par un manque de réponse juridique (1).

1. Approche historique de la législation

9 - Au fil du temps, les infractions liées à l'informatique ont longtemps souffert d'un manque de régulation juridique détaillée. Cette absence quasi totale de textes spécifiques a contribué à la création d'une véritable zone de « vide juridique[9] ». Mais, à travers le temps, le législateur congolais a tenté de légiférer sur les actes infractionnels réalisés ou facilités par l'usage des outils informatiques[10].

À cet effet, on peut citer par exemple l'Ordonnance 87-243 du 22 juillet 1987 portant réglementation de l'activité informatique en République du Zaïre[11]. Qui dispose à son article 9 : « *Tout acte accompli à l'occasion d'une application informatique et qui porte atteinte à la sécurité de l'État, à l'ordre public ou aux bonnes mœurs, est punissable conformément aux lois pénales en vigueur* ». Et à son article 12,

[4] Migisha, D. (2021, 27 janvier). Réaction issue du compte X de Dominique Migisha. Disponible en ligne https://x.com/migishaofficiel/status/1353320320606863360

[5] Constitution de la République démocratique du Congo, modifiée par la Loi n° 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006

[6] Présidence de la République Démocratique du Congo. (s. d.). *Plan national du numérique Horizon 2025*. Disponible en ligne : https://www.presidence.cd/services/1/plan_national_du_numerique_horizon_2025

[7] Élections en RDC : des milliers de tentatives de piratage sur le site de la Commission électorale nationale indépendante. (2023, 20 décembre). *La Libre*. Disponible en ligne : https://www.lalibre.be/international/afrique/2023/12/20/elections-en-rdc-des-milliers-de-tentatives-de-piratage-sur-le-site-de-la-commission-electorale-nationale-independante-TBJHVKCY2VB5ZAUYUCHBO3DFNY/

[8] Révélations graves : Katumbi aurait tenté de pirater le serveur de la CENI via une organisation russe - Enquete.cd. (s. d.). Enquete.cd. Disponible en ligne : https://enquete.cd/2023/12/18/revelations-graves-katumbi-aurait-tente-de-pirater-le-serveur-de-la-ceni-via-une-organisation-russe/

[9] Le vide juridique est une notion qui désigne l'absence de normes applicables à une situation donnée.

[10] Panza, J., & Kandolo, B. (2024). « L'histoire du numérique et ses défis réglementaires en République Démocratique du Congo ». *Droit-Numérique.cd, Dossier n° 1*, juillet 2024, pp. 1-9. Article disponible en ligne : https://droitnumerique.cd/lhistoire-du-numerique-et-ses-defis-reglementaires-en-republique-democratique-du-congo/

[11] Ordonnance n° 87-243 du 22 juillet 1987 portant réglementation de l'activité informatique en République du Zaïre. Disponible en ligne : https://www.leganet.cd/Legislation/Droit%20administratif/SP/O.87.243.22.07.1987.htm

alinéa 2 : « *Toute manœuvre visant intentionnellement à détruire totalement ou partiellement la banque de données ou à s'approprier frauduleusement des informations qu'elle recèle, est punissable conformément à la législation pénale en vigueur.* »

À la lecture de ces dispositions, on peut percevoir notamment les prémisses de la volonté du législateur congolais de l'époque d'ériger en infraction l'intrusion dans un système informatique contenant les données au point de les rendre indisponibles. Le renvoi au Code pénal congolais démontre que c'est le cadre répressif général qui s'applique. Étant général et datant de 1940, le Code pénal devant instituer les délits et les peines a longtemps montré ses limites sur le numérique. Il n'a pas intégré rapidement les nouveaux modes de commission d'infractions.

10 - La République Démocratique du Congo n'est pas démunie de dispositions légales concernant la cybercriminalité. La loi-cadre n° 013/2002 du 16 octobre 2002 sur les télécommunications prévoyaient des infractions et des peines en rapport avec la divulgation illicite de correspondances transmises par ondes, protégeant ainsi les données personnelles dans les réseaux téléphoniques.[12] Cependant, cette loi a été entièrement abrogée en 2020 par la loi n° 20/017 du 25 novembre 2020 sur les télécommunications et les technologies de l'information et de la communication.

11 - La loi de 2020 sur les télécommunications et les technologies de l'information et de la communication, à son article 153, criminalise les atteintes à la confidentialité, à l'intégrité, à la disponibilité des systèmes informatiques, ainsi qu'aux données informatiques en général et aux données personnelles spécifiques. Cependant, pour compléter la régulation en matière de télécommunications, l'introduction d'un code du numérique s'avère nécessaire.

2. Le cadre répressif des cyberattaques dans le Code du numérique

12 - Le 13 mars 2023 a été marqué par la promulgation de l'ordonnance-loi n°23/010 portant sur le Code du numérique, dit : « *la loi KOLONGELE* ». Ce texte vient combler les lacunes juridiques des anciens textes dans le domaine du numérique, c'est également un texte de base et de référence pour les questions liées au numérique.

Le Code du numérique, notamment dans son Titre IV, qui traite de la protection pénale des systèmes informatiques, fournit des précisions sur les infractions spécifiques au domaine numérique. En particulier, le Chapitre 3 de ce titre définit les incriminations et les peines associées aux cyberattaques.

L'article 332, alinéa 1, du Code du numérique érige en infraction l'accès illicite à un système informatique. L'accès illicite dont il est question ici pourrait être perpétré au moyen d'une cyberattaque, est ainsi défini : « *Quiconque accède ou se maintient frauduleusement et sans droit, dans l'ensemble ou partie d'un système informatique, avec une intention frauduleuse est puni d'une peine de servitude pénale de trois à cinq ans et d'une amende de cinquante millions à cent millions de francs congolais, ou de l'une de ces peines seulement. […].* »

L'article 333 complète les dispositions de l'article 332 en introduisant des peines renforcées pour les infractions entraînant des dommages aux données ou au système informatique. Si l'accès illicite engendre des violations de l'intégrité des informations — telles que l'altération, la modification ou la destruction des données — les sanctions sont augmentées. L'article précise : « *Lorsqu'il résulte des faits visés à l'article précédent la suppression, l'obtention ou la modification de données contenues dans le système informatique, ou une altération du fonctionnement de ce système, les peines sont augmentées à cinq à dix ans de servitude pénale et une amende de cent millions à trois cents millions de francs congolais, ou de l'une de ces peines seulement.* ».

En cas de violation des mesures de sécurité, les sanctions sont encore plus sévères : « *Si les faits visés à l'article précédent sont commis en violation de mesures de sécurité, l'auteur est puni d'une peine de servitude pénale de dix à vingt ans et d'une amende de trois cents millions à cinq cent cinquante millions de francs congolais, ou de l'une de ces peines seulement.* ».

Conclusion

13 - Dans de nombreux cas de cyberattaques touchant les entreprises privées et les institutions publiques congolaises, il est fréquent que les enquêtes, lorsqu'elles sont réalisées, n'aboutissent à aucune suite concrète. Un exemple récent est celui du site Internet du ministère de l'Enseignement Supérieur et universitaire. Le site a été à ce qui a plus ressemblé à une cyberattaque, sans en être une dans le vrai sens du mot, il était question d'une erreur humaine.[13] Durant plusieurs heures, le 7 juillet 2024, le site Internet

[12] Ndukuma Adjay, K. (2020, 23 mai). « Cybercriminalité en RD Congo : Faire du vieux avec du neuf, pour un renouveau sans révolution ». *Zoom Eco*. Disponible en ligne : https://zoom-eco.net/wp-content/uploads/2020/05/V4-Article-Cybercrime-Dr-Kodjo-Mai-2020.pdf

[13] Kalonji, T. (2024, 8 juillet). « Piratage du site de l'ESU : que s'est-il vraiment passé ? », *TDK*. Disponible en ligne : https://tresorkalonji.pro/2024/07/piratage-du-site-de-l-esu-que-s-est-il-vraiment-passe.html

www.minesu.gouv.cd/ du ministère de l'Enseignement supérieur et universitaire congolais présente une image d'une jeune dame à moitié habillée et un message en indonésien faisant la promotion d'un service de loterie.

Le ministère de l'Enseignement Supérieur et universitaire, étant potentiellement en possession de données personnelles sensibles telles que celles des étudiants, du personnel universitaire et des fonctionnaires, ainsi que d'autres informations confidentielles[14], aurait dû émettre un communiqué officiel. Ce communiqué aurait permis de clarifier la situation, d'informer le public des potentielles implications, et de fournir des directives sur les mesures à prendre en cas de violation de données personnelles. Même si aucune atteinte substantielle n'a été constatée, la transparence est cruciale, surtout dans le contexte de la mise en place de l'écosystème d'e-Gouvernement et d'e-Administration en RDC.[15]

Pour remédier à ces lacunes, la création de l'Agence Nationale de Cybersécurité (ANCY), comme le prévoient les articles 275 à 280 du Code du numérique, apparaît comme une solution essentielle vers la mise en œuvre effective de la Stratégie nationale de Cybersécurité[16]. L'ANCY sera chargée de réguler la cybersécurité et la sécurité des systèmes d'information à l'échelle nationale. Elle devra collaborer avec les structures en charge de la protection des données personnelles, de la lutte contre la cybercriminalité et de la cyberdéfense militaro-sécuritaire. Ce dispositif vise à assurer une coordination efficace et à renforcer les efforts de protection du cyberespace congolais. Cependant, il est important de noter qu'à ce jour, l'ANCY n'a pas encore été établie.

[14] Ordonnance n°22/003 du 7 janvier 2022 fixant les attributions des ministères

[15] eGov de la RDC - Ministre du Numérique RD Congo. (s. d.). Ministère du Numérique RD Congo. https://numerique.gouv.cd/actualites/egov-de-la-rdc-ebt5ey

[16] Présidence de la RDC, « La stratégie nationale de la Cybersécurité », disponible en ligne : https://www.presidence.cd/uploads/files/Strategie%20Nationale%20de%20Cybers%C3%A9curit%C3%A9.pdf

Droit Numérique.cd

Droit-Numerique.cd est un cadre d'études dédié à l'analyse, la réflexion et la diffusion des connaissances juridiques relatives aux enjeux du numérique en République démocratique du Congo. Nous sommes enregistrés sous le numéro SIREN 931152144.

Pourquoi nous contacter ?

Partenariats

Collaborons pour renforcer l'écosystème numérique en RDC.

Consultations juridiques

Obtenez des conseils sur les questions légales liées au numérique.

Participation

Nous pouvons contribuer dans vos études, séminaires, et autres activités.

Suggestions

Partagez vos idées ou proposez des sujets que vous aimeriez voir abordés

contact@droitnumerique.cd

+ 33 6 05 50 17 84

www.droitnumerique.cd