M.E.S., Numéro 123, Juillet – Septembre 2022
https://www.mesrids.org
Dépôt légal : MR 3.02103.57117
N°ISSN (en ligne) : 2790-3109
N°ISSN (impr.) : 2790-3095
Mise en ligne le 30 juin 2022

Revue Internationale des Dynamiques Sociales

Mouvements et Enjeux Sociaux

Kinshasa, juillet - septembre 2022

NECESSITE DE LA REPRESSION DES ATTEINTES CONTRE LA CONFIDENTIALITE, L'INTEGRITE ET LA DISPONIBILITE DES DONNEES ET SYSTEMES INFORMATIQUES EN RDC

par

Bernard LETA LETA
Assistant, Faculté de Droit, Université de Kinshasa

Pierre SHINDANO BULENGE
Avocat général au Parquet près la Cour d'Appel de Kinshasa/Gombe

Adrien MUAKUILAYI KAMAYI
Assistant à la Faculté de Droit de l'UNIKIN
(Tous) Apprenants en DES/DEA, Université de Kinshasa

Résumé

Cette étude participe, dans une petite portion, à l'évolution du droit pénal congolais, en le rendant capable de relever les défis lancés par la cybercriminalité en matière de protection des données et systèmes informatiques et de lui permettre d'être à la page avec l'évolution de la technologie de l'information et de communication.

Cette analyse alerte le législateur congolais sur le danger que présente la cybercriminalité, en général, et des atteintes contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques en particulier, en lui suggérant quelques moyens pour combattre ces infractions nées de la révolution informationnelle.

Abstract

This study contributes, in a small portion, to the evolution of Congolese criminal law, by making it capable of meeting the challenges posed by cybercrime in terms of data protection and computer systems and allowing it to be up to date with developments in information and communication technology.

This analysis alerts the Congolese legislator to the danger presented by cybercrime, in general, and attacks on the confidentiality, integrity and availability of data and computer systems in particular, by suggesting some means of combating these offenses arising from the information revolution.

Mots-clés : *Repression des atteintes, confidentialite, disponibilite des donnees, systemes informatiques, RDC*

INTRODUCTION

Aujourd'hui, le recours aux réseaux numériques et en particulier à l'Internet est une arme à double tranchant, faite de perspectives positives mais aussi de risques et de menaces pesant sur l'activité des Etats, des entreprises et sur la vie quotidienne des citoyens qui sont très souvent des internautes[1].

Nous traitons cette question en deux points : le premier débat des concepts opératoires et le second examine des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques. Une très brève conclusion met un terme à cette étude.

[1]M. QUEMENER, ***cybermenaces, entreprises et internautes***, enonomia, Paris, 2008, p.1.

I. ANALYSE DES CONCEPTS OPERATOIRES

Il nous revient de bien circonscrire les significations de quelques concepts qui soutiennent la présente réflexion. Il s'agit de quelques valeurs à protéger dans le cyberespace et des techniques de perpétration des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques et leurs auteurs.

1.1. Quelques valeurs à protéger dans le cyberespace

Le concept de cyberespace est emprunté à un roman de science-fiction de William Gibson écrit en 1984, en l'occurrence « Neuromancer » (le neuromancien), dans lequel il utilise le concept de cyberespace pour désigner un espace utopique et abstrait où circule l'information[2].

Cet espace renferme des notions et valeurs qu'il faut protéger juridiquement, nous avons notamment les données informatiques et les systèmes informatiques (1), la confidentialité, l'intégrité et la disponibilité (2) comme valeurs importantes dans cet espace.

1.1.1. Données et Systèmes informatiques

Ce sont des notions très importantes en informatique et dans le cadre de notre réflexion, d'où tout intérêt pour nous de traiter des données informatiques (a) et des systèmes informatiques (b).

- ***Données informatiques***

D'après la convention sur la cybercriminalité, par donnée informatique, on entend, toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction[3].

- ***Systèmes informatiques***

Au sens de la convention, par système informatique, il faut entendre, tout dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé des données numériques ; il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau[4].

1.1.2. La confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Comme nous l'avons noté ci-haut, ce sont des valeurs qu'il faut protéger dans le cyberespace dont la confidentialité, l'intégrité et la disponibilité.

- ***La confidentialité***

La confidentialité est le caractère de ce qui doit rester secret, par exemple respecter la confidentialité du courrier ou encore la préservation du caractère secret, comme par exemple, le fait d'assurer la confidentialité des données[5].

---

[2] M. KALONJI, ***notion de cybercriminalité : praxis d'une pénalisation de la délinquance électronique en droit pénal congolais,*** p. 6 disponible sur www.tgk.centerblog.net (consulté le 25 Mars 2013).
[3] Article 1 pt. b de la convention sur la cybercriminalité.
[4] Rapport explicatif, ***op.cit***.
[5] Voir Microsoft® Encarta® 2009. © 1993-2008 Microsoft Corporation.

C'est le maintien du secret de l'information. En tant que critère de sécurité, la confidentialité est la protection des données contre une divulgation non autorisée[6].

- ***L'intégrité***

L'intégrité est définie par le *dictionnaire Encarta* comme l'état de ce qui n'a subi aucune altération, aucun dommage ou aucune diminution ou encore une qualité consistant à conformer ou à être conforme à ce que commandent le devoir et la conscience morale[7]. Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle)[8].

- ***La disponibilité***

Elle permet de maintenir le bon fonctionnement du système d'information. L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources[9]. La disponibilité d'une ressource qualifie le fait qu'elle peut être utilisée pour rendre le service pour lequel elle a été conçue.

1.2. Techniques de perpétration des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques et leurs auteurs

Destinés à porter atteinte aux biens d'une technologie de pointe ou à s'en servir pour perpétrer les crimes, les cybercrimes relèvent d'une grande ingéniosité dont les techniques sont plutôt modernes et ne se ressemblent guère à celles des crimes traditionnels[10].

1.2.1. Techniques de perpétration des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques

Comme le titre l'indique clairement, nous nous focalisation sur les techniques de perpétration de la cybercriminalité qui facilitent la commission des infractions que nous analysons plus bas.

- ***Les infections informatiques portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques***

Un expert en sécurité informatique, Eric Filiol, définit une infection informatique comme « un programme simple ou autoreproducteur, à caractère offensif, s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ce système ou susceptible d'incriminer à tort son possesseur ou l'utilisateur dans la réalisation d'un crime ou d'un délit »[11].

- ***Les infections simples***

Un programme simple contient une fonctionnalité malveillante cachée qui est appelée à se déclencher à un instant donné, sur un critère donné. Il n'y a pas propagation. Ce programme doit être introduit (volontairement ou non) dans l'ordinateur ciblé. On le retrouvera en seul exemplaire. Lorsque l'utilisateur exécute le programme, la fonctionnalité malveillante (PAYLOAD) s'exécute immédiatement. Une action destructive ou simplement perturbatrice est alors mise en œuvre. Selon son but, elle sera visible ou non par l'utilisateur. Une fois l'action accomplie, le programme se termine. Il

[6] S. GHERNAOUTI-HELIE, ***op.cit***, p.33.
[7] Idem
[8] Voir sur http://www.commentcamarche.net/contents/secu/secuintro.php3, consulté le 14 Avril 2013.
[9]Idem.
[10] M. N'KUSU KALEBA, idem, p.71.
[11] FILIOL (Eric), ***Les virus informatiques : théorie, pratique et applications***, Ed. Springer, 2004, p.79 et s.

n'est généralement pas résident en mémoire. Dans cette catégorie, on distingue : les bombes logiques, les chevaux de Troie, les bombes ANSI, les logiciels espions (spyware), les canulars informatiques et les accès dissimulés[12].

- ***Les infections autoreproductrices***

Il existe une quantité phénoménale des programmes indésirables. Tous ces programmes portent le nom de « malware ». Mais sous cette appellation, se cachent des familles bien différentes les unes des autres. La majorité des malwares récents sont en fait une combinaison des protocoles possibles, fait des malwares un risque élevé pour tout ordinateur ayant accès à l'internet[13]. Nous avons notamment les virus, les vers, etc.

- ***Les attaques cybernétiques portant atteinte à la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques***

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Cette dernière peut être définie comme l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables[14].

- ***Les attaques cryptographiques[15]***

Il existe trois types d'attaques cryptographiques dont l'attaque des mots de passe, l'attaque man in the middle et l'attaque par rejet.

- ***Les attaques par déni de service***

Ces attaques sont de deux catégories dont les dénis de service simple (Dos), utilisant soit des vulnérabilités précises du système d'exploitation, soit utilisant des techniques plus génériques comme le SYN flood ; les dénis de service distribués (DDos), utilisant un grand nombre de serveurs compromis sur lesquels tournent des programmes « Zombies » attendant les instructions de ceux qui les ont implantés et qui les contrôlent à distance[16]. Ils existent six formes de ces attaques: le déni de service proprement dit[17], la technique dite par réflexion[18], l'attaque par fragmentation[19], l'attaque du Ping de la mort, l'attaque LAND et l'attaque SYN.

1.2.2. Les auteurs des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques

Nous ne les voyons pas, nous ne les connaissons pas, nous ne nous en méfions pas et c'est leur force. Pourtant, nous sommes tous concernés[20].

Il existe un bon nombre des personnes qui sont à la base des infractions commises dans le cyberespace et parmi elles, se trouvent les personnes physiques ou individus, les Etats et les personnes morales autres que les Etats. Mais dans le cas qui nous concerne, nous mettons plus l'accent sur les personnes physiques dont les vandales, les hackers et

[12] M. KALONJI, ***op.cit***, p. 16.
[13] ARNAUD Jacques, cité par MANASI, ***op.cit***, p.86.
[14] Idem, p.86.
[15] ibidem, pp.74-75
[16] M. QUEMENER, ***op.cit***, p.77.
[17] idem
[18] ibidem
[19] ibidem
[20] S. GHERNAOUTI-HELIE, ***op.cit***, p.9.

les espions parce que ce sont elles les auteurs des infractions portant atteinte à la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques[21].

II. ANALYSE DES INFRACTIONS PORTANT ATTEINTE A LA CONFIDENTIALITE, A L'INTEGRITE ET A LA DISPONIBILITE DES DONNEES ET SYSTEMES INFORMATIQUES

Il nous parait important d'identifier les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, c'est-à-dire nous analysons l'accès illégal dans un système informatique et l'interception illégale des données informatiques et l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et l'abus de dispositifs, ainsi que les possibilités de leur intégration en droit pénal congolais.

Nous tenons à préciser une chose, notre analyse se fera en fonction des infractions telles prévues dans la convention sur la cybercriminalité du 23 novembre 2001 du Conseil de l'Europe et nous pouvons aussi de temps à temps, recourir aux droits pénaux étrangers évolués en à la matière, cela pour une bonne et simple raison que toutes ces infractions ne sont pas réprimées en droit pénal congolais, et même le résultat des recherches du professeur Manasi va nous permet d'affirmer cela.

2.1. Analyse de l'accès illégal et de l'interception illégale

Sur ce point, nous analysons tour à tour l'accès illégal (1) et l'interception illégale (2) en donnant la définition de chacune d'elle, leurs éléments constitutifs et en proposant leur intégration dans le code pénal congolais.

2.1.1. L'Accès illégal dans un système informatique

Comme nous l'avons indiqué ci-haut, nous en donnerons la définition en nous référant à la convention sur la cybercriminalité et en faisant ressortir ses éléments constitutifs (a) et nous essayerons de proposer son intégration dans le code pénal congolais (b).

- ***Définition***

D'après l'article 2 de la convention sur la cybercriminalité, l'accès illégal est « l'accès intentionnel et sans droit à tout ou partie d'un système informatique. » Donc, il consiste dans les intrusions non autorisées dans des systèmes informatiques appartenant à une autre personne que le pirate. Dans la majorité des Etats comme la Belgique, il est connu sous le jargon de « *hacking* ».

- ***Eléments constitutifs***

Ici, nous faisons sortir ces éléments en référence de la définition donnée par la convention sur la cybercriminalité parce que comme l'affirme Ndukuma, cette convention est jusqu'à ces jours, le seul instrument de référence à vocation universelle clairement affichée[22], et aussi, il n'y a aucune loi en RDC qui réprime ces infractions.

- ***Elément légal***

Dans le cadre de cette réflexion, c'est l'article 2 de la convention sur la cybercriminalité qui dispose que « *Chaque Partie adopte les mesures législatives et autres qui*

[21] M. N'KUSU KALEBA, ***op.cit***, p. 100.
[22] N. NDUKUMA, ***cyberdroit, télécoms, internet, contrats de e-commerce. Contribution au droit congolais***, PUC, Kinshasa, 2009, p.327.

se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique.

Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.[23]»

- ***Eléments matériels***

Sur ce point, nous indexons le fait extérieur par lequel l'infraction se révèle ou le fait pour lequel l'infraction prend corps[24]. Dans le cas d'espèce, l'accès illégal est une infraction de commission, c'est-à-dire qu'elle exige un acte positif[25] pour sa commission.

En ce qui concerne l'accès illégal, l'élément matériel est l'accès dans un système informatique donc cela nécessite une pénétration matérielle dans toute ou partie du système informatique, son élément matériel se définit par rapport à un procédé[26], nous pensons aussi que dans le cas où il y a accès, le pirate doit se maintenir dans ce système pour que cette infraction soit retenue.

L'accès comprend la pénétration dans l'intégralité ou une partie quelconque d'un système informatique (matériel, composants, données stockées du système installé, répertoires, données relatives au trafic et au contenu). Toutefois, il ne comprend pas le simple envoi de message électronique ou de fichiers au système en question. L'accès comprend la pénétration dans un autre système accessible par les réseaux de télécommunications publics ou d'un système informatique connecté au même réseau, tel qu'un réseau local ou un intranet (réseau privé d'une entreprise). Le mode de communication (par exemple à distance, y compris le sans-fil, ou rapprochée) n'entre pas en ligne de compte[27].

En parlant de l'accès, on vise ici toutes les modalités de pénétration irrégulières d'un système informatique, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication où il ne lui est pas permis l'accès.

- ***Elément intellectuel***

C'est la conscience chez le délinquant que l'accès ne lui ait pas autorisé, en quelque sorte, son élément moral résulte de l'expression « sans droit ». Même si on ajoutait l'adverbe frauduleux comme nous l'avons proposé, il ne pourrait constituer un dol général de l'attitude volontaire, ni un dol très spécial de l'intention de nuire.

- ***Possibilité de l'intégration de l'accès illégal dans le droit pénal congolais***

Dans le souci de voir notre droit pénal évolué dans le temps avec tous les changements plus précisément l'évolution de la technologie avec l'avènement des nouvelles technologies de l'information et de la communication, nous proposons l'ajout dans le code pénal congolais de l'accès illégal dans un système informatique.

Le législateur congolais peut s'inspirer de l'expérience étrangère en complétant son code pénal soit à la manière du législateur Belge qui réprime à l'article 550bis.

[23] Article 2 de la convention du conseil de l'Europe sur la cybercriminalité.
[24] NYABIRUNGU, M.S, ***Traité de droit pénal général congolais***, 2eme éd., EUA, Kinshasa, 2007, p.201.
[25] Idem.
[26] M. QUEMENER, ***op.cit.***, p.92.
[27] Idem.

Le législateur congolais peut insérer une nouvelle disposition pour réprimer cette infraction en disposant que :

> « *Quiconque sachant qu'il ne lui ait pas permis l'accès à un système informatique, s'introduit frauduleusement et s'y maintien sera puni d'une servitude pénale de deux mois à un an et d'une amende de 100.000 francs congolais ou l'une de ces peines seulement.*
>
> *Quiconque commettra l'infraction prévu à l'alinéa premier de cette disposition, avec l'intention de nuire en outrepassant son pouvoir d'accès à un système informatique, sera puni d'une servitude pénale de quatre mois à 2 ans et d'une amende de 200.000 francs congolais ou d'une de ces peines seulement.* »

2.1.2. L'interception illégale des données informatiques

- *Définition :*

C'est l'article 3 de la convention citée ci-haut qui définit l'interception illégale en ce sens que c'est « l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Elle peut être commise soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique[28].»

- ***Eléments constitutifs***

- *Elément légal*

Comme nous l'avons déjà dit dans la définition, c'est l'article 3 de la convention sur la cybercriminalité qui réprime cette infraction en disposant que « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.*[29]»

- ***Elément matériel***

L'élément matériel consiste dans le fait d'intercepter des données informatiques pendant qu'elles sont en train d'être transmises. L'interception effectuée par des moyens techniques concerne l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu soit directement, au moyen de l'accès au système informatique et de son utilisation, soit directement, au moyen de l'emploi des dispositifs d'écoute[30].

- ***Elément intellectuel***

[28] Article 3 de la convention sur la cybercriminalité de 2001.
[29] Idem.
[30] Rapport, ***op.cit***.

L'élément moral résulte de la disposition même qui réprime l'infraction, c'est l'intention qu'a le délinquant d'intercepter les données informatiques en sachant qu'il ne lui ait pas permis de le faire.

2.1.3. Possibilité de son intégration dans le droit pénal congolais

En ce qui concerne l'interception illégale, elle est en partie réprimée en RDC dans la loi cadre sur les télécommunications, plus précisément dans sa partie concernant l'interception les correspondances et communications qui sont des données, mais la partie des données informatiques reste impunie. Voilà pourquoi, nous suggérons législateur congolais l'intégration d'une disposition dans le code pénal de la RDC qui réprimera cette infraction dans son ensemble, en ces termes :

> « *quiconque aura intentionnellement intercepter sans autorisation par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, sera puni d'une servitude pénale de six mois à 2 ans et d'une amende de 200.000 francs congolais ou l'une de ces peine seulement.*
>
> *Lorsqu'elle est commise avec une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique, le délinquant sera puni du double de la peine prévue ci-haut.* »

III. ANALYSE DE L'ATTEINTE A L'INTEGRITE DES DONNEES, DE L'ATTEINTE A L'INTEGRITE DU SYSTEME ET L'ABUS DE DISPOSITIFS

3.1. L'atteinte à l'intégrité des données et l'atteinte à l'intégrité du système

3.1.1. L'atteinte à l'intégrité des données

Comme pour les infractions précédentes, nous donnerons la définition selon la convention sur la cybercriminalité où nous faisons ressortir les éléments constitutifs.

- *Définition :* La convention sur la cybercriminalité définie l'atteinte à l'intégrité des données comme le fait intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

- *Eléments constitutifs*

Il s'agit ici de la base légale, de l'élément matériel et de l'élément moral qui feront l'objet de ce point.

- *Elément légal* **:** c'est l'article 4 de la convention sur la cybercriminalité qui consacre cette incrimination, en disposant que « 1. *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.*»[31]

- *Eléments matériels*

Comme nous l'avons retenu dans la définition, l'élément matériel contient plusieurs actes dont le fait d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

[31] Article 4 de la convention, op.cit.

L'introduction de codes malveillants tels que des virus ou des chevaux de Troie relève de cette disposition, de même que la modification des données qui résulte de cet acte.

- *Elément intellectuel*

L'élément moral est l'intention frauduleuse qu'a le délinquant, sachant qu'il lui est interdit d'entrer dans un système informatique pour modifier, endommager ou supprimer les données qui y est stockées. Par conséquent, l'usager qui propage un virus à son insu n'est pas punissable.

3.1.2. Possibilité de son intégration dans le droit pénal congolais

Voyant comment d'autres droits pénaux évoluent dans le monde, ayant remarqué que le droit pénal congolais est en retard par rapport aux autres, le souci nous est venu de proposer l'intégration de l'atteinte à l'intégrité des données dans le code pénal de cet Etat.

Toujours dans les perspectives précédentes, nous proposons au législateur congolais à s'inspirer du législateur français en s'inspirant à l'article 323-3 du nouveau code pénal français.

Et le législateur congolais pourrait s'exprimer en ce sens :

> « *Quiconque aura introduit frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier les données qu'il contient sera puni d'une servitude pénale de cinq ans et d'une amende de 150.000 francs congolais.*»

3.2. L'atteinte à l'intégrité du système

Ce point est consacré à l'analyse de l'atteinte à l'intégrité du système, c'est-à-dire nous la définissons, en ressortissant ses éléments constitutifs et proposons son intégration en droit pénal congolais.

3.2.1. Définition et éléments constitutifs

- *Définition*: « c'est l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques[32]. »

- *Eléments constitutifs*

  - *Elément légal*

Comme nous l'avons reconnu ci-haut, c'est l'article 5 de la convention sur la cybercriminalité qui prévoit cette incrimination dans le sens que « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.* »[33]

  - *Elément matériel*

[32] Article 5 de la convention sur la cybercriminalité.
[33] Article 5 de la convention, ***op.cit***.

L'entrave au système, le terme « *entrave* » se rapporte à des actions qui portent atteinte au bon fonctionnement du système informatique. L'entrave doit résulter de l'introduction, du transfert, de l'endommagement, de l'effacement, de l'altération ou de la suppression de données informatiques. En plus l'entrave doit être grave pour que l'infraction soit retenue.

- *Elément intellectuel*

C'est l'intention de causer une entrave grave à un système informatique sans droit, c'est-à-dire de porter atteinte au bon fonctionnement du système sans autorisation de son propriétaire.

3.2.2. Possibilité de son intégration en droit pénal congolais

De même que les infractions analysées ci-haut, l'atteinte à l'intégrité du système n'est pas réprimée en droit congolais. Et pourtant, elle se commet déjà en RDC. Voilà pourquoi, nous renforçons encore notre lutte dans la proposition de l'intégration cette infraction dans le code pénal congolais et ainsi, il n'y aura plus de vide juridique dans cette matière.

Pour cela, nous suggérons une modification du code pénal en ces termes :

> « *Quiconque causera intentionnellement une entrave grave au bon fonctionnement d'un système informatique, sera puni d'une servitude pénale de 2 ans et d'une amende de 200.000 francs congolais ou l'une de ces peines seulement.* »

3.2.3. L'abus de dispositifs

- *Définition :* C'est le fait de poser des actes tels que la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus, d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et la possession d'un élément visé ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5.

- ***Eléments constitutifs***

  - *Elément légal*

De ce qui précède, il ressort clairement que l'article 6 de la convention sur la cybercriminalité est le siège de la matière qui dispose :

> « *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:*
>
> *a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:*
>
> *i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;*

ii. d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article. »[34]

- *Eléments matériels :*
    - *la production d'un dispositif ou un programme informatique ;*
    - *la vente des dispositifs et programmes informatiques ;*
    - *l'obtention pour utilisation d'un dispositif ou programme informatique ;*
    - *l'importation des dispositifs ou programmes informatiques ;*
    - *la Diffusion des dispositifs ou programmes informatiques.*

- *Elément intellectuel*

C'est l'intention qu'a le délinquant de poser les actes énumérés ci-haut sans droit en sachant que les outils mis à la disposition serviront pour la commission des infractions citées en sus.

- *Possibilité de l'intégration de l'abus de dispositifs dans le droit pénal congolais*

Le fait pour nous d'avoir proposé l'insertion des infractions sus analysées dans le code pénal congolais, nous oblige aussi de le faire pour l'abus de dispositif, cela pour une bonne et simple raison que cette incrimination est la source même des infractions précédentes, parce que, sans les outils mis à la disposition des pirates par le délinquant, on ne pourra retenir les autres infractions.

Légiférer sur la sécurité informatique peut s'avérer un art délicat, car en voulant élargir l'efficacité de la sanction pénale contre les fraudeurs, on risque dans le même temps d'incriminer des actes destinés à la prévention de la fraude informatique et à l'amélioration de la sécurité des systèmes d'information[35].

C'est ainsi que nous suggérons au législateur congolais l'intégration de cette incrimination en ces termes :

> « *Quiconque aura intentionnellement, sans motif valable, importé, offert, cédé ou mis à disposition des outils, équipements, instruments, programmes informatiques ou toute donnée conçue ou spécialement adaptée pour la commission de l'une ou plusieurs infractions portant atteinte à la*

[34] Article 6 de la convention, ***op.cit***.
[35] M. QUEMENER, ***op.cit***., p.95.

> *confidentialité, intégrité et la disponibilité des données et systèmes informatiques, sera puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévère réprimée.* »

CONCLUSION

Au terme de cette étude, nous sommes en droit de conclure qu'il existe bel et bien des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques dont l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et l'abus de dispositifs.

Mais force est de constater que ces infractions ne sont pas encore réprimées en RDC, nous les avons analysées en nous référant à la convention sur la cybercriminalité, en cherchant leurs définitions dans la convention, pour ensuite faire ressortir leurs éléments constitutifs et, enfin, nous avons proposé leur intégration dans le code pénal congolais en formulant des suggestions des futures dispositions pénales, et cela en nous inspirant des autres droits pénaux.

BIBLIOGRAPHIE

- QUEMENER M., *Cybermenaces, entreprises et internautes*, enonomia, Paris, 2008, p.1.
- KALONJI M., *Notion de cybercriminalité : praxis d'une pénalisation de la délinquance électronique en droit pénal congolais,* p. 6 disponible sur www.tgk.centerblog.net
- http://www.commentcamarche.net/contents/secu/secuintro.php3, consulté le 14 Avril 2013.
- FILIOL E., *Les virus informatiques : théorie, pratique et applications*, Ed. Springer, 2004, p.79 et s.
- NDUKUMA N., *Cyberdroit, télécoms, internet, contrats de e-commerce. Contribution au droit congolais*, PUC, Kinshasa, 2009.
- Convention du conseil de l'Europe sur la cybercriminalité de 2001.
- NYABIRUNGU, M.S, *Traité de droit pénal général congolais*, 2eme éd., EUA, Kinshasa, 2007.