La lutte contre la cybercriminalité en République Démocratique du Congo

Commentaire article publié le **21/09/2022**, vu **14077 fois**, Auteur : Etude Dominic Cassini & Co. Law Firm

Lutter contre les crimes informatiques est une obligations pour l'Etat. Ne pas s'en prévaloir à l'ère actuel, c'est exposé tant l'Etat lui-même que ses propres sujets.

LA REPRESSION DE LA CYBERCRIMINALITE EN DROIT CONGOLAIS.

THE REPRESSION OF CYBERCRIME IN CONGOLESE LAW.

Dominic Cassini Tshikolasony Luvundo Jr.

Lawyer at the Bar of the Lualaba Court of Appeal

Research Professor in Digital Law at the University of Kolwezi.

L'ampleur de la criminalité numérique, autrement appelé cybercriminalité ne cesse de faire état de la faiblesse du système judiciaire congolais tant pour la lutte contre cette nouvelle pratique de criminalité que pour la répression. Les acteurs judiciaires, entendre ici le personnel judiciaire qui concourent à assurer le maintient de l'ordre public, ne sont pas soit à mesure lutter efficacement contre ces actes criminels et cette impuissance du système judiciaire fait de la république Démocratique du Congo, un paradis numérique. Rare sont les cas où le juge congolais a réellement pris la peine de juger le cybercriminel et au pire même les organes politiques s'adonnent à des violations manifestes de la loi relative à la télécommunication et aux technologies de l'information et de la communication. L'instauration d'une fiscalité irrégulière en a été la preuve irréfutable de l'absence d'efficacité dans la lutte contre la criminalité information pour autant que le congolais moyen trouve tout à fait normal de poser autan des actes criminels dans le cyberespace sans être inquiété.

Mots clés : cyberespace, - cybercriminalité, - droit pénal, -procédure pénale, - droit numérique, - cyberattaque.

ABSTRACT

The degree of digital crime, otherwise known as cybercrime, continues to highlight the weakness of the Congolese judicial system both in the fight against this new criminal practice and in its repression. The judicial actors, to hear here the judicial personnel who contribute to maintain the

public order, are not able to fight effectively against these criminal acts and this impotence of the judicial system makes the Democratic Republic of Congo, a digital paradise. Rare are the cases where the Congolese judge has really taken the trouble to judge the cybercriminal and at worst even the political bodies are engaged in clear violations of the law on telecommunications and information technology and communication. The introduction of irregular taxation has been irrefutable proof of the lack of effectiveness in the fight against information crime for as much as the average Congolese finds it quite normal to commit so many criminal acts in cyberspace without being worried.

Keywords : cyberspace, - cybercrime, - criminal law, - criminal procedure, - digital law, - cyber attack.

INTRODUCTION.

Le cyberespace ou univers numérique a transformé la notion de l'État ainsi que celle de la souveraineté même. N'ayant plus besoin de se déplacer ou de se retrouver dans un État pour opérer des actes criminels, le recours à l'intersection des outils informatiques (architecture ou data Center) en est un bouillon de développement de cette criminalité grandissante du reste constante, mais plus encore de la sensation du confort dans lequel se retrouve le criminel.

Pour les criminels la facilité à commettre les crimes numériques se résume en ceci que même si de nos jours des textes législatifs dans la plupart des États répriment la cybercriminalité, il n'existe pas de coordination ou d'entraide judiciaire à proprement parlé pour permettre aux États de prévenir ce risque grandissant. D'ailleurs même l'ONUDC, l'organisation des nations unis en charge de la lutte contre la criminalité et la drogue en paie les frais et parfois, les victimes ont peines à communiquer ou à rapporter les faits à la justice en préférant au mieux négocier avec le criminel information, non pas parce qu'elles ont peur des effets liés à cet acte criminel mais question de sauvegarder l'image.

Le cyberterrorisme[1] par exemple est une preuve probante de l'existence même de ce caractère favorisant de la criminalité grandissante à l'échelle planétaire et de la faiblesse que présentent l'INTERPOL et les autres États. Les organisations terroristes comme État-Islamique, Al-Qaida, Shebab font trop souvent recours aux Nouvelles technologiques de l'information et de la communication pour recruter des jeunes à leurs causes dans l'intérêt de faire plus des dégâts[2] sans qu'ils soient inquiétés ni moins encore bannis du cyberespace.

Si l'entreprise Signal ®, un des leaders de la protection des données numériques, est pointé du doigt en ceci qu'elle ne partage jamais les données de ses utilisateurs même si ceux-ci sont un vrai danger sociétaire[3], cet état de chose facilite le crime à grande échelle aussi bien pour des pays comme la République Démocratique du reste considérée comme paradis numérique tant pour sa législation faible que pour l'absence des mécanismes assez conséquents.

Dans notre analyse, nous avons constaté que la criminalité informatique est de deux sortes : il peut s'agir soit des attaques informatiques contre les infrastructures des nouvelles technologies et de l'information et de la communication soit encore des attaques directement visées contre les personnes.

Les attaques informatiques contre les infrastructures visent essentiellement les données des entreprises ou des États stockés dans des datacenter ou encore des ordinateurs alors que les attaques informatiques contre les personnes visent essentiellement les données à caractère personnel que chaque individu sauvegarde soit sur un support soit encore en recourant aux prestataires de services qui le font à leur place principalement avec la technologique dite Cloud Computing[4] . Cette attaque contre les personnes peuvent aller plus loin en visant aussi le patrimoine numérique pour autant les données numériques ont la nature juridique des biens meubles incorporels.

Dans notre pays, la RDC, l'an 2019 a fait ressortir la pertinence majeure de la protection des données numériques aussi bien pour les entreprises que pour les particuliers. Avec Facebook ou SnapChat par exemple, beaucoup des personnalités essentiellement des artistes musiciens ont vu leurs données à caractères privés être mises en ligne soit par des proches dont ils ont un passif (dans ce cas on parle de Revenge-porn[5]) soit par des hackers après avoir eu accès à des données stockées sur les serveurs du fournisseur cloud (Drive, OneDrive ou Mega) qui les revendent aux plus offrants capables de faire des chantages à la victime.

L'émergence des systèmes d'échanges de fichiers sur le réseau Internet, le développement de sites pirates et la démocratisation du numérique facilitent ces actes criminels si bien que lutter contre les hackers est à priori un combat partiellement perdu par les institutions publiques.

Dans une affaire par exemple, le Tribunal de Grande Instance de Nanterre avait condamné pour proxénétisme un individu qui diffusait des messages sur le réseau Internet afin d'attirer des clients potentiels au bénéfice d'une personne se livrant à la prostitution[6].

L'on comprend dès lors que la répression des infractions numériques ne nécessite pas essentiellement une modification complète de la loi pénale congolaise, mais l'effectivité de la loi 20/017 qui peut combler ce vide juridique pour cette problématique de droit trouve sa raison d'être dès lors qu'il faut présenter les preuves devant le juge.

N'a-t-on pas lu dans la constitution que le droit à la vie privée est sacré ? Ou même que les données à caractère personnel sont frappées du droit à la confidentialité, c'est-à-dire à la non-divulgation sauf accord exprès de l'utilisateur ou sauf le cas où la loi l'a prévue ? C'est en cela qu'il faut connaitre le criminel informatique.

Robert Badinter qu'a si souvent rappelé Maître Eric Morreti[7], disait que lorsqu'un délinquant commet un crime, il ne l'accomplit pas un code pénal à la main. Ce qui n'est pas le cas toujours des criminels informatiques qui, dans plusieurs occasions, ont connaissance des causes des actes posés, ils savent bien que c'est interdit, c'est illégal et la peine encourue est même connu d'avance, mais cela ne les empêche que trop rarement à agir. Voilà pourquoi il importe de connaitre le criminel informatique, parce qu'il diffère du criminel classique, il est partout, mais presque invisible, il a une réputation à sauvegarder dans la communauté internationale du crime organisé. Ce criminel-là reste un danger public pour la société, si bien qu'à un moment donné que certains d'entre eux sont désormais de l'armée numérique des États.

I. LES EXIGENCES PREALABLES A LA REPRESSION DE LA CYBERCRIMINALITE

▪

L’analyse de la cybercriminalité *impose* deux exigences préalables qui peuvent permettre de lutter de manière efficace et assurer la sécurité de chaque citoyen congolais. Comme nous le verrons, il y a d’abord l’exigence liée à l’identification du cybercriminel (A) : il s’agit d’identifier le criminel informatique pour permettre à la justice de le sanctionner efficacement. L’identification devient donc un moyen de dissuasion en ceci que le criminel informatique, techniquement appelé Hacker, prend conscient du risque qu’il court dès lors qu’il ose s’adonner à des pratiques criminels dans le cyberespace.

Toutefois, cette exigence ne peut qu’aller de paire qu’avec la détermination de la forme de cybercriminalité que consacre le système pénal congolais (B). Il est vrai que le droit pénal a un caractère textuel, c’est-à-dire comme l’indique Beccaria, l’application du droit pénal suppose un texte qui réprime l’acte réputé criminel. Ainsi, une détermination du cybercrime permet de connaitre quel acte est réputé cybercrime par rapport à l’autre et quelle considération est donnée en droit étranger. D’où l’importance de l’analyse ces exigences, que nous considérons comme préalable à la répression de la cybercriminalité.

A. L’identification du cybercriminel

1. Les hackers.

Nous l’avons dit ci-haut, l’une des particularités de la cybercriminalité c’est le criminel lui-même. Qu’il agisse seul ou en réseau, le criminel informatique est avant tout connu pour son gout très prononcé à des défis numériques : voler dans une banque, faire du carding cashout : une technique qui consiste à voler des informations bancaires contenues sur une carte de crédit[8] , etc. Il ne s'agit pas là d’une classification des criminels informatiques sur base de la théorie de Lombroso, mais de donner un profil type propre aux cybercriminels quel que soit le milieu où il se trouve. Avant de parler du cybercriminel, il faut déjà penser aux hackers parce que le cybercriminel fait partie de la grande famille des hackers qui, eux-mêmes, se classent en fonction de la capacité à agir et des intérêts pécuniaires à poursuivre. Tous les hackers ne sont pas de cybercriminel, mais une grande partie d’entre-deux s’adonnent à des pratiques criminelles sans vergogne et sont même recrutés par les États ou les Organisations criminelles internationales comme l’État islamique qui a sa propre armée numérique. La guerre entre la Russie et l’Ukraine n’a fait que trop ressurgir la problématique de cyberguerre au centre de laquelle jonche le cybercriminel qui agit en groupe ou individuellement au grand mépris des règles de droit international sur la souveraineté.

- Le Black HAT: il s'agit d'un professionnel dans la cybersécurité[9] et qui a pour intention primaire de s'attaquer à tout système informatique pour des intérêts souvent pécuniaires. Cette catégorie des hackers a fait du hacking une profession à part entière. En effet, ils opèrent souvent dans les deepweb, essentiellement pour des activités criminelles comme la vente des armes, l'entretien des réseaux de prostitutions ou de vente d'organes, les recrutements des jeunes pour le djihad ou encore la vente des informations sensibles des gouvernements… Ils sont généralement recherchés par les agences de renseignements, car bien souvent ils sont à la base de plusieurs crises dans le monde, notamment le krach boursier, les manipulations des élections ou encore les incitations à des haines et les manipulations des peuples. Les Black Hat sont souvent à la recherche du confort psychologique, une sensation de supériorité, un besoin excessif, etc. c'est la grande famille des cybercriminels qui prône la criminalité informatique au sens pur du terme.

- White Hat : l'antithèse même du Black Hat, il est le Hacker du bien-être, celui qui prévient le risque et le danger encouru par les utilisateurs lambda. Il s'agit d'un professionnel de la cybersécurité et n'ont aucune intention malicieuse de procéder à des attaques contre les systèmes de sécurités informatiques des entreprises. Généralement, ils ont une très grande connaissance des réseaux informatiques, des Protocoles des sécurités, et l'administration des systèmes d'exploitation (programmation, Système d'exploitation). Ils ont aussi de très bonnes maîtrises de prévention des risques informatiques. Par ailleurs, le White Hat est caractérisé par l'idéal de la recherche scientifique pour trouver des failles informatiques dans le système et en proposer des solutions pour pallier à ces failles .

Dans la plupart des cas, le White Hat est engagé par des organisations pour effectuer des tests de pénétration et des évaluations de vulnérabilité sur leurs systèmes afin d'améliorer leurs défenses de sécurité. Ils effectuent des tests et des attaques sur les sites web et les logiciels afin d'identifier les vulnérabilités éventuelles, tout en respectant les règles établies, telles que les politiques de prime aux bogues. Ils informent directement le fournisseur concerné de tout problème afin qu'un correctif puisse être publié pour corriger la faille[10]

- Grey Hat : il s'agit des personnes qui sont classées entre les White Hat et les Black Hat. Généralement, ils offrent des services de cybersécurité moyennant un paiement trop souvent en cryptomonnaie. Cette catégorie des cybercriminels crée parfois des failles sécuritaires ou découvre (0day[11]) et ne peuvent donner des solutions que si seulement ils sont payés. Il s'agit des individus qui ont passé plus du temps dans la catégorie de Black Hat et ont une difficulté à s'en passer des leurs activités criminelles malgré le fait qu'ils se sont rangés. Ils sont utilisés comme consultants lorsque le besoin se fait sentir ;

- Hactiviste : il s'agit des Hackers (cybercriminel ou non) ayant souvent des intentions politiques dans leurs actions. L'on peut citer Anonymous, Edward Snowden, Kevin Luteya ou encore Julian Assange. Parfois, les Hactivistes sont à la base de beaucoup des scandales dénoncés comme Wikileaks, Panama Papers et Paradise Papers ou Radio Okapi sur Facebook. Cette activité s'est beaucoup plus intensifiée en RDC avec pour base de repère Twitter où certains en on fait pratiquement de cette activité criminelle du numérique, un métier à part entière ;

- Script Kiddies : Un Hacker généralement amateur qui n'a pas beaucoup des connaissances en informatiques, mais qui recourt à des outils de Hackings développés par les White Hat, Black Hat ou des Grey Hat. Généralement, ce sont des novices dans le cyberespace qui démarquent plus par un besoin de reconnaissance par la communauté criminelle dans le secteur du numérique.

2. Le Crasher.

Le crasher est un cybercriminel qui se démarque plus de l'hacker classique par sa vision de voire les choses dont il veut opérer une attaque informatique. Le crasher est avant tout un informaticien et possède aussi de bonnes connaissances en sécurité informatique. Le Crasher comme le nom l'indique n'a qu'un seul but, c'est détruire tout ce qui passe devant lui. En effet, le crasher ne se préoccupe pas trop souvent des contenues qu'il est à même de découvrir lorsqu'il entre dans un système informatique. Pour lui, l'ambition n'est pas nécessairement de trouver un gain ou un avantage, mais de se venger ou de faire payer à la victime en effaçant les données, quelle que soit sa valeur ou la sensibilité. Généralement, ils ne sont pas si nombreux par rapport aux hackers et œuvrent souvent en solitaire, mais les dégâts causés par eux sont sans conteste énormes en ceci qu'ils consacrent plus de temps qu'il en faut à un seul projet dans le seul but de tout détruire.

3. Le Cracker.

À l'opposer des Crashers, les crackers pénètrent dans des systèmes informatiques, détruisent les fichiers ou se décident d'y rester pour d'autres fins que la destruction des données numériques.

Il convient de proposer une définition de ce terme dans une logique comparative, en considérant le crasher comme la personne qui pénètre à l'intérieur d'un système informatique et détruit un de ses éléments par plaisir. Dans cette optique, la distinction entre le crasher et le cracker est trouvée dans la finalité de l'acte posé. Le crasher pénètre à l'intérieur d'un système informatique et détruit les données, le cracker soit détruit soit introduit des données dans ce système pour d'autres fins.

B. La détermination du cybercrime : la notion de la cybercriminalité en droit congolais, droit comparé et les infractions rattachées.

Utiliser Internet n'est pas un problème en soi, mais les facteurs générés par les utilisateurs peuvent concourir à des actes criminels très grandissants allant d'un simple acte attentatoire contre un individu jusqu'à des actes qui affectent les États.

Ces facteurs concourent à déterminer la notion de la cybercriminalité tant sur le plan pénal que sur le plan de lutte efficace contre cette forme de crime. Une étude comparative permet à tout le moins de nous situer sur la situation en République Démocratique du Congo puisque certains pays à l'instar de la France, la Belgique ou même de l'Afrique austral ont largement avancé dans la lutte et la répression des crimes informatiques et, une analyse comparative facilite ainsi la tâche lorsqu'il s'agira de faire la critique juridique sur l'effectivité de la loi.

En effet, le cyberespace (entendre ici, univers numérique) présente la particularité de se faire ressentir dans la vie réelle lorsque le cyberconsommateur pose des actes aussi minimes soient-ils. Un utilisateur peut voler de l'argent en banque sans qu'il ait besoin d'y être physiquement ; commettre un homicide sans y être physiquement sur le lieu du crime, détruire des données numériques en prenant à distance le contrôle des terminaux.

Les nouvelles technologies impactent sérieusement le quotidien de la vie et d'ailleurs RAYNA opine à bon sens qu'on ne peut pas trouver une activité humaine qui n'ait pas migré vers l'Internet, que ce soit le business, la politique, la recherche scientifique, le drague ou…la délinquance

[12].

Donc aujourd'hui, plusieurs activités sont sur Internet du simple tweet d'un citoyen congolais aux actes criminels ou de terrorismes souvent butés à la technicité des plus en plus grandissantes de l'informatique. Les nouvelles technologies de l'information et de la communication facilitent impérativement les échanges du quotidien, mais bien plus des activités criminelles. Oussama Ben Laden, les cartels de Sinaloa, Al-Qaida…les nouvelles technologies influencent de plus en plus la vie criminelle et la délinquance numérique s'imprègne peu à peu dans la vie des Congolais pour devenir une routine.

Comme nous l'avons dit ci-haut, utiliser les technologies numériques n'est pas mauvais, mais l'abus est susceptible d'entrainer des poursuites judiciaires pour des faits prévus par les lois pénales du pays. Cependant, une différence majeure existe entre les infractions de droit commun que le délinquant commet dans la vie réelle de celle qu'il pourrait commettre dans le cyberespace du fait même de la particularité de ces infractions qui présentent une difficulté en ce qui concerne la preuve.

De la sorte, il convient dès lors de comprendre la criminalité informatique, en quoi elle consiste et au mieux faire une étude sur ce que la loi prévoit comme définition de la cybercriminalité.

La notion de cybercriminalité est un néologisme dont on peine toujours à trouver une définition appropriée. Parfois appelé cyberdélinquance ou encore délinquance numérique, criminalité informatique voire même délit informatique ; les définitions sont pléthores . S'il est généralement admis qu'au centre de la cybercriminalité, on y trouve des individus qui posent des actes informatiques au moyen des outils informatiques. Pour parler de la cybercriminalité, il faut déjà parler du cybercriminel qui, dans bien des cas, a un profil type très différent du criminel traditionnel.

De nos jours, certaines auteurs sont d'avis commun avec les experts de l'Organisation pour la Coopération et le Développement économique (OCDE) sur la considération apportée à la cybercriminalité, il s'agit donc de *« tout comportement illégal ou contraire à l'éthique ou non autorisée, qui concerne un traitement automatique de données et/ou de transmissions de données »*[13].

Depuis lors, il résulte qu'une approche précise de la moralité semble être intégrée dans la considération de la cybercriminalité qui en opposé du droit pénal, considère que le système répressif d'un État ne peut à lui seul contenir toute l'approche « sanction » de l'utilisation frauduleuse de l'informatique.

Toutefois, cette ambigüité de définition entre la cybercriminalité et le délit informatique devient de plus en plus grande à cause de la difficulté d'avoir une acception conventionnelle sur cette forme de délinquance. Cette analyse logique rentre essentiellement dans le débat selon lequel « la seule démarche acceptable consiste à réserver l'acception de fraude informatique aux hypothèses dans lesquelles la technique informatique est au cœur de l'agissement incriminable » tout en sachant fort bien qu'il est parfois difficile d'isoler le « noyau dur » de la « périphérie »[14].

Dans le système judiciaire de la République Démocratique du Congo, le législateur comme toujours a défini la notion même de la cybercriminalité de manière assez ambiguë. Selon lui, il s'agit d'une notion large qui regroupe toutes les infractions commises sur ou au moyen d'un système informatique généralement connecté à un réseau[15].

Mais ce sont les approches doctrinaires et jurisprudentielles qui ont donné naissance à des jalons sur la question même de l'assimilation ou de la distinction du crime et de la cybercriminalité. En Droit français par exemple, la cybercriminalité recouvre « l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus

particulièrement sur les réseaux partageant le protocole TCP-IP[16], appelé communément l'Internet »[17].

Au dixième Congrès des Nations Unies, à Vienne, les Nations-Unies avaient considéré que la « cybercriminalité » doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », et dans une acception plus large « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique »[18].

Jean Colombain, par ailleurs, estime que lorsque nous poursuivons notre tour d'horizon de la cybercriminalité sur les réseaux sociaux avec ce qui constitue sans doute le stade ultime de la menace : la propagande cyberdjihadiste. Là c'est ne plus seulement à votre porte-monnaie qu'on en veut, mais à votre esprit. Surtout si vous êtes jeune et en quête de personnalité et d'idéal[19].

Le droit suisse a une approche bien plus généraliste en ce qui concerne la cybercriminalité, elle s'entend comme « de nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels »[20]. Enfin, le Collège canadien de police définit la cybercriminalité comme « la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale »[21].

Aux États-Unis, la notion de cybercriminalité diffère d'un État à l'autre, et d'un département de police à l'autre. Selon le Département de la justice (United States Department of Justice), la cybercriminalité est considérée comme « une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa perpétration, son investigation, ou ses procédures pénales »[22]. De son côté, le Code pénal californien (section 502) définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Il considère comme cybercriminalité le fait « d'accéder, ou de permettre intentionnellement l'accès, à tout système ou réseau informatique afin de :

- Concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ;

- Acquérir de l'argent, des biens, ou des services, dans le but de frauder

- Altérer, de détruire, ou d'endommager tout système, réseau, programme, ou données informatiques »[23] et le Code pénal texan (section 33.02) va plus loin parce qu'il considère comme cybercriminalité, le fait d'accéder à un ordinateur, à un réseau, ou à un système informatique sans avoir l'autorisation de son maître[24].

En République Démocratique du Congo, une définition équilibrée de la cybercriminalité est celle qui prend en compte l'économie de l'article 9 de l'ordonnance 87/243 du 22 juillet 1987 relative aux activités informatiques. La cybercriminalité peut dès lors s'entendre comme étant tout acte criminel posé par un ou plusieurs personnes au moyen des logiciels informatiques dans le but d'attenter aux biens des personnes et à leurs vies. Il s'agit ici de porter critique à la définition de la loi de 2020, qui s'est contentée de parler de notion large uniquement et circonscrire à l'article 153 de manière exhaustive les actes réputés cybercriminels alors que les activités informatiques vont au-delà de onze actes uniquement.

D’aucun n’ignore que l’infrastructure informatique est composé d’une partie physique et de l’autre immatérielle. Or, c’est cette partie immatérielle, le logiciel, comme les techniciens aiment bien l’appeler qui fait tourner le système et les autres logiciels ou applications informatiques et il est à noter que la criminalité informatique ne peut se faire sans le recours à une application informatique et il est de bon à loi de considérer la cybercriminalité comme une forme de criminalité dont l’élément matériel essentiel c’est l’application informatique appelée logiciel, outres les éléments constitutifs classiques de l’infraction.

1. La cybercriminalité en droit comparé.

Toutes ces définitions mieux reprises ne doivent pas être considérées à fortiori comme définitives et totalement satisfaisantes en ce qui concerne la notion de cybercriminalité. En droit français, la définition adoptée par le ministère de l’Intérieur français vise seulement les infractions dirigées contre les réseaux de télécommunications. Elle ne recouvre ni les infractions susceptibles d’être commises sur les systèmes informatiques ni les infractions directement générées par le fonctionnement des réseaux informatiques. Il s’agit des infractions portant sur l’information véhiculée par le système informatique comme l’escroquerie, l’abus de confiance, et les atteintes aux libertés individuelles par la création illicite de fichiers nominatifs[25].

Les mêmes confusions se retrouvent également dans les législations américaines où l’on confond la cybercriminalité et la criminalité informatique, et cela s’avère symptomatique d’une difficulté d’appréhender cette forme de délinquance. Ainsi, M. WALL déclare que « le terme cybercriminalité ne signifie plus qu’un acte illicite qui est, d’une façon ou d’une autre, relatif à l’ordinateur »[26].

Dans notre droit congolais, le législateur a toujours le mérite d’être ambigu dans ses définitions ce, qui laisse une appréciation libre court à chaque personne. Une étude de la loi 20/017 permet d’appréhender la cybercriminalité en quelques articles alors que l’ordonnance 87/243 a le mérite de renvoyer tous les actes criminels à la criminalité informatique dès lors qu’il ressort de l’analyse des éléments ayant concouru à l’infraction, la preuve d’un recours à une application informatique.

2. Le Droit congolais

Avant l’an 2020, le droit congolais d’une manière générale ne possédait pas de textes répressifs uniformisés traitant de manière spécifique de la criminalité informatique en tant que telle. À l’époque, le système pénal congolais trouvait sa force de répression que dans la loi 13/2002 où il était fait référence à des peines relatives à l’interception des communications et la violation du secret des courriers électroniques, etc.

Une fouille très poussée de la législation congolaise principalement en ce qui concerne l’ordonnance 87/243 du 22 juillet 1987 portant réglementation de l'activité informatique en République Démocratique du Congo, permettait de donner une porte de sortie aux cours et tribunaux congolais de connaitre des affaires pénales ayant trait à la criminalité informatique. L’adoption de la loi n° 18/019 relative aux systèmes de paiement et de règlement-titres du 9 juillet 2018 en avait apporter un vent nouveau en consacrant des notions de la signature numérique, la preuve numérique et l’association des malfaiteurs cybercriminels.

Or, depuis novembre 2020, la République Démocratique du Congo s'est plutôt dotée de la loi 20/017 qui a abrogé la loi 13/2002 alors que l'ordonnance 87/283 reste largement méconnu aussi bien des praticiens que des justiciables faute de vulgarisation, mais aussi d'éducation numérique justifiée en grande partie par le retard technologique que connait le pays.

Par ailleurs l'ordonnance 87/243 bien que méconnue produits toujours des effets juridiques notamment lorsqu'on fait la lecture combinée de ses articles 8 et 9 où il est disposé que toutes les applications informatiques existant au Congo font l'objet d'un inventaire établi par les services présidentiels d'études, pour en déterminer la nature, les domaines et la caractéristique…tout acte accompli à l'occasion d'une application informatique et qui porte atteinte à la sécurité de l'État, à l'ordre public, aux bonnes mœurs, est punissable conformément aux lois pénales en vigueur.

Il est vrai qu'une infraction l'est que par le fait de la loi d'où le mérite du principe général de droit pas de sanction pénale sans texte. La plupart des infractions commises dans le cyberespace sont quasiment les mêmes que celles dans le monde réel à quelques exceptions près. Prenons par exemple le blanchiment d'argent, si les moyens traditionnels sont déjà connus, les techniques de blanchiment sont devenues de plus en plus complexe qu'avant et cela grâce aux nouvelles technologies de l'information et de la communication ce qui donne plus des fils à retordre aux organes poursuivants, situation qui tend à remettre en question l'application effective de la Loi n°2004-16 du 19 juillet 2004 portant lutte contre le blanchiment des capitaux et le terrorisme en République Démocratique du Congo..

Un autre cas type est celui de l'espionnage, l'atteinte à sûreté intérieure et extérieure du pays. Les moyens classiques des éléments constitutifs sont connus de tout ce temps, mais la technologie a apporté un vent nouveau à cette forme de criminalité et d'ailleurs les personnes incriminées ne fournissent pas beaucoup d'effort comme avant pour autant que la guerre classique s'est transformée en cyberguerre. Le Mossad par exemple n'hésite pas à recruter directement sur son propre site, l'état islamique auquel l'ADF s'est allié n'hésite pas aussi à recruter directement sur son propre site si bien qu'il suffit que la personne ose cliquer sur un lien publicitaire pour être redirigé vers le portail approprié.

Que donc, l'adoption de la loi 20/107 est une aubaine, si bien que la précarité des dispositions légales sur la criminalité informatique va se sentir avec le temps tant pour la question de compétence matérielle que territoriale [27]. Cette lutte contre la cybercriminalité ne s'attèle pas uniquement aux infractions de droit commun, mais aussi aux infractions économiques et pour preuve, le législateur a pensé aussi en adoptant la loi n°18/019 relative aux systèmes des paiements et de règlement-titres.

L'apport de cette loi est celle d'avoir consacrée non seulement la notion de la preuve numérique en droit congolais mais aussi et surtout celle de la répression de l'association des malfaiteurs cybercriminels pour autant que l'acte se soit effectué en bande.

D'ailleurs, cette innovation de l'association des malfaiteurs permet à tout le moins de prendre en compte le principe de la responsabilité pénale des acteurs du cyberespaces tant qu'ils agissent en bande et que l'un d'entre-eux pose un acte criminel susceptible de troubler l'ordre public.

L’autre critique est portée sur la loi n°20/017. En effet, le législateur a crû bien faire lorsqu’il a circonscrit certains comportements criminels à de la cybercriminalité et de renvoyer certaines infractions au code pénal ordinaire sans qu’il ne soit réellement pris en compte le caractère essentiel de l’infraction, c’est-à-dire les éléments constitutifs. Cette situation est de nature à créer à la longue une ambiguïté dans l’appréciation des infractions tant pour certains actes qui seront considérés comme cybercriminels et d’autres non alors qu’au fond, le droit pénal lui, reste sur le principe textuel, c’est-a-dire pas de peine sans texte.

3. Les infractions rattachées au cyberespace.

La particularité de la cybercriminalité demeure intrinsèquement dans son caractère d’extranéité.

Les plus souvent, les auteurs des infractions informatiques sont pour la plupart du temps en dehors du territoire de la victime ciblée.

Il est vrai que le Code pénal congolais a tenté de résoudre la question, mais elle demeure largement butée à la problématique de territorialité que peuvent lui opposer certains prestataires du cyberespace tant pour l’acquisition des données numériques incriminées que pour l’inculpation du prévenu.

En 1977, Esika Makombo avait déjà compris ce problème sur la territorialité. D’ailleurs, il disait lui-même que le principe de la territorialité a une autre conséquence négative : il interdit à l’État de poursuivre celui qui se réfugie dans son territoire, c’est-à-dire dans cet État, après avoir commis une infraction à l’étranger. Il continue en disant, cependant, nous pouvons nous féliciter d’avoir une législation progressiste. Néanmoins, cette législation exige d’être améliorée. Car nous devrions d’une part décourager tous les étrangers qui voudraient faire de notre pays un lieu d’asile des malfaiteurs, et d’autre part, tous les Congolais qui croiraient pouvoir échapper à la répression en allant assouvir leurs appétits criminels à l’étranger[28].

Il se pose dès lors un problème, celui de la compétence, mais aussi celui de la territorialité, si l’on peut se pencher sur l’approche de l’extradition, la solution demeure toute trouvée, mais si l’on plonge un peu plus, l’on comprendrait que la procédure même d’extradition, la collaboration de fichage avec INTERPOL et la réciprocité entre États sont les raisons majeures qui peuvent justifier d’un manque d’effectivité de la nouvelle loi sur la télécommunication et les nouvelles technologies de l’information et de la communication ce, sans compte les difficultés techniques pour identifiés les criminels informatiques.

L’informatique, en RDC, demeure encore un vrai mythe. Chacun est informaticien, criminel informatique (Hacker), geek, mais au fond, c’est à peine que quelques uns puissent facilement manipuler un terminal, oser accéder à un système informatique, faire de l’encodage, etc.

Il est clair qu’avec l’absence d’une éducation numérique, les dérives ne sont plus à compter tant pour le domaine judiciaire que pour le Congolais lambda. Raison qui justifie que l’on doit aussi se pencher sur le criminel informatique pour comprendre son essence, son comportement et comment agir quant à ce.

Les infractions rattachés au cyberespace présent dès lors ce caractère d'extranéité, l'on vit maintenant avec des infractions qui ont une connotation internationale dans l'ensemble. L'auteur peut certes se retrouver sur le territoire du pays qui le poursuit, là le problème ne se pose mais lorsqu'il importe de prendre en compte la problématique de domiciliation ou encore de d'anonymisation, les infractions rattachées au cyberespace présenteraient dès lors non pas qu'un conflit des lois mais aussi et surtout la question pertinente de compétence.

II. LA MISE EN ŒUVRE DE LA REPRESSION DE LA CYBERCRIMINALITE.

Le législateur congolais a eu le mérite d'adopter la loi 20/017 qui couvre le secteur du numérique dans l'ensemble. Cette loi a au moins prévu certaines infractions essentiellement liées aux activités informatiques sur le sol congolais. Toutefois, il faut le dire ici, le législateur en abrogeant la loi de 2002 sur la télécommunication, n'a même pas tenu compte de revoir l'ordonnance numéro 87/243 relative sur les activités informatiques en République Démocratique du Congo. Cette situation dans l'ensemble, malgré les innovations apportées par la nouvelle loi du 25 novembre 2020[29] n'augure en rien une bonne mise en œuvre de la répression de la cybercriminalité en République Démocratique du Congo pour autant que les lois dénotent d'un caractère vague et presque imprécis dans certains cas.

Comme nous l'avons dit, l'ordonnance 87/243 a au moins le mérite de définir la notion de responsabilité pénale aussi longtemps que le délinquant poserait son acte au moyen d'un logiciel informatique. Il se dégage dès lors que la pratique les cours et tribunaux doit être telle que la poursuite des criminels informatiques ne peut l'être que s'il est établi le recourt à un logiciel informatique.

Pour les législateurs congolais, les infractions numériques sont répréhensibles, quelles que soient la forme prise par l'infraction. L'analyse faite par nous démontre de manière très objective qu'aucune infraction réputée numérique (infraction informatique) ne peut s'effectuer sans passer par un logiciel informatique approprié, ce qui rentre dans l'esprit du législateur congolais en son article 9 de l'ordonnance 87/243 pré rappelée.

Pour les informaticiens, un logiciel est un programme qui s'exécute selon une suite des commandes bien précises en fonction d'une programmation spécifique qui résulte quant à elle des algorithmes[30].

Si les actes physiques contre les infrastructures numériques sont rares en y prenant en compte le risque de se faire prendre, l'attaque informatique par des logiciels généralement de distribution libre est très courante dans le cyberespace.

Par contre, il ne s'agit pas d'une pratique adaptative du Code pénal congolais, chose que Esika Makombo interdit[31],mais plutôt d'une application effective qui rentre dans les attributions des officiers de police judiciaire ou du ministère public voire des juges pénaux.

Vendre sur Internet une maison ne vous appartenant, en se créant des fausses pièces afférentes à la maison reste tout même du stellionat de la même manière que voler des crédits dans le compte de son proche et y supprimer la notification de confirmation de la transaction constitue le vol.

Donc, à la lecture de l'article 9 de l'Ordonnance précitée, le principe d'administration des preuves ne pose aucunement problème sauf dans le cas où la loi prévoit des modalités d'ordre public qui protègent les intérêts publics et ceux des particuliers.

L'autre critique apportée à la loi de 2020, c'est celle d'avoir circonscrit les infractions numériques en onze point essentiels en son article 153 si bien que certains points demeurent ambigus tel est le cas du faux en écriture qui semble désormais s'apparenter à la destruction méchante. L'on est face à une opposabilité des lois pénales internes tout en prenant en compte les principes généraux de droit notamment celui de la rétroactivité de la loi pénale.

A. Le déploiement des instances de répression de la cybercriminalité.

En République Démocratique du Congo, les cours et tribunaux sont seuls compétents de connaitre des affaires judiciaires aux fins d'y rendre des décisions. Or, avec l'ère de la cybercriminalité dans le cyberespace, la conception pénale en droit congolais devra en principe changer au risque d'appliquer un droit évolutif en l'absence d'une quelconque réforme de l'arsenal judiciaire pénale.

Pour ce faire, dans les jours à venir, les cours et tribunaux devront connaitre des affaires répressives ayant trait exclusivement au droit numérique dans son ensemble ou encore des affaires qui sont entre les deux univers dont l'administration de la preuve exige que les données numériques soient reçues par le juge pénal.

Pour la preuve, la doctrine reste unanime sur ce point : le juge apprécie les moyens de preuves qu'on lui soumet souverainement d'après son intime conviction d'où le principe de la liberté des preuves avec comme corollaire l'intime conviction du juge. Cependant, il existe des limitations à ces principes de la liberté des preuves et de l'intime conviction : d'abord le juge doit respecter la force probante que la loi attribue à certains actes (…) puis les moyens de preuves doivent être rationnels et respectueux de la dignité humaine, mais aussi respecter le droit de la défense[32].

Par contre, la problématique de droit qui ressurgit c'est quand l'on doit présenter les moyens de preuves numériques dès lors qu'ils ont été acquis dans une irrégularité formelle ou si cette procédure est contre l'ordre public, mais bien encore porte atteinte au droit de la propriété qui est un droit fondamental dans notre système judiciaire.

Il importe donc de comprendre les preuves numériques avant même d'envisager une étude sur les actes criminels effectués dans le cyberespace.

Si les articles 8 et 9 de l'Ordonnance portant sur les activités informatiques donnent une porte de sortie aux cours et tribunaux congolais de poursuivre les auteurs des infractions commises aux moyens des outils informatiques. La difficulté rencontrée c'est plutôt dans la considération même du logiciel information. Les logiciels informatiques deviennent donc des moyens qui permettent de commettre un acte délictuel, un acte répréhensible par la loi de telle sorte que l'auteur sera puni conformément aux droits du pays.

Or, le système d'exploitation lui-même est un logiciel informatique et l'application utilisée pour commettre l'acte criminel demeure ni plus ni moins un logiciel informatique et c'est à se demander si l'on doit prendre en compte le principe de la participation criminelle tant pour l'auteur de l'acte que pour la société propriétaire de l'application que pour celle détentrice de l'application.

La cybercriminalité transforme les juridictions classiques en juridiction spécialisée pour autant le juge pénal congolais connait d'une matière nouvelle, une notion bien qu'à la frontière avec le droit

commun n’est pas ordinaire. Le juge doit aborder la technique au droit et la configuration judiciaire de la République Démocratique du Congo n’augure en rien un déploiement aisé des mécanismes juridiques assez conséquents dans les instances judiciaires classiques.

1. La cyberattaque.

L’article 4-16 de la loi 20/107 du 25 novembre 2020 dispose que la cyberattaque comme actes malveillants de piratage informatique dans le cyberespace. Une cyberattaque inclue la désinformation, l’espionnage électronique, la modification clandestine des données sensibles ou la perturbation d’infrastructures critiques d’un pays.

Cette définition de la loi demeure non seulement pauvre dans son essence, mais aussi très lacunaire pour laisser les personnes qui manipule la loi à considérer certains actes relevant de la criminalité informatique comme une cyberattaque d’autre pour des simples actes.

Une cyberattaque ne se limite pas uniquement aux données sensibles à la perturbation des infrastructures critiques d’un pays. Elle devient une cyberguerre lorsqu’il s’agit d’un État ou d’une organisation criminelle qui entre en guerre numérique contre un autre État ou une organisation considérée comme ennemies,. Il s’agit d’une cyberattaque quand les infrastructures numériques sont mises à mal par les hackers. Un Ddos ou attaque par dénis de service ne fait pas assez de mal à quelqu’un mais à des organisations et entreprise surtout. D’ailleurs une cyberattaque peut facilement se transformer en cyberterrorisme, mais à dire vrai elle demeure toujours distincte du cyber espionnage, lequel a le mérite de la furtivité et du secret tant par le caractère de déni que représente cet acte criminel que par le refus que manifeste les criminels informatiques quat à la paternité de l’acte.

En 2007, la première cyberattaque visant directement un État est a eu lieu. Un blackout informatique avait frappé l’Estonie, à tel enseigne que les sites de l’administration, les banques et les journaux seront quasiment inaccessible pendant un bon moment. En 2008, c’est autour de la Géorgie de payer les frais d’une cyberattaque à grande échelle ; cette fois-ci presque toutes les infrastructures étaient inopérantes rendant la vie plus compliquée pour les citoyens géorgiens. Toutefois, vu l’importance qu’avait cette cyberattaque en termes de complexité et sophistication, l’on ne pouvait que croire à une attaque provenant d’un autre État[33].

Vers 2010, la conception de cyberguerre commence à prendre une autre tournure lorsque l’agence américaine de cybersurveillance, la NSA, ensemble avec l’unité 8200, une autre agence de renseignement électronique, mais cette fois-ci, israélien ; sur base des inquiétudes de l’occident concernant l’intention iranien sur le nucléaire dont notamment des centrales nucléaires, mais aussi du fait que l’Administration Obama été en froid total avec l’Iran, un virus informatique va être développé pour provoquer un dysfonctionnement des centrifuges nucléaires, conduisant même à leur destruction physique. Ce virus, du nom de stuxnet, avait mis la puce à l’oreille à des entreprises de tous genres ainsi qu’aux États de la menace réelle qu’expose la technologie, mais surtout de la capacité à nuire que pourrait avoir une personne en se servant en mal de son ordinateur[34].

Le virus informatique Stuxnet avait profité d’une faille de sécurité dans le système d’exploitation Windows pour causer des dégâts quantifiables en millions de dollars. En 2017, l’année la plus emblématique dans l’univers des hackers connu essentiellement pour ses trois attaques dont Warnancy, au mois de mai, NotPetya et Industroyer au même mois[35].

L’Afrique semble d’apparence épargnée par les cyberattaques mêmes si certains États ont vu des élections être truquées par des hackers ou des citoyens lambdas être victimes d’escroquerie en ligne à grande échelle avec pour mauvais élevé pour exemple le Bénin et le Nigéria.

La République Démocratique du Congo a connu l’apogée des cyberattaques entre 2019 et 2021. Nos études statistiques, ont abouti à la conclusion que 31% des infrastructures de l’administration sont vulnérable et tourne sur des vieux systèmes d’exploitation qui ne jouissent pas des mesures de sécurités ; 40% des terminaux à usage privé sont infectés et 65% du système informatique tant pour les privés et pour l’administration public fait l’objet de plusieurs fuites des données numériques sans que les auteurs ne soient inquiétés. Le système judiciaire en a même payé les frais. Les décisions des justices sont débattus sur WhatsApp par exemple, et à titre d’exemple, la jugement dans la cause dite Kamerhe, le jugement était déjà rendu public, deux heures avant son prononcées .

Cet acte criminel ont toujours un fonctionnement propre à eux, l’on parle de fonctionnement d’une cyberattaque, qui du reste nécessite non seulement des connaissances pratiques mais aussi des outils adéquates puisque la cyberattaque ne peut se concevoir sans base.

2. Fonctionnement d’une cyberattaque.

Une cyberattaque nécessite des ressources adéquates en termes de matériels, du personnel, mais aussi des compétences techniques. Si le Hacker ose espérer sur son seul ordinateur, il risque de passer plusieurs années pour parvenir à déchiffrer certains systèmes de sécurité dont le niveau de sécurité et de sophistication est très avancé. Pour le Hacker, le temps restera à jamais son ennemie numéro un puisque tous les délinquants informatiques préfèrent passer d’une activité à une autre afin de s’en mettre plein les poches.

Pour ce faire, plusieurs techniques sont effectuées pour permettre de gagner en temps. Des Hackers financés par des organisations criminelles ou des organismes privés voire étatiques sont n’ont généralement pas des difficultés à ses procurer des matériels informatiques qui coutent trop souvent cher. Pour les autres, l’imagination est toujours une bonne solution et c’est là qu’intervient la magie de l’informatique.

Le Hacker qui veut procéder à une cyberattaque peut utiliser les terminaux[36] ne lui appartenant pas comme une machine zombie[37] seulement si ces machines sont en réseau et ainsi faciliter l’exécution de l’attaque visée ce, grâce à un rootkit[38] déjà installé sur toutes ces machines zombies et la plupart des cas c’est un moyen très usuel pour hackers.

Ce comportement criminel de prise de contrôle d’un ordinateur d’un inconnu qui, lui-même, n’est au courant de rien, est une violation grave de l’atteinte à la vie privée, mais aussi et surtout une forme de criminalité frôlant l’association des malfaiteurs dès lors qu’ils agissent en groupe parce que l’intention est de nuire aux personnes ou aux propriétés.

3. Techniques des cyberattaques.

Il s’agit pas d’un secret ni moins d’un mythe comme on le croyait avant les années 1970, les hackers (criminels informatiques) sont friands des techniques les plus complexes pour mettre à rude épreuve et les États et les particuliers lors de la traque contre eux.

Prenons un cas, celui de la société russe Kaspersky accusée de voler des données personnelles de ses abonnées pour le revendre à la FSB, il s'agissait là d'un acte avéré non seulement d'espionnage, mais aussi d'atteinte à la vie prive, car, au moins le Gouvernement américain était obligé de chasser des diplomates russes de son sol ce qui lui a couté le revers de son acte[39].

Or, à un moment donné, entre la période allant de 2016 à 2020, Kaspersky était devenu l'antivirus par excellence des Congolais et des africains en général à tel point que même les ordinateurs payés par les utilisateurs embarquaient déjà un antivirus Kasperky. Quant à Avast, elle demeure l'antivirus gratuit le plus populaire, mais aussi le plus gourmand en termes de collectes de données numériques des utilisateurs. Derrière des entreprises ou ces organisations privées ou publiques, on y retrouve aussi des hackers, qui offrent des services criminels notamment la révente des données. Ces criminels avérés sont souvent à la solde de leurs patrons pour purger leurs peines faute de pas survivre longtemps en prison. Ainsi donc, il en existe des pléthores puisque les Hackers aiment recourir à des techniques très sophistiques ou parfois très simples dans le seul but de se faire de l'argent.

B. L'analyse des règles de compétence répressives en matière de cybercriminalité.

Pour les infractions commises en ayant recourt aux applications informatiques, une partie de la doctrine estime que la question du droit pénal international applicable aux infractions commises par Internet est à la fois simple et extrêmement complexe[40]. Cette position de la doctrine se justifie par le fait que l'application des règles juridiques est assez simple dans la mesure où il existe une unité de solutions entre compétences juridictionnelle[41] et la loi applicable, mais la difficulté s'accroît lorsqu'il s'agit de lutter de manière de la coordination à l'échelle internationale de la lutte contre la cybercriminalité.

1. Du principe de rattachement applicable à la cybercriminalité.

Le principe de rattachement tire sa source du droit international, mais dans notre système interne, c'est l'article 3 qui fait ressortir les effets juridiques de ce principe, mais de manière partielle. Ce principe permet de résoudre la difficulté de l'entraide judiciaire en l'absence d'un accord si l'on est en présence d'une infraction relevant de la cybercriminalité.

Le principe de la règle de rattachement consiste en ceci que le juge d'un État peut dès lors que les faits criminels reprochés à un délinquant sont établis justifier de sa compétence à connaitre de la cause parce qu'il est compétent d'un point de vue territorial (*ratione loci*), ou lorsqu'il y a extension de la compétence territoriale.

L'évolution de la procédure pénale en droit belge et droit français a contribué largement à faire asseoir ce principe de rattachement d'une infraction au droit interne.

Olivier Michiels opine que pour le droit belge, les articles 6 à 14 du titre préliminaire du Code de Procédure pénale, permettent, dans les cas qu'elles déterminent et selon les modalités qu'elles fixent, la poursuite d'un Belge pour des infractions commises à l'étranger ou pour des infractions commises par des étrangers à l'étranger[42]. D'ailleurs L'article 10, 5° du titre préliminaire du Code de procédure pénale permet, quant à lui, la poursuite en Belgique d'un crime commis à l'étranger par un étranger contre un ressortissant belge si le fait est punissable en vertu de la législation du pays où il a été commis d'une peine dont le maximum dépasse cinq ans de privation de liberté[43].

Ce principe de compétence que l'on trouve aussi en droit français règle de manière équivoque la difficulté de poursuite des étrangers ayant commis des infractions à l'étranger dont les victimes sont sur le sol belge ou français.

Le Professeur Bernard Bouloc, souligne que s'agissant d'une infraction commise à l'étranger par un étranger, les juridictions répressives françaises ne sont pas en principe compétentes puisqu'aussi bien l'ordre social français n'a pas été troublé, et cela même si cet étranger réside en France. Le simple fait qu'une connexité avec certains faits commis en France ne suffit pas à rendre le juge pénal français compétent[44].

Il renchérit d'ailleurs que c'est qu'exceptionnellement, pour des considérations d'intérêt national, que les juridictions répressives françaises peuvent juger, en application des lois pénales françaises, un étranger qui s'est rendu coupable à l'étranger, soit comme auteur, soit comme complice, d'un crime ou d'un délit qualifié d'atteinte aux intérêts fondamentaux de la Nation… de même par dérogation, pour connaitre des infractions commises à l'étranger par un étranger, l'étranger qui, hors de la République, s'est rendu coupable d'un crime, ou d'un délit puni d'emprisonnement peut être poursuivi et jugé d'après les dispositions des lois françaises (c.pén. art. 113-7), lorsque la victime de cette infraction est française. L'on parle dès lors de la personnalité passive de compétence de juridiction[45].

Dans notre système juridique, la question ne se pose pas lorsque le criminel est sur le sol congolais et a eu à commettre une infraction prévue par nos lois pénales ou encore lorsqu'il est sur le sol congolais, mais qu'il aurait commis une infraction à l'étranger.

À la question de savoir quand il s'agit des infractions commises à l'étranger par un étranger dont les victimes sont congolaises, nos recherches conclue un silence du côté législateur tant pour le Code pénal, que pour le code de procédure pénale ou même des lois qui traitent de l'organisation juridicier à tel enseigne que même la nouvelle loi sur la télécommunication est dénudée de son sens dans la lutte contre la Cybercriminalité.

Aujourd'hui par exemple, l'on fait face à des pratiques d'extorsion, de vol, d'escroquerie, de harcèlement, d'association des malfaiteurs… commis par des étrangers, par des étrangers sur des victimes congolaises. Ces pratiques criminelles sont telles que les auteurs sont souvent en dehors du sol congolais, mais les effets de ces actes se font sentir sur notre sol où réside la victime. La règle de rattachement justifie alors d'application quant l'article 3 du Code pénal qui du reste se doit d'être observé de manière motu proprio avec une interprétation stricte même si elle ne suffit pas. Lorsque le lieu de l'émission se retrouve, en dehors du sol congolais, si les actes criminels ont un point de contact avec le sol congolais, considéré ici comme lieu de réception ; nous pensons que le juge congolais sans qu'il ait besoin de procéder au principe de la territorialité est compétent dès par l'article 3 du Code pénal congolais si le criminel a au moins une résidence sur le sol congolais, mais dans le cas contraire il se doit d'éviter d'appliquer la compétence dite de la personnalité passive puisque jamais prévue par notre droit.

2. Règle applicable aux infractions réputées en contact avec le territoire de la République Démocratique du Congo ou applicables en droit congolais.

Le recours au droit international pénal permet d'avoir une appréhension sur ce principe, mais uniquement pour les cas des infractions prévues par le Titre III et Titre VIII de notre code pénal comme l'indique l'article 3 en son dernier aliéna. Si toute infraction qui présente à la fois un élément d'extranéité et un point de contact avec la République Démocratique du Congo peut être de la compétence des juridictions congolaise avec application du droit congolais dans une certaine mesure notamment en ce qui concerne les infractions contre la foi publique et celles qui sont contre la sûreté de l'État. Donc, il n'en demeure pas moins que la lecture formaliste du droit pénal doit rester une priorité pour éviter les analogies que le Doctrinaire Esika makombo n'a cessé de dire dans ses études.

Dans la deuxième édition de son ouvrage, le Professeur Nyabirungu fait évidemment une analyse du principe de la compétence passive des juridictions congolaises, mais à la seule condition que la victime soit l'État congolais[46].

Il se constate de ce fait un sérieux problème avec les infractions du cyberespace couramment appelé cybercriminalité, elles répondent souvent à une théorie double, celle de l'émission et de la réception. Les hackers agissent rarement contre le pays qui les accueille ou dont ils sont originaires. Avec la sophistication des technologies numériques, la vulgarisation de l'anonymisation avec des VPN dont les plus puissants Tor ou NordVPN, le lieu de l'émission demeurent une équation sans précédent pouvant mettre plus de temps pour les appréhender. Voilà pourquoi, il est fort rare d'entendre qu'un cybercriminel est devant les instances judiciaires et prenant compte de la réalité dans notre pays, les Congolais ont un parcours à faire pour être protégés comme les criminels informatiques qui œuvrent à l'étranger.

3. De la loi applicable et la participation criminelle.

Lorsque l'infraction est réalisée de manière concertée par plusieurs personnes, on entre dans ce qu'on appelle la participation criminelle. En d'autres termes, la participation criminelle est concevable lorsque plusieurs personnes ont contribué à la commission d'une infraction en y prenant une part plus ou moins active et directe.

La participation criminelle est, cependant, prévue dans le droit congolais par les articles 21 à 23 du Code pénal. Elle peut se présenter sous deux formes : la coactivité autrement dit la corréité : lorsque la contribution s'avère directe ou indispensable ; la complicité : lorsque l'aide apportée, sans être nécessaire, est néanmoins utile. Ces deux formes de participation criminelle se réalisent selon les modes spécifiques limitativement énumérés par les articles 21 et 22 du Code pénal. Il est disposé que sont considérés comme auteurs d'une infraction :

- ceux qui l'auront exécutée ou qui auront coopéré directement à son exécution;

- ceux qui, par un fait quelconque, auront prêté pour l'exécution une aide telle que, sans leur assistance, l'infraction n'eût pu être commise;

- ceux qui, par offres, dons, promesses, menaces, abus d'autorité ou de pouvoir, machinations ou artifices coupables, auront directement provoqué cette infraction;

- ceux qui, soit par des discours tenus dans des réunions ou dans des lieux publics, soit par des placards affichés, soit par des écrits, imprimés ou non et vendus ou distribués, soit par des dessins ou des emblèmes, auront provoqué directement à la commettre, sans préjudice des peines qui pourraient être portées par décrets ou arrêtés contre les auteurs de provocations à des infractions, même dans le cas où ces provocations ne seraient pas suivies d'effets.

Et les articles 22 et 23 il est renchérissent que seront considérés comme complices :

- ceux qui auront donné des instructions pour la commettre;

- ceux qui auront procuré des armes, des instruments ou tout autre moyen qui a servi à l'infraction sachant qu'ils devaient y servir;

- 3°. ceux qui, hors le cas prévu par l'alinéa 3 de l'article 22, auront avec connaissance aidée ou assisté l'auteur ou les auteurs de l'infraction dans les faits qui l'ont préparée ou facilitée ou dans ceux qui l'ont consommée;

- 4°. ceux qui, connaissant la conduite criminelle des malfaiteurs exerçant des brigandages ou des violences contre la sûreté de l'État, la paix publique, les personnes ou les propriétés, leur auront fourni habituellement un logement, lieu de retraite ou de réunion.

Sauf disposition particulière établissant d'autres peines, les coauteurs et complices seront punis comme suit :

- les coauteurs, de la peine établie par la loi à l'égard des auteurs;

- les complices, d'une peine qui ne dépassera pas la moitié de la peine qu'ils auraient encourue s'ils avaient été eux-mêmes auteurs;

- lorsque la peine prévue par la loi est la mort ou la servitude pénale à perpétuité, la peine applicable au complice sera la servitude pénale de dix à vingt ans

La participation criminelle n’est concevable et punissable que si elle consiste à favoriser l’accomplissement d’une infraction, c’est-à-dire, un acte que la loi condamne et sanctionne d’une peine. Cette infraction principale doit être consommée ou simplement tentée. Il importe peu que l’infraction soit imputable à l’auteur principal. Ainsi, un participant pourra être condamné pour une infraction dont l’auteur matériel a été acquitté pour cause de non-imputabilité ou absence de l’élément moral. Si l’acte principal n’est pas une infraction, on ne peut parler de la participation criminelle.

On ne peut parler de la participation criminelle dans le chef de celui qui vient au secours de son prochain injustement agressé. Il en est de même de celui qui apporte son aide à un individu qui se suicide. Toutefois, certaines observations circonstanciées ou qualifiées sont retenues comme de participation lorsque, à l’analyse, elles s’avèrent revêtir un aspect positif[47].

En outre, un arrêt de principe de la Cour de cassation française estime que la complicité à l'étranger d'un acte principal commis en France est passible de poursuites et de condamnation en France [48].

Pour notre système pénal, dès lors que la participation criminelle est établie, que l’on se trouve à l’étranger comme c’est le cas avec les infractions numériques, ou sur le sol congolais, l’application des articles 21 à 23 du Code pénal congolais livre I nous est opposable et justifierait même

l'entrée en lice de l'article 3 du même code pour définir la compétence du juge surtout quand le caractère d'extranéité est ressorti.

Il s'en suit avec logique que cette justification de l'application de la loi pénale partant de l'ordonnance 243/87 de 1987 relative aux activités informatiques en République Démocratique du Congo, dès lors qu'il est établi qu'une application informatique a été utilisée pour commettre les actes contraires à la loi.

Donc une justification légale a été dès lors déjà été trouvé et d'aucuns ne pourra en contester la validité d'une législation pénale en rapport avec la cybercriminalité dans notre système pénal.

CONCLUSION.

Tout au long de notre étude, nous avons relevé plusieurs aspects aussi bien techniques que pratique qui justifient les difficultés rencontrées par l'Etat congolais à lutter de manière efficace contre la criminalité informatique.

En effet, la cybercriminalité connait une hausse en ce qui concerne son taux par rapport à la criminalité classique tant en ce pour les actes criminels que pour les préjudices causés. Toutefois, le système judiciaire souffre d'un déficit décriant aussi bien pour son personnel judiciaire (Magistrats du parquet et de siège, officier de police judiciaire, etc…) et force est de constater que le système pénal congolais au lieu de lutter contre la cybercriminalité comme c'est le cas en France ou au Ruanda, en injectant plus d'argent pour une mise à niveau du système, l'on s'attelle souvent à porter critique sur la victime et enfin de compte, l'auteur du crime demeure pour la plupart du temps impuni. L'on vit donc une impunité numérique en République Démocratique du Congo.

Cette étude sur la cybercriminalité cherche à soulever les questions pertinentes relative à l'inefficacité du système pénal congolais à lutter contre cette forme de criminalité. Malgré l'adoption de la loi n°20/017 du 25 novembre 2020 relative aux télécommunication et aux technologie de l'information et de la communication, l'on assiste à une effectivité de la loi presque théorique que pratique, raison pour laquelle il a été impérieux de faire ladite étude parce que la criminalité informatique, faute d'être régulier, elle devient aussi dévastatrice que la criminalité classique, avec un risque tel que l'on peut facilement assister à un trouble à l'ordre public voire même à une atteinte de la sûreté de l'Etat.

[1] L'article 4-30 dispose que le cyberterrorisme est une action préméditée des activités perturbatrices, ou la menace de celles-ci contre les ordinateurs et/ou réseaux, un État, pour intimider toute personne physique ou morale, dans l'intention de causer un préjudice social, idéologique, religieux, politique ou encore des objectifs similaires.

[2] L'Attentat à la bombe de Mogadisco, le 14 octobre 2017 par des terroristes avaient fait au moins 600 victimes (blessées ou mortes), la réclamation en paternité attribuée à Harakat al-Chabab al-Moudjahidin (Shebab), de cet acte abominable s'est fait d'abord sur le darkweb avant d'être relayé sur le deepweb,

[3] La messagerie Signal oppose une fin de non recevoir à la justice américaine, https://www.usine-digitale.fr/article/la-messagerie-securisee-signal-refuse-de-transmettre-des-donnees-a-la-justice-car-elle-ne-les-a-pas.N1156767 , consulté le 11 novembre 2021.

[4] Le cloud computing, en français « informatique en nuage » (ou nuagique ou encore infonuagique au Québec), consiste à utiliser des serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet, pour stocker des données ou les exploiter.

[5] Le revenge porn, ou pornodivulgation1 en français, est un contenu sexuellement explicite qui est publiquement partagé en ligne sans le consentement de la ou des personnes apparaissant sur le contenu2,3, dans le but d'en faire une forme de « vengeance ». Le revenge porn peut être mis en ligne par un ex-partenaire avec l'intention d'agresser ou d'embarrasser la personne sur la photo ou la vidéo. Elle peut aussi être mise en ligne par un pirate qui exigera une somme d'argent *pour supprimer le contenu exposé. Lire KEITH COFFMAN, Colorado Lawmakers Advance Bill To Crack Down On 'Revenge Porn',* Huffington Post" (June 24, 2014), consulté le 11 novembre 2021

[6] TGI Nanterre, 12e ch., [18 mai 2000], ministère public c. Jacques L., Comm. Com. Electr. [Novembre 2000], p. 21. Commentaire de Jean Christophe GALLOUX., cité par Célestin Serugendo Kifende, cybercriminalité et criminalité technologique, Cours destiné aux étudiants de MASTER I (S.I. & C.E.E.), École de criminologie, Lubumbashi, 2017, p.16

[7] E. DUPOND MORETTI, le dictionnaire de ma vie, Ed. Kero, 2018, p. 47

[8] Il existe même des prestaires web qui offrent des cours et manuels pour faire du carding cashout. Le plus connus, hors du deep web est justement le site web https://www.carding-cashout.com/ disponible en consultation libre.

[9] La cybersécurité est au sens de l’article 4-29 de la loi 20/017, l’ensemble des mesures de prévention, de protection et de dissuasion notamment d’ordre technique, organisationnel, juridique, financier, humain et procédural permettant d’atteindre les objectifs de sécurité fixés à travers les réseaux de télécommunications et de technologie de l’information et de la communication, les systèmes d’information, et dans l’écosystème numérique national et international, en vue d’assurer la protection de la vie privée des personnes et des activités effectuées, de manière générale, dans le cyberspace.

[10] https://actualiteinformatique.fr/cybersecurite/ consulté le 11 novembre 2021.

[11] En Cybersécurité, une faille 0day fait partie des failles informatiques non encore résolues ou qui ne sont pas encore découvertes par les constructeurs informatiques dans les systèmes informatiques conçus par eux. La découverte d’une faille 0days est une aubaine pour les hackers, soit il le communique à l’entreprise pour la corriger c’est le cas des White Hat, mais les autres peuvent le vendre ou les même les utiliser personnellement.

[12] R. STAMBOLISKA, *la face cachée d’internet,* Ed. Larousse, Paris 2017, pp.8-9.

[13] H. ALTERMAN et A. BLOCH, La fraude Informatique, Paris, Gaz. Palais, 1988, p. 530.

[14] A. LUCAS, Le Droit de l'Informatique, Paris, PUF, 1987.

[15] Article 4-25 de la loi n°20/017 relative aux télécommunication et technologies de l'information et de la communication du 25 novembre 2020, in JORDC, numéro spéciale du 25 septembre 2021

[16] Désigne les protocoles communs de communication utilisés par l'Internet, permettant l'interconnexion généralisée entre réseaux hétérogènes.

[17] Il s'agit d'une définition donnée par le ministère de l'Intérieur Français disponible, sur http://www.interieur.gouv.fr

[18] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », [10 – 17 avril 2000], disponible sur http://www.uncjin.org/., consulté le 10 mars 2020

[19] J. COLOMBAIN, Faut-il quitter les réseaux sociaux ?, les 5 fléaux de Facebook, Twitter, Instagram et Youtube, Editions Dunod, 2019, pp.36-124.

[20] Rapport d'analyse stratégique, [Octobre 2001].

[21] Centre canadien de la statistique juridique, disponible à l'adresse : http://collection.nlc-bnc.ca/ , consulté le 18 mars 2020.

[22] U.S. Department of Justice http://www.justice.gov/

[23] Code pénal de l'État de Californie (section 502).

[24] Code pénal de Texas (section 33.02).

[25] G. ROMAIN : La Délinquance Informatique : Où en Est-on ? (Sécurité Informatique), [Juin 1998], n° 20, p. 1.

[26] D. WALL, Crime and the Internet , Routledge, New-york, 2001] p. 3.

[27] Conformément au principe de légalité des infractions (nullum crimen sine lege) et des peines (nulla poena sine lege), les dispositions du droit pénal sont, en effet, d'interprétation stricte : elles ne peuvent être interprétées de manière extensive ou analogique et ainsi appliquées à des situations non visées par la lettre du texte. Une interprétation évolutive ou téléologique est toutefois possible, pourvu que soit respectée, d'une part, l'intention du législateur, d'autre part, la lettre du texte concerné : « Le juge peut appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de pressentir à l'époque de la promulgation de la disposition pénale, à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit

certaine et que ces faits puissent être compris dans la définition légale de l'infraction » (Cass., 15 mars 1994, Pas., 1994, I, p. 261). Avant l'adoption de la loi du 28 novembre 2000, des juges — dont on attend toujours plus qu'ils soient les gardiens de nos libertés dans un monde en mutations — n'ont pas hésité à adapter le sens de certaines dispositions aux nouvelles formes de délinquance issues de l'évolution technologique (On songe notamment à la prévention de « vol » applicable, en principe, à des objets matériels et qui a été appliquée — sans unanimité — à des biens immatériels tels que des données et programmes informatiques). On devine aisément combien la marge est étroite entre une interprétation évolutive des règles pénales et une interprétation extensive ou analogique. Sur l'interprétation en matière pénale, F. TULKENS et M. VAN DE KERCHOVE, Introduction au droit pénal, 4e éd., Diegem, Kluwer, 1988, pp. 221 et s.

[28] E. MAKOMBO, Le code pénal Zaïrois annoté, Lubumbashi, (Ae), 1997, pp.67 et 68.

[29] Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la com

[30] https://www.larousse.fr/dictionnaires/francais/logiciel/47666

[31] La première conséquence du principe de la légalité des incriminations et des peines, c'est l'interdiction faite au juge d'imaginer et suppléer aux textes répressifs ainsi que cela a été précisé au IV^{e} congrès international de droit pénal, l'interdiction de combler les lacunes des textes qui renferment les incriminations, qui déterminent les peines ou qui prévoit les causes d'aggravation de celle-ci. Esika Makombo, op.cit. p.18

[32] N. MWENE SONGA, droit pénal général zairois, Ed. DES (Droit et société), Kinshasa, 1989, pp.378-386.

[33] https://www.lemonde.fr/europe/article/2007/06/27/l-estonie-tire-les-lecons-des-cyberattaques-massives-lancees-contre-elle-pendant-la-crise-avec-la-russie_928568_3214.html;

[34] R STAMBOLIYSKA, op.cit. pp.87 à 110.

[35] https://www.informatiquenews.fr/10-cyberattaques-ont-marque-lannee-2017-55112

[36] Entendre ici, tout objet numérique tournant sur un système d'exploitation, connecté à Internet et capable de fonctionner de manière autonome ou pas. Il peut s'agir des ordinateurs, téléphones, vehicules connectés, serveurs de l'armée ou d'un État, base des données, etc.

[37] Une machine zombie est un terminal tournant sur système d'exploitation ayant une faille de sécurité dont profite le hacker pour l'utiliser à l'insu de son propriétaire aux fins de lui aider à effectuer des taches plus complexes le plus rapidement possible.

[38]

[39] Disponible sur https://www.silicon.fr/lantivirus-kaspersky-complice-ou-victime-dun-vol-de-donnees-de-la-nsa-186223.html,

[40] . C. Castets-Renard, Droit de l'Internet : droit français et européen, 2e éd., Montchrestien, 2012, no 961 s. et no 1070 s. ; D. CHILSTEIN, Droit pénal international et lois de police, Essai sur l'application dans l'espace du droit pénal accessoire, Dalloz, coll. « Nouvelle Bibliothèque de Thèses », 2003 ; V. FAUCHOUX, P. Deprez, J.-M. BRUGUIERE, Le droit de l'Internet, 2e éd., LexisNexis, 2013, no 99 s. ; J. Huet, E. Dreyer, Droit de la communication numérique, LGDJ, 2011, no 207 s. – J. Francillon, « Le droit pénal face à la cyberdélinquance et à la cybercriminalité », RLDI 2012/81 no 2728 ; A. Huet, « Droit pénal international et Internet », in Mélanges en l'honneur de Philippe Kahn, Litec, 2000, p. 663 s. ; A. LEPAGE, « Droit pénal et Internet : la part de la tradition, l'œuvre de l'innovation », AJ pénal 2005. 217 s. ; M. VIVANT, « Cybermonde : droit et droits des réseaux », JCP 1996, I, no 3969.

[41] L. BAMBI LESSA, Manuel de procédure pénale, PUC, 2è trimestre, Kinshasa, 2011 Dépôt légal n°: M/3.01105-57089 , N° ISBN : 99951-15-16-6,.

[42] Voir M. FRANCHIMONT, A. JACOBS et A. MASSET, Manuel de procédure pénale, Collection de la faculté

de droit de Liège, Larcier, 4ed, 2012, pp. 1444-1462, cité par Olivier Michiels et Elodie Jacques, les principes de droit pénal, 3e éd, notes de Cours, Université de Liège, p.20., voy aussi Sur l'avis officiel lorsque l'infraction a été commise contre un étranger voir Cass., 7 avril 2004, Rev. dr.pén., 2004, p. 851.

[43] Idem.

[44] La Cour de cassation française avait estimé qu'une décision de classement sans suite d'une juridiction allemende ne s'oppose pas au jugement en France de l'auteur des faits ; Cass. 2 avr. 2014, Bull, n°101, D. 2014. 1128, note D. BrachèThiel. Voy B. BOULOC et Coll., Précis de Procédure Pénale, 27e éd , Dalloz, 2020, p.598

[45] B. BOULOC, op.cit.p.598.

[46] Nyabirungu Mwene Songa, Droit pénal général, 2e éd., p.126. ? L'auteur se réfère à MERLE et VITU, lesquels soutiennent que le système de la personnalité passive est dit aussi principe de la réalité lorsque la victime dont la loi doit s'appliquer est l'État lui-même. Voy MERLE & VITU, Traité de droit criminel, cujas, Paris, 1967, 1980, 1999, 1997.

[47] STEFANI (G), LEVASSEUR (G) et BOULOC (B), Droit pénal général, 11e éd., Dalloz, Paris, 1980 et 13e éd., 1987, p. 257.

[48] . Arrêt de principe en matière de presse, Crim. 30 avr. 1908, préc.