NOTION DE CYBERCRIMINALITE : PRAXIS D'UNE PENALISATION DE LA DELINQUANCE ELECTRONIQUE EN DROIT PENAL CONGOLAIS.

PAR MITONGO KALONJI Trésor-Gauthier

- Licencié en droit
- Responsable de la salle informatique ScienceNet de la faculté des sciences

Université de Lubumbashi

Blog : www.tgk.centerblog.net E-mail : kalonjit@unilu.ac.cd; tgk720@gmail.com; tel : +243 993197078

INTRODUCTION GENERALE

Le millénaire actuel reste prédominé par l'apparition des *(nouvelles) technologies de l'information et de la communication* (NTIC)[1] qui s'avèrent omniprésentes, et dont la tendance à la numérisation va grandissant. *Internet*[2] en est l'une des infrastructures techniques dont l'explosion et la croissance sont très *spectaculaires*[3]. La demande de connectivité à Internet et d'interconnexion des *systèmes*[4] a conduit à l'intégration de l'*informatique*[5] dans des produits qui, jusqu'alors, en étaient dépourvus, notamment les *voitures*[6] et les *bâtiments*[7].

[1] Les expressions « technologies de l'information et de la communication (TIC), « nouvelles technologies de l'information et de la communication » (NTIC) ou encore « information technologies » (IT) désignent tout ce qui relève des techniques utilisées dans le traitement et la transmission des informations, principalement l'informatique, l'internet et les télécommunications. [Source : http://www.techno-sciences.net/?onglet=glossaire&definition=10714 (consulté le 9 juillet 2010)]

[2] Internet est le réseau informatique mondial qui rend accessibles au public des services comme le courrier électronique et le world wide web (w w w). Ses utilisateurs sont désignés par le néologisme « internaute ». Techniquement, Internet se définit comme le réseau public mondial utilisant le protocole de communication IP (Internet Protocol).
Le nom Internet vient de INTERconnected NETworks (en français : réseaux interconnectés). L'usage francophone est d'écrire le mot avec une majuscule et sans article, bien que ce ne soit pas plus un nom propre qu'une marque. [Lire le dossier « Internet » sur http://www.techno-science.net/?onglet=glossaire&definition=4008 (consulté le 9 juillet 2010)]

[3] En effet, Internet est né efficacement en 1990 ; mais déjà à ces jours (2010), les statistiques déchiffrent plus de 940 millions d'internautes qui feraient partie d'un réseau social seulement. (Source : http://www.statistique-mondiales.com/apcopos.htm : consulté le 9 juillet 2010).

[4] En langage plus simple, un Système d'information ou système informatique est un ensemble des programmes (fonctionnalités) qui permettent de faire fonctionner un ordinateur, en mettant à la disposition de l'utilisateur les fonctions de base les plus courantes.

[5] Mot-valise créé par P. DREYFUS en 1962 et reconnu par l'Académie française en 1966 sous la définition suivante : « Science du traitement rationnel, notamment par machines automatiques, de l'information considéré comme support des connaissances humaines et sociaux ». (Voir la définition du mot « Informatique » dans le dictionnaire informatique DICO, disponible sur http://dictionnaire.phpmyvisites.net : consulté le 9 juillet 2010).

[6] Notamment avec l'automatisation des portières. Lorsque le véhicule a dépassé un seuil maximal de vitesse, les portières se verrouillent automatiquement. Inversement, pour certains véhicules, lorsque les portières ne sont pas convenablement verrouillées, il ya disfonctionnement de certains dispositifs…

Il n'est point question, dans cette étude, de procéder à une apologie d'Internet ; néanmoins il est pertinent de mentionner qu'au regard de l'avalanche des bienfaits qu'il accorde à ses millions d'utilisateurs disséminés à travers le monde, c'est devenu un outil dont on ne peut se passer ; quasiment tous les services du monde moderne en dépendent directement ou indirectement. A ce propos, l'on peut sans doute citer, entre autres, la *distribution d'électricité*[8], les *infrastructures de transport*[9], les *services (même logistiques) des armées*[10], la *médecine*[11],… la *justice*[12] ou le Droit en général.

Malheureusement, toute invention humaine porteuse de progrès peut être aussi génératrice de comportements illicites. Le coté élogieux d'internet occulte la face la plus redoutable ; et parmi les menaces liées à cet outil, une se démarque par sa dangerosité et sa complexité : la ***cybercriminalité*** [13]. Celle-ci est l'une des nouvelles formes de criminalité ou de *délinquance*[14] sur le réseau Internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité humaine. De toute évidence, *COLIN ROSE*[15] souligne que « la cybercriminalité est la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires »[16]. C'est « un véritable *tsunami*[17] informatique au regard des dégâts et pertes qu'elle occasionne »[18],

[7] Il en est de même pour les bâtiments. Certaines portes ne s'ouvrent qu'à l'approche d'un obstacle qui peut être un individu ou un objet…

[8] Avec notamment l'automatisation des postes électriques améliorant ainsi la fiabilité du service électrique tout en réduisant les coûts opérationnels et de maintenance.

[9] Avec l'apparition de la monétique, il est désormais possible de payer les frais de transport à domicile ou à quelques mètres de chez soi, sans pour autant se déplacer vers une agence de transport.

[10] Actuellement l'on rencontre sur Internet des sites des différentes armées, permettant aux internautes de s'enquérir, par exemple, sur les dates de recrutement, etc. Nous pouvons citer antre autres le site officiel de recrutement de l'Armée de terre (France) qui est le www.recrutement.terre.defense.gouv.fr

[11] Il est désormais possible pour un médecin de donner un avis médical via un site Internet ou par échanges de mails entre son patient et lui. D'ailleurs, grâce à Internet, le jargon médical est enrichi de nouveaux concepts tels que celui d'Internet médical, etc.

[12] Internet peut être utilisé par un avocat par exemple, comme une banque des données juridiques permettant l'accès aux textes législatifs et réglementaires, à la jurisprudence (…). [Voir Emery MUKENDI WAFWANA, « Avocats congolais sur Internet : information ou publicité ? », disponible sur www.Juriscom.net , 15 Juin 2000 (consulté le 20 juillet 2010)]

[13] Dans cette étude, nous utiliserons indistinctement les concepts de cybercriminalité, cyberdélinquance, délinquance électronique, etc. (voir infra note…)

[14] Nous préférons le terme de délinquance à celui de criminalité, compte tenu de l'approche juridique du thème sous analyse.

[15] Chercheur écossais dans le domaine de la piraterie sur Internet.

[16] Colin ROSE, cité par Mohammed CHAWKI, **Essai sur la notion de cybercriminalité**, IEHEI, Juillet 2006, p.2 (disponible sur le site www.iehei.org).

[17] *Tsunami* : terme japonais désignant une « vague gigantesque, souvent destructrice, résultant habituellement d'un tremblement de terre ou d'un volcan sous-marin ; aussi appelé raz-de-marée » (voir la définition de tsunami dans le glossaire disponible sur www.dfo-mpo.gc.ca). Ce terme est employé par MUKADI pour, estimons-nous, marquer l'ampleur du danger que revêt le phénomène cybercriminalité

souligne un spécialiste congolais en cybercriminalité. « En plus, estime toujours ce dernier, il ne serait pas exagéré de la qualifier de *SIDA*[19] numérique ou informatique »[20].

Parler de la cybercriminalité est assez délicat, puisqu'il s'agit d'une notion émergente, dont la conceptualisation est assez complexe. Nous verrons que cette notion est polymorphe, car elle peut concerner aussi bien des infractions *classiques ou conventionnelles*[21] commises par le biais d'Internet, que de nouvelles infractions nées de l'essence même de cet outil informatique. Ainsi donc, cette oscillation entre la nouveauté et le classique ou le conventionnel, soulève une certaine confusion quant à la nature du concept de la cybercriminalité et suscite des interrogations inédites quant à l'adéquation entre le droit pénal classique et la délinquance informatique : faudrait-il ingénieusement assimiler les différentes inconduites de la cybercriminalité aux infractions classiques codifiées dans l'arsenal du droit pénal ; ou, inversement, faudrait-il considérer la cybercriminalité comme un décor d'infractions nouvelles ou naissantes, à incriminer et à intégrer spécifiquement au code pénal ? Comment donc adapter le Droit pénal à la cybercriminalité, alors que celui-là reste figé à des principes cardinaux tels que ceux de **légalité criminelle** et de **stricte interprétation de la loi pénale**, etc. ; et que celle-ci (cybercriminalité) est une notion fuyante, évolutive, malaisée à contenir par des principes classiques du droit pénal?

Voilà miette de questions suscitées par la cybercriminalité, auxquelles le juriste moderne en général, et congolais en particulier reste, au quotidien, confronté. La présente étude prend position sur toutes ces préoccupations, et dans cette approche, nous envisagerons une opportunité, d'abord, d'incrimination au code pénal congolais de nouvelles infractions nées de NTIC, et ensuite d'adaptation du code pénal congolais aux NTIC, c'est-à-dire une requalification et redéfinition des certaines infractions par rapport à l'évolution de la délinquance facilitée par les NTIC. Dans une démarche scientifique de mise en valeur d'un terrain de recherche quasiment complexe, nous plaiderons particulièrement pour une pénalisation du vol des données et informations numériques, c'est-à-dire le vol opéré dans l'espace virtuel dont l'internet est le principal moyen.

---

[18] MUKADI MUSUYI (Emmanuel), « La cybercriminalité est une réalité en RDCONGO », article disponible sur http://www.digitalcongo.net/article/47215. (Consulté le 8 juillet 2010).

[19] *SIDA* : Syndrome d'Immuno Déficience Acquise. Maladie due à l'infection par le virus VIH. La transmission du virus se fait par voie sexuelle, sanguine et materno-fœtale. Le virus entraine une défaillance du système immunitaire permettant l'apparition des maladies opportunistes et des cancers. Nous estimons que MUKADI compare le SIDA à la cybercriminalité compte tenu de dégâts que celle-ci cause aux systèmes informatique au moyen des infections informatiques et autres.

[20] MUKADI MUSUYI, « Cybercriminalité, le SIDA informatique », Revue LUBILA N°001 du 18 au 31 Janvier 2008, disponible sur http://www.lepotentiel.com (consulté le 8 juillet 2010).
Ce chercheur congolais en technologie de l'information et de la communication et spécialiste en cybercriminalité note ce qui suit : « *plus que jamais, la cybercriminalité s'érige toutes proportions gardées, en « SIDA » de l'informatique, car comme la redoutable pandémie, elle est tout aussi mondiale, transnationale, tentaculaire, endémique, budgétivore qu'invaincue(…) »*

[21] Nous appelons infractions classiques ou conventionnelles, toutes celles qui sont inscrites au code pénal.

Pour ce faire, en vue de mieux cerner le thème sous analyse, nous nous proposons de le saucissonner en trois fractions dont voici la teneur :

I. LA CYBERCRIMINALITE : UNE DELIQUENCE ELECTRONIQUE.

La *mondialisation*[22] revêt plusieurs aspects dont le plus scintillant reste l'apparition des nouvelles technologies de l'information et de la communication (NTIC). Celles-ci tendent à prendre une place croissante dans la vie humaine et le fonctionnement des sociétés ; Elles regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, des télécommunications et de l'internet.

Il est à noter qu'Internet reste un outil privilégié de transmission de l'information, de communication et d'échange entre individus. Il a dépassé le simple phénomène de *mode*[23] pour devenir un standard dans la communication vitale au niveau international. C'est grâce à Internet qu'il est désormais possible -et juste par un simple clic- de conclure une transaction à des milliers de kilomètres de distance de son interlocuteur[24] ; d'envoyer et de recevoir plus rapidement possible des courriers électroniques[25] ;de rechercher et retrouver des détails sur une information à l'aide d'un *moteur de recherche*[26] et ce, grâce à toile *w w w* [27] qui dispose de *milliards* [28] de pages

[22] Le terme *mondialisation* désigne simplement ici le développement de liens d'interdépendance entre hommes, activités humaines et systèmes politiques à l'échelle du monde. Ce phénomène touche la plupart des domaines aves des effets et une temporalité propre à chacun (…).ce terme est souvent utilisé aujourd'hui pour désigner la mondialisation économique, et les changements induits par la diffusion mondiale des informations sous forme numérique sur Internet. [Source : http://www.techno-science.net/ ?onglet=glossaire&definition=5465 (page consultée le 26 juillet 2010)]

[23] Bien évidemment, comme toute innovation, Internet était considéré à ses débuts comme faisant partie d'une manière de vivre réservée à une catégorie de personnes nanties, eu égard notamment à son coût (prix) d'utilisation très élevé. A ces jours, il est possible à tous individus, peu importe les rangs sociaux, d'utiliser cet outil informatique à un coût raisonnable.

[24] Notamment grâce au e-commerce (abréviation de « electronic commerce ou commerce électronique), c'est-à-dire le « commerce électronique », le « commerce en ligne », ou encore la « boutique en ligne » qui désigne l'achat et la vente en ligne sur les réseaux informatiques dont Internet. Le moyen le plus usité est celui de la monétique.
[Source : http://www.radisnoir.com/mini-lexique/site-e-commerce (consulté le 26 Juillet 2010)]

[25] Notamment avec la méthode de communication par « tchat »ou « chat » (anglais) sur des sites de rencontre (Hi5, Facebook, Netlog, etc.) et de messagerie (Yahoo, Gmail, Hotmail, etc.).

[26] Un moteur de recherche est une application permettant de retrouver des ressources (pages web, images, vidéo, etc.) associés à des mots quelconques. Certains sites web offrent un moteur de recherche comme principale fonctionnalité ; on appelle alors moteur de recherche le site lui-même (exemple : le sigle Google est un moteur de recherche (outil de recherche), mais aussi un site de messagerie(Gmail). [Source : http://fr.wikipedia.org/wiki/moteur-de-recherche; http://www.fknet.fe/definition_moteur-de-recherche.htm (consultés le 21 juillet 2010)]

[27] Le world wide web (ou w w w ou w3, souvent appelé web) signifie littéralement la "toile d'araignée recouvrant le monde ». Cette image représente tous les ordinateurs interconnectés à travers le monde, mais le world wide web désigne plus précisément le système hypertexte que supporte le réseau Internet. Les liens hypertextes sont comme les fils d'une toile d'araignées qui relient les pays d'un site à l'autre.[voir Louis MPALA Mbabula, **Pour vous chercheur, Directives pour rédiger un travail scientifique, suivi de recherche scientifique sur Internet**, 5ème édition augmentée, Lubumbashi, p.90-91, disponible sur www.louis-mpala.com]

[28] Le nombre est estimé à 3 milliards de pages contenant textes, images, sons, etc, reliés entre elles par des liens hypertextes, c'est-à-dire qu'une page peut contenir l'adresse d'une autre page à laquelle on peut accéder d'un simple clic de souris. [Source :

disponibles; de charger un *fichier* [29] depuis un *serveur* [30] ou d'y déposer un autre grâce au protocole *FTP* [31]; etc[32].

Bref, de manière incontestable, la vulgarisation d'Internet de par le monde a provoqué des bouleversements majeurs, tant au niveau de la communication à l'échelle mondiale qu'au niveau du droit applicable. Et à ce propos, c'est un truisme de constater depuis tout un temps une transfiguration par l'internet de la science et de l'art juridiques, avec notamment l'existence de nombreuses lois spécifiques au secteur informatique. L'on est donc passé d'un *vide juridique*[33] au Droit de l'Internet; d'où l'évocation des nouveaux concepts, tel que celui de *Cyberdroit*[34] ; etc.

Néanmoins, le développement d'Internet dans la société moderne a aussi apporté l'émergence des nouvelles formes de criminalités. En effet, grâce à Internet ; il s'est développé une certaine capacité de commettre des *délits*[35] tout en étant caché derrière un écran et à distance ; *ce qui permet l'ubiquité du délinquant dans le temps et dans l'espace*[36]. C'est cette délinquance *électronique*[37] qui porte le nom de **Cybercriminalité.** *Celle-ci a débuté en même temps que*

---

http://ite.tunisie.overblog.com/article-26085722.html; http://fr.wikipedia.org/wiki/technologie-delinfo-et-de-la-com. (Consultés le 11 juillet 2010)]

[29] En informatique, un fichier est un lot d'informations portant un nom et conservé dans une mémoire. En d'autres termes, c'est un ensemble d'informations stockées sur différents supports et dont la méthode de stockage implique un format. [Source : http://www.linux-france.org/prj/jargon/F/fichier.html; Dictionnaire informatique, définition de fichier, disponible sur http://dictionnaire.phpmyvisites.net (consultés le 12 Juillet 2010)]

[30] Un serveur est un logiciel ou ordinateur destiné à l'administration d'un réseau informatique. Il gère l'accès aux ressources et aux périphériques et les connexions d'autres ordinateurs appelés clients ou utilisateurs. [Voir la définition de serveur sur les sites ci-après : www.dicofr.com; www.futura-sciences.com; fr.wikipedia.org (consultés le 12 juillet 2007)

[31] Le **File Transfer Protocol** (protocole de transfert de fichier) ou FTP en sigle, est un protocole de communication destiné à l'échange informatique de fichier sur un réseau Internet. Il permet depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. [Voir la définition de File Transfer Protocol sur http://www.futura-sciences.com (consulté le 12 Juillet 2007)].

[32] Internet offre encore une gamme variée des services modernes, notamment SKYPE qui permet de communiquer entre individus à des bonnes conditions.

[33] Selon CAHEN, on entend encore trop souvent dire qu'Internet est un vide juridique. Mais l'application par exemple des règles du droit d'auteur sur le réseau Internet illustre parfaitement la situation réelle [Voir Murielle-Isabelle CAHEN, **Internet et le droit d'auteur**, Dossier SAM « question juridique », Novembre 2000, disponible sur le site web www.Avocat-online.com (consulté le 20 juillet 2010].

[34] Le concept de Cyberdroit désignerait l'application des règles du Droit dans un espace virtuel, en l'occurrence Internet. Il s'est beaucoup développé avec la notion de la protection de droits d'auteur sur Internet.

[35] En Droit français, un délit est une infraction jugée par le tribunal correctionnel. Il se situe entre la contravention et le crime. Il est passible d'une peine d'emprisonnement qui ne peut dépasser 10 ans (lire à ce sujet Jean-Claude SOYER, **Droit pénal et procédure pénale**, 10ème édition, LGDJ, 1993, p.19-22). Le Droit pénal congolais ne fait aucune distinction entre une contravention, un délit et un crime.

[36] Nacer LALAM, **La délinquance électronique**, Dossier problèmes politiques sociaux, Documentation française, N° 953, Octobre 2008, p.15

[37] A lire « délinquance sur le réseau ».

l'expansion d'Internet[38]. Le développement de la société de l'information s'est donc accompagné mécaniquement d'une augmentation des actes de délinquance dans le *Cyberespace*[39]. Grâce à la fluidité de la circulation de l'information permise par Internet, *des acteurs aux motivations et aux intérêts multiples commettent sur des réseaux informatiques des actes délictueux très dangereux*[40].

Il est à noter que le concept de cybercriminalité demeure difficile à conceptualiser, car *il n'est l'objet d'aucune définition légale. Ce choix des législateurs a conduit la doctrine à multiplier les définitions de ce terme, contribuant ainsi à rendre plus complexes les analyses Juridiques*[41].

Essayons tout de même à cerner cette notion par une appréhension étymologique. En effet, le concept de cybercriminalité renvoi à deux termes : « Cyberespace » et « Criminalité ».
Le terme *Cyberespace*[42] ou *Cybermonde*[43] désigne *un lieu imaginaire appliqué métaphoriquement aux réseaux internet et dans lequel les internautes qui y naviguent (surfent) s'adonnent à des activités diverses*[44]. C'est donc *l'environnement virtuel dans lequel se déroule la transmission des*

[38] Voir « Délits de la cybercriminalité », un article de Jurispedia, in http://fr.jurispedia.org/index.php/D%C3%Adelits-de-la-cybercriminalite%C3%A9_(fr) (consulté le 11 Juillet 2010)

[39] Pour des plus amples détails sur le sens et la portée du concept de *cyberespace*, voir infra (Note 42) au sujet de l'étymologie du concept de *cybercriminalité*.

[40] Nacer LALAM, **op.cit**., p.4

[41] M.CHAWKI, **Op.cit**., p.6

[42] Le concept de cyberespace est emprunté à un roman de science-fiction de william GIBSON (romancier américain né à Caroline du sud le 17 Mars 1948) 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.
Le préfixe « cyber » serait emprunté au terme « cybernétique » créé à partir du grec *Kubernésis* ou *kubernân* qui signifie « l'action de diriger ou de gouverner ». Le terme serait utilisé pour la premier fois en 1948 par l'un des ses pères fondateurs, N.WIENNER, dans son ouvrage « *Cybernetic or control and communication in the machine* »(Cybernétique ou contrôle et communication dans une machine) qui voulait signifier, par cyber, la science nouvelle destinée à couvrir tous les phénomènes mettant en jeu des mécanismes de traitement de l'information…
GIBSON est considéré comme étant le parrain du lexique foisonnant des *cybermots* dont, notamment *cybercriminalité*, *cyberespionnage, cyberterrorisme, cyberpolicier, cybervigilance, cybercafé, cyberespace*..., pour désigner un fait, un acte ou une activité réelle qui se transposerait dans l'espace virtuel du Net. [Lire à ce sujet : M. CHAWKI, **Op.cit**., p.10 ; Stéphane LEMAN-LANGLOIS, **Criminologie**, vol. 39, N°1, 2006, p.65, disponible sur www.erudit.org (consulté le 18 Juillet 2010)]

[43] Cybermonde est synonyme de cyberespace. (Voir la définition de cybermonde dans le dictionnaire LAROUSSE PRATIQUE, édition LAROUSSE, 2005, disponible sur www.larousse.fr)

[44] Au sujet du sens du concept de *cyberespace*, les lecteurs pourront utilement consulter la documentation suivante : M.CHAWKI, **Op.cit**., p.10-14 ; CICA MATHILDA DADJO, **Les contrats dans le cyberespace à l'épreuve de la théorie générale :problèmes et perspectives**, Maîtrise en Droit des affaires et carrières judiciaires, Université d'Abomey CALAVI-Benin, in www.memoireonline.com (consulté le 21 Juillet 2010) ; B.BENHAMOU, **Petit essai de prospectives pour le cyberespace**, Mars 2001, disponible sur http://www.homo-numericus.net/IMG/articlePDF/article60.P.df. (Consulté le 21 Juillet 2010) ; Définition du cyberespace sur http://www.futura-sciences.com/fr/definition/t/hight-tech-1/d/cyberespace_3964/. (consulté le 21 Juillet 2010) ; Le jargon français : le cyberespace, in http://www.linux-france.org/prj/jargonnf/C/Cyberespace.htm/. (Consulté le 21 Juillet 2010).)

informations via internet, qui est considéré comme un moyen de communication[45]. La question qui se pose est elle de savoir alors si *le Cyberespace n'est qu'un simple moyen de communication comme le téléphone par exemple ou s'il représente une réalité rien plus complexe ?*[46].

De toute manière, le cyberespace est *un lieu dépourvu de murs au sens concret du terme, voire de dimensions physiques*[47]. STERN et TAXIL ont pu écrire que *la vie sur internet ressemble à la vie urbaine, avec ses accès (portails), sa circulation gratuite sur ses trottoirs et sur les autoroutes de l'information, ses cafés (Forums de discussion), ses boutiques (e-commerce), et ses lieux de loisir (sites musicaux, musées virtuelles)(…)*[48].

Le second concept mis en relief par le vocable de Cybercriminalité est celui de « Criminalité ». Il n'est point utile de souligner ici les sempiternelles difficultés que la *criminologie*[49] a pu avoir avec cette notion ; nous nous limitons, dans le cadre de la présente étude, à une acception Juridique de ce phénomène. Nous ne nous intéressons point aux causes de la cybercriminalité, mais nous essayons de la définir et d'en tirer les conséquences Juridiques. Ainsi donc, nous considérons le « *crime* »[50] comme simplement synonyme de « délit » ou *« d'infraction »*[51]. De ce point de vue, la criminalité dévient synonyme de la *délinquance*[52]. D'ailleurs, il importe de mentionner ici que la plupart de rapports, guides et publications sur la cybercriminalité, commencent d'abord par une définition du terme « Cyberdélit ». Selon une acception courante, un Cyberdélit désigne *toue*

[45] Voir GUILLEMARD S., **Le Droit international privé face au contrat de vente cyberspatial**, thèse de Doctorat, Faculté des études supérieures, Université LAVAL-Québec, Janvier 2003.

[46] CICA MATHILDA DADJO, **Op.cit**., in idem.

[47] CHAWKI, Op.cit., p.11

[48] STERN B. et TAXIL B., **Internet comme système social**, International Law, Forum du Droit international, cité par Cica MATHILDA, **Op.cit**., in idem.

[49] La Criminologie peut être définie plus simplement comme étant *l'étude scientifique de l'ensemble du phénomène criminel*. Au sujet de la notion de Criminologie, les lecteurs peuvent utilement consulter les auteurs ci-après : Emile DURKHEIM, **Les règles de la méthode sociologique**(1895), P.U.F., Quadrige, 1981, p.35 ; Enrico FERRI, **La sociologie criminelle** (1882), Ed. Alcam, 1905, p.2 ; Maxime LAIGNEL LAVASTINE et Vasil STANGU, **Précis de Criminologie**, Lib. Payot, 1950, p.4 ; Jacques LEAUTE, **Criminologie et science pénitentiaire** (1972), P.U.F., Collection Thémis, p.11 ; Gaston STEFANI, Georges LEVASSEUR et R. JAMBU-MERLIN, **Criminologie et science pénitentiaire**, 5ème édition, 1982, p.2 ; Raymond GASSIN, **Criminologie**, Dalloz, 6ème édition, 2007, p.33 ; etc.

[50] Un crime est une infraction punissable d'une peine infamante (grave). Voir Jean-Claude SOYER, **Op.cit.**, idem.

[51] L'infraction peut être définie comme étant *« la commission ou l'omission d'un fait prévu et puni par la loi, imputable à son auteur ne se justifiant pas par l'exercice d'un droit quelconque ». (*Voir T. NGOY, **Le droit de la preuve dans l'avant-procès en procédure pénale congolaise**, DES en Droit, UNIKIN, 2006, p.8). Rubens note que « ce qui caractérise l'infraction, c'est qu'elle est une violation du Droit, de la règle de conduite imposée par la communauté, sanctionnée par une peine.»(Voir A. RUBBENS, **Le droit judiciaire congolais : l'instruction criminelle et la procédure pénale**, Université Luvanium et Maison Larcier, Léopoldville-Bruxelles, 1965, p.5)

[52] Le mot « délinquance » renvoie étymologiquement au mot latin « delinquere » qui signifie commettre une faute. En Droit pénal, le délinquant est défini comme étant l'auteur d'une infraction, qui peut faire l'objet d'une poursuite de ce chef. Le cyberdélinquant est donc l'auteur d'une infraction commise contre ou via le réseau Internet.

activité mettant en jeu des ordinateurs ou des réseaux en tant qu'outils, cible, ou lieu d'une infraction[53].

De l'intelligence sémantique des concepts *Cyberespace* est *criminalité* tels que sus définis, il ressort que la cybercriminalité est *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général et plus particulièrement sur le réseau internet*[54].

Selon les Nations-Unies, 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*.[55]

MUKADI MUSUYI explique extensivement le vocable de cybercriminalité comme impliquant *toutes les informations commises par l'utilisation frauduleuse ou illicite des réseaux informatiques telles que les atteintes aux systèmes d'informations ou aux données informatisées, l'envoi des courriers commerciaux non sollicités (spam), la violation de la vie privée et des données personnelles, la fraude à la carte bancaire, la propagation des virus informatiques, les actes racistes ou néonazis, le blanchiment d'argent, des escroqueries de tout genre, l'organisation de réseaux terroristes, de maffieux, de xénophobes, etc.*[56]

SYMANTEC[57] s'inspire de nombreuses définitions sur la cybercriminalité et donne la définition concise suivante : *Tout acte criminel perpétré à l'aide d'un ordinateur sur un réseau, ou à l'aide de matériel informatique*[58]. Et donc, selon SHINDER, la cybercriminalité requiert obligatoirement *l'intervention directe ou indirecte d'un réseau de télécommunication pour commettre l'infraction*[59].

---

53 Lire le dossier « Comprendre la cybercriminalité : Guide pour les pays en développement », Union internationale des télécommunications, Avril 2009, disponible en ligne au www.itu.int/ITU-D/cybersecurity/legislation.html (consulté le 10 Juillet 2010)

54 Lire à ce sujet les définitions émises, à titre illustratif, par les auteurs suivants : Nacer LALAM, **Op.cit.,** p.4 ; CHAWKI, **Op.cit**., p.23.

55 ONU : **Manuel pour la prévention et la répression de la criminalité informatique**, Revue internationale de politique pénale, N° 43 et 44, 1995. (Publication des Nations Unies, Numéro de vente : F.94.IV.5)

56 MUKADI MUSUYI (Emmanuel), **Op.cit.,** in idem

57 *SYMANTEC CORPORATION* est une société américaine fondée en 1982, spécialisée dans la conception des logiciels informatiques utilitaires (notamment liés à la sécurité et à la protection des données) pour PC tournant sur plateforme Microsoft.

58 Voir l'article « Qu'est-ce que la cybercriminalité ? », in http://www.symantec.com/fr/fr/norton/cybercrime/definition.jsp (consulté le 21 juillet 2010).

59 SHINDER, cité par CHAWKI, **Op.cit**., p.23

Toute chose étant égale par ailleurs, le concept de cybercriminalité est usité de façon interchangeable avec ceux de « Netcrime »[60], de « cyberdélinquance », de « délinquance électronique », de « délinquance informatique » et j'en passe, pour désigner *toute activité criminelle malveillante sous une forme ou une autre, qui utilise Internet et/ou des applications informatiques ou qui les attaques*[61].

Tout bien considéré, pour définir la délinquance électronique, le critère de la légalité constitue l'élément le moins contestable ; cependant, l'extension et la diversité de pratiques déviantes sur et via Internet nécessiteraient une mise à jour constante des dispositions pénales. Nous y reviendrons ultérieurement au point III de cette étude.

Somme toute, il est à constater qu'un nombre non négligeable de pays n'ont encore aucune législation spécifique de répression de la délinquance électronique ; et dans cette vase, nous pouvons citer la République Démocratique du Congo qui manifeste une certaine indolence dans l'abord de la question et, par ricochet, accuse un décalage de notre *système répressif* [62] par rapport à la percée exponentielle des nouvelles technologies de l'information et de la communication. Sous d'*autres cieux*[63], par contre, des avancées remarquables sont à répertorier avec déjà l'apparition d'une vague de néologismes, notamment celui du Droit des nouvelles technologies de l'information et de la communication, etc.

[60] Netcrime est un terme anglais dont l'équivalent en français est « crime sur Internet ».

[61] Shendam MORRIS, The futur of Netcrime now, Part 2 : Responses, Ministère de l'intérieur, Royaume-Uni, Rapport en ligne du Home 63/04, 2004, cité par Nacer LALAM, **Op.cit.,** p.42

[62] En effet, il transpire de nos investigations que jusqu'ici, la législation pénale congolaise relative aux nouvelles technologies de l'information et de la communication est composée seulement : une loi, en l'occurrence la loi-cadre n°13/2003 du 06 octobre 2002 sur les télécommunications ; d'une ordonnance, l'Ordonnance n°87/243 du 22 juillet 1987 portant réglementation de l'activité informatique au Zaïre ; et d'un arrêté, l'Arrêté ministérielle n°22/CAB/Min/PTT/98 du 16 juin 1998 portant interdiction de pratique « call back ».
Cette législation n'édicte que neuf infractions, et nous paraît donc rudimentaire, compte tenu de la spectaculaire progression de la cybercriminalité. A quoi donc est concentrée l'action du pouvoir législatif ?
Par ailleurs, des initiatives privées restent à signaler dans le souci tant soit peu d'éveiller les congolais sur les dangers liés aux NTIC. Ceci mérite bien nos éloges ! A titre illustratif, nous pouvons citer les Ateliers de la Société civile congolaise sur la gouvernance d'Internet en République Démocratique du Congo, tenus du 9 au 11 Janvier 2007 à Kinshasa (Résumé disponible sur www.societecivile.cd/mode/3214 : consulté le 20 juillet 2010) ; et même, antérieurement, un certain « Observatoire Congolais de la Cybercriminalité » aurait été mis sur pied par monsieur MUKADI MUSUYI, lors de la journée mondiale de la société de l'information organisée par le Ministère des Poste et Télécommunications de notre pays le 25 Mai 2001 autours du thème central « Connecter les jeunes :possibilités offertes par les TIC » (voir à ce sujet les détails sur www.lepotentiel.net); Au reste, dans le domaine scientifique, la faculté de Droit de l'Université protestante du Congo, aurait organisé une journée de réflexion sous le thème « le Droit congolais à l'épreuve des NTIC », en date du vendredi 29 Avril 2005 sous la modération d'une journaliste de la chaine de radio-télé TROPICANA…

[63] Notamment, la France possède un arsenal juridique suffisamment aiguisé contre la cybercriminalité. Nous pouvons citer entre autre la Loi du 15 Novembre 2001 relative à la sécurité quotidienne ; la Loi du 21 Juin 2004 pour la confiance dans l'économie numérique ; la Loi du 23 Janvier 2006 relative à la lutte contre le terrorisme, etc.

II. CYBERCRIMINALITE : UNE DELINQUANCE POLYMORPHE

Au point précédent, nous avons appréhendé la cybercriminalité comme étant une constellation d'actes illicites commis via et contre des réseaux de télécommunication, particulièrement et surtout sur le réseau Internet ; l'absence de cette interconnexion empêchant donc la perpétration desdits actes.

La difficulté de la conceptualisation de la cybercriminalité est liée non seulement au manque de définition légale de cette notion, mais aussi à la manière dont celle-ci se présente sur le plan pratique. Le champs de cette délinquance électronique se laisse difficilement appréhendé ; il est vaste et hétérogène parce qu'il englobe un grand nombre et une grande variété d'activités de par le monde. De même, les pratiques et les objectifs des acteurs impliqués varient grandement. En outre, *une même pratique peut avoir divers objectifs et, inversement, un même objectif peut être réalisé à l'aide de pratiques différentes*[64].

La cybercriminalité, cette délinquance électronique, recouvre deux grandes catégories d'infractions[65] : D'une part, des infractions spécifiques aux NTIC et, d'autre part, des infractions dont la commission est liée ou facilitée par l'utilisation de ces NTIC.

Cette typologie apparemment claire, *occulte pourtant en réalité le flou sémantique dans lequel la cybercriminalité de NTIC nage à son tour et qui se caractérise par une confusion, curieusement pittoresque, mais certainement très dangereuse entre les techniques de perpétration du crime et le crime lui-même.*[66]

Avant de procéder à une analyse panoramique de la typologie sus énoncée des infractions relevant de la cybercriminalité, il nous parait très cohérent d'éclairer d'abord nos lecteurs sur la nature de l'artisan de cette forme de délinquance qui est, au fait, le *cyberdélinquant*[67]. En effet, les motivations de ceux qui mettent en œuvre la délinquance électronique sont diverses[68] : Quête du risque, défi, appât du gain, espionnage industriel ou politique, etc.

---

[64] Nacer LALAM , **Op.cit.,** p.5

[65] Idem, p.4

[66] MANASI NKUSU, **Le Droit congolais et la criminalité de NTIC**, mémoire de DEA en Droit, UNIKIN-RDC, Texte de présentation du mémoire disponible sur http://ccn.viabloga.com/news/memoire-de-dea-en-cybercriminalite-unikin-rdc (consulté le 20 Juillet 2010).

[67] Cfr supra (note 52). Nous l'appelons cyberdélinquant ou cybercriminel.

[68] Nacer LALAM, **Op.cit**, p.5

Ce délinquant en informatique, généralement qualifié de respectueux par sont statut social et par son niveau culturel, ne bénéficie pas de l'image stéréotypée du délinquant classique,. La délinquance informatique étant peu violente, *elle n'épouvante pas les victimes*[69]. Rose distingue à cet effet[70] : (a)l'utilisateur qui recherche le profit d'un capital financier ; (b) les destructeurs qui composent une frustration professionnelle ou personnelle et qui ne commettent que dans le but de nuire aux Entreprises ou aux organisations ; et (c) l'entrepreneur qui vise l'activité ludique et le défi des agressifs qui compensent une frustration personnelle ou professionnelle.
Quant à M. BOLONGA, il isole quatre types de délinquants[71] : (a) l'utilisateur qui recherche le gain financier ; (b) l'utilisateur qui recherche une reconnaissance sociale ; (c) l'utilisateur qui recherche la perte du sens des réalités ; et enfin (d) l'utilisateur ayant un comportement idéologique, qui veut se venger de la société.

D'une manière générale, on catégorise, au cœur de la cyberdélinquance, trois groupes d'acteurs majeurs, à savoir : les *Hackers*, les *Crackers* et les *Script-kiddies*.[72]

Le *Hacker*[73] est le *spécimen d'un individu qui, par jeu, curiosité, défi personnel, souci de notoriété, ou envie de nuire, cherche à pénétrer un système informatique auquel il n'a pas légitimement accès. Les motivations financières sont très loin de ses intentions*[74]. En d'autres termes, le Hacker, *pirate d'Internet, utilise les technologies de communication pour s'introduire dans des systèmes protégés dans un but malveillant. L'objectif primaire est la notoriété, mais certains ont des desseins de destruction ou de récupération de données confidentielles*[75].

Le *Cracker*[76], souvent confondu avec le Hacker, pénètre les systèmes informatiques avec l'intention de nuire. Il se différencie du Hacker par le fait que celui-là attaque les systèmes informatiques pour essayer de tirer un gain de ses méfaits ; il poursuit un enrichissement personnel ou l'acquisition de données confidentielles. Bien souvent, *il s'agit de véritables criminels,*

---

[69] CHAWKI, **Op.cit.,** p.16

[70] ROSE P., **Menaces sur les autoroutes de l'information**, Paris, Harmattan, 1996, p.15

[71] BOLONGA, cité par MARTIN D., **La criminalité informatique**, Paris, PUF, 1997, p.68

[72] Pour des plus amples précisions sur ces trois catégories de cyberdélinquants, les lecteurs peuvent se référer au dossier « Cyberdélinquants », Fiche thématique 032 F, disponible sur le site www.caseo.lu

[73] Mot anglais synonyme de pirate en français

[74] Nacer LALAM , **Op.cit**., p.116

[75] Voir la définition du *Hacker* dans le dictionnaire informatique, disponible sur http://dictionnaire.phpmyvisites.net/definition-hacker-4572.htm (consulté le 21 juillet 2010).

[76] Pirate en français

fonctionnant dans des réseaux maffieux, pour leur propre compte ou le compte d'autrui. Ils sont spécialisés dans le cassage des codes, des mots de passe ou de protection de logiciels[77].

Enfin, le *Script-kiddy*[78], quant à lui, forme le bas-de-gamme du piratage informatique. Si les Hacker et Cracker se focalisent sur des cibles spécifiques, le script-kiddy lui, *lance ses attaques de manière totalement aléatoire en utilisant des listes de commande groupées dans un script ; d'où le nom qu'il porte*[79]. Ce type d'attaque ne demande pas un très haut niveau de connaissance informatique ; c'est pourquoi le script-kiddy est souvent un adolescent, voire parfois un *enfant*[80].

A présent, tournons notre regard vers les deux catégories d'infractions désignées sous le vocable de cybercriminalité : dans un premier point, nous aborderons les infractions ontologiques aux NTIC (II.1.), et dans le second volet, nous nous pencherons sur les infractions dont la commission est seulement facilitée par les NTIC (II.2.).

II.1. Les infractions directement liées aux NTIC

Dans cette sphère, la cybercriminalité recouvre un éventail d'inconduites dont l'existence est entièrement dépendante de celle des réseaux. C'est *le cas dans lequel les NTIC, dans leur essence ontologique, sont l'objet même desdites inconduites*[81].

Cette typologie vise *toutes atteintes à la sécurité des systèmes et réseaux informatiques ou des données informatiques*[82]. Concrètement, ce sont des atteintes à la confidentialité, à l'intégrité, à l'authenticité et à l'intégrité des systèmes et données informatiques. Plusieurs inconduites peuvent être relevées dans la catégorie sous analyse ; à titre d'échantillon, nous en énumérons 9 seulement[83] :

1) L'accès illégal aux données et systèmes d'information ;
2) L'interception illégale des données ;
3) L'atteinte à l'intégrité des données ;

---

[77] Lire la définition du Cracker informatique disponible sur http://fr.wikipedia.org/wiki/cracker-informatique (consulté le 21 juillet 2010)

[78] Littéralement en français « scénario de gosse ».

[79] Voir la définition du Script-kiddy sur http://www.bimarysec.fr/cms/docs/ressources/glossaire/p-5.html (consulté le 21 juillet 2010).

[80]Nous employons le terme « enfant » ou « adolescent » ici, pour signifier le niveau informatique moins élevé de ce type de pirate informatique. Nous estimons donc qu'en pratique, dans le pays en retard par rapport à l'évolution de la technologie, un Script-kiddy peut valablement être un adulte, ou mieux un considéré « expert » par son entourage selon, évidemment, l'adage « dans le royaume des aveugles, un borgne est roi » !

[81] MANASI NKUSU, **Op.cit**., in idem
[82] Jurispedia, **Art.cit**., in idem.
[83] MANASI, NKUSU, **Op.cit**., in idem.

4) L'atteinte à l'intégrité des systèmes ;
5) L'abus de dispositif ;
6) La falsification informatique ;
7) La fraude informatique ;
8) La fraude en matière de télécommunication ;
9) L'obstruction non intentionnelle aux correspondances par télécommunication.

Toutes ces cyberinfractions se perpètrent par le truchement de différentes techniques que nous verrons ultérieurement au point II.3.

II.2. Infractions dont la commission est facilitée par les NTIC

Dans cette catégorie, la cybercriminalité désigne *des cas où l'informatique n'est qu'un moyen de commission des certaines infractions classiques*[84]. Ici, la délinquance est en relation indirecte avec un réseau de télécommunication, c'est-à-dire que ce dernier se comprend comme *un outil ou un moyen pour commettre l'infraction*[85]. LEMAN note que *ce sont en fait des crimes relativement conventionnels dont les auteurs ont adopté des outils modernes pour arriver à leurs fins. On peut s'approprier une infinité de biens physiques, de valeurs symboliques et d'informations confidentielles dans le monde tangibles, et l'idée de le faire avec une technologie procurant de nouveaux outils et de nouvelles cibles n'est particulièrement difficile à formuler, ni à mettre en pratique*[86].

Plusieurs[87] infractions relèvent de cette catégorie de la cybercriminalité ; mais nous pouvons en citer quelques uns seulement :

1. la pornographie enfantine et la pédophilie ;
2. les atteintes à la législation relative à la propriété intellectuelle et aux droits connexes ;
3. la xénophobie et le racisme ;
4. les escroqueries de tous bords ;
5. le terrorisme et le blanchiment des capitaux ;
6. la contrefaçon ;
7. la fraude fiscale ;
8. le harcèlement et le chantage ;
9. etc.

[84] Jurispedia, **Art.cit**., in idem.
[85] BENSOUSSAN A., **Les télécommunications et le Droit**, Paris, Hermès, 1996, p.484 et s.
[86] Stéphane LEMAN-LANGLOIS, **Op.cit.,** p.65
[87] MANASI en énumère 23 au total. Voir MANASI NKUSU, **Op.cit**., in idem

Dans les lignes qui suivent, nous verrons quelques-unes des méthodes usuellement employées par les cyberdélinquants pour arriver à perpétrer les forfaits sus-énumérés. C'est l'objet du point suivant.

II.3. Les techniques de la cybercriminalité

Par techniques de la cybercriminalité, nous entendons les différentes manières d'action fréquemment employées par les cyberdélinquants pour arriver à leurs fins.

Il existe toute une panoplie de techniques dans la cybercriminalité ; lesquelles peuvent être subdivisées en trois typologies[88] : *les infections informatiques, les attaques cybernétiques et les arnaques.*

Dans les lignes qui suivent, nous nous évertuerons à donner à nos lecteurs une vue panoramique de toutes ces techniques, sur base de données systématiques et *expérimentales*[89]. Mais, avant l'entame de cela, nous les (lecteurs) invitons préalablement à prendre connaissance de ce décor en rapport avec la délinquance sous analyse ; décor peint par MUKADI MUSUYI que nous avons cité précédemment :

> *« (…) l'on assiste ici à des saturations intempestives des bandes passantes de nos fournisseurs d'accès à Internet sans que les gens ne se posent des questions sur le comment et le pourquoi de ce phénomène. Or, il s'avère que des particuliers et des personnes aguerris, autrement dit des cybercriminels, utilisent des routeurs pour se connecter gratuitement dans leurs domiciles à Internet, en usurpant les paramètres de connexion des serveurs des cybercafés qui sont géographiquement proches de leur maison. La démarche de ces pirates est assez simple. Ils se présentent dans un cybercafé qui est proche de leur domicile, et s'attellent à récupérer l'adresse IP, le masque de sous-réseaux, les passerelles, ainsi que les adresses DNS présentes sur le serveur Internet dudit cybercafé.*
>
> *Les cybercafés fonctionnant suivant une architecture de type client serveur et dont les serveurs sont dotés de Windows XP sont vulnérables en terme de sécurité dans les partages des ressources avec les machines clientes. Grâce aux failles de ces versions de XP, les pirates peuvent ainsi, via un PC client, se connecter au serveur. Mais étant donné que les réseaux LAN ne tolèrent généralement que les partages de fichiers ou d'imprimantes, ils prennent soin d'installer un petit Trojan (entendez cheval de Troie) qui leur permettra de récupérer toutes ces informations sans faire mouche. Une fois toutes ces données récupérées, il ne reste plus qu'à programmer le routeur chez soi. Le serveur du cybercafé procède au partage de la connexion en*

[88] MANASI NKUSU, **Op.cit**., in idem

[89] Nous nous inspirerons largement de notre expérience. Nous mettrons à la disposition de nos lecteurs quelques mails (spam) personnels pour essayer d'étayer les explications théoriques des quelques techniques.

croyant avoir à faire à une nouvelle machine qui vient de s'ajouter au réseau local du cyber. Or en réalité, il s'agit d'une machine distante qui se trouve à un endroit très éloigné.

Bien évidement, la conséquence sur ce genre de piratage est très perceptible : ralentissement notable de la connexion dû à un engorgement de la bande passante qui, en réalité, est partagé entre le cybercafé et le pirate (impossible de détecter une pareille anomalie sans procéder à un monitoring du trafic réseau), chose rare dans le cybercafé et même chez la plupart de nos fournisseurs d'accès »[90]

II.3.1. Les infections informatiques

Un expert en sécurité informatique, Eric FILIOL, définit une infection informatique comme *un programme simple ou auto-reproducteur, 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, 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*[91].

A ces jours, les infections informatiques ont un but lucratif. En effet, beaucoup de pirates informatiques contrôlent des milliers d'ordinateurs grâce aux *virus* et *malwares*[92] installés sur les ordinateurs de victimes. Un pirate, responsable d'un *botnet*[93], gagnerait de l'argent par l'acheteur qui peut être par exemple une Entreprise *pharmaceutique*[94] illégale d'articles de contrefaçon de grandes marques. Certaines infections sont destinées *à dérober des numéros de cartes bancaires afin d'être revendus et utilisés par des groupes maffieux*[95].

De la définition de FiLIOL sus énoncée, il transpire que les infections informatiques sont de deux ordres : les infections simples (A) et les infections autoreproductrices (B).

[90] MUKADI MUSUYI (Emmanuel), **Art.cit**, in idem.
[91] FILIOL (Eric), **Les virus informatiques : théorie, pratique et applications**, Ed. Springer, 2004, p.79 et s.
[92] Virus et malware sont des infections informatiques.

[93] Un botnet est un groupement d'ordinateurs zombies ; tandis qu'un zombie c'est un ordinateur infecté par des virus informatiques, contrôlable à distance via Internet. (http://www.sixi.be/glossary : consulté le 20 juillet 2010)

[94] L'adjectif « pharmaceutique » employé en informatique ferrait référence au pouvoir thérapeutique qu'ont certains logiciels informatiques dans la protection des ordinateurs contre des infections informatiques.

[95] Lire « le but des infections informatiques », sur http:// www.pegase-secure.com/les-virus.html (consulté le 18 Juillet 2010)

A. LES INFECTIONS SIMPLES[96]

Un programme simple contient une fonctionnalité malveillante cachée qui est appelée à se déclencher à un instant donné, sur un critère donné. Il n ya 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 n'est généralement pas résident en mémoire. Dans cette catégorie, on distingue[97] : les bombes logiques, les chevaux de Troie, les bombes ANSI, les logiciels espions (spyware), les canulars informatiques et les accès dissimulés.

B. LES INFECTIONS AUTO-REPRODUCTRICES[98]

La finalité d'un programme auto-reproducteur est identique à celle d'un programme simple. Il s'agit de perturber ou de détruire. A sa première exécution, le programme cherche à se reproduire. Il sera donc généralement résidant en mémoire et, dans un premier temps, discret. Comme leur nom l'indique, leur finalité est de se dupliquer, afin de se diffuser, de se propager, via les vecteurs pour lesquels ils ont été programmés.

Parmi ces infections, nous pouvons citer[99] : les virus et les vers.

II.3.2. Les attaques cybernétiques[100]

Par attaque cybernétique, on entend l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système, et généralement préjudiciable. Les principales attaques cybernétiques sont de quatre ordres suivants :

A. Trois attaques cryptographiques :

- L'attaque des mots de passe ;
- L'attaque man in the middle ; et
- L'attaque par rejet.

[96] Voir le dossier « Typologie des infections informatiques » sur le site du club de la sécurité de l'information (CSIF) : www.clusif.asso.fr
[97] Fréderic DUFLOT, **Les infections informatiques bénéfiques**, DESS en Droit du numérique et des nouvelles techniques, Université Paris XI-Faculté de Droit, 2003-2004, p.16 et s.
[98] Dossier « Typologie des infections informatiques » sur le site du club de la sécurité de l'information (CSIF) : www.clusif.asso.fr
[99] Voir le dossier « Sécurité et aspects juridiques des TIC », **les infections : vers/Worms ; chevaux de Troie ; Spyware ;** etc., in http://www.awt.be/web/sec/index.aspx?fr. (Consulté le 10 Juillet 2010)
[100] MANASI NKUSU, **Op.cit**., in idem

B. Six attaques déni de service:

- le déni de service proprement dit ;
- la technique dite « par réflexion » ;
- l'attaque par fragmentation ;
- l'attaque du Ping de la mort ;
- l'attaque LAND ; et
- l'attaque SYN.

C. Huit attaques techniques qui sont :

- l'usurpation de l'adresse IP ;
- le vol de session TCP ;
- l'attaque du protocole ARP ;
- l'analyse réseau ou écoute réseau ;
- le balayage de ports ;
- l'attaque par débordement de tampon ;
- le spam, spim ou pollupostage ;
- le mail bombing, c'est-à-dire bombardement de mail

D. Quatre attaques web, à savoir :

- l'attaque par falsification des données ;
- l'attaque par manipulation d'URL ;
- l'attaque cross-site Scripting ou injection de code malicieux ; et
- l'attaque par injection de commandes SQL

II.3.3. Les arnaques

La troisième catégorie des méthodes usitées par les cyberdélinquants est constituée des arnaques. Celles-ci sont les techniques d'escroquerie, de tromperie. Nous pouvons en distinguer de quatre ordres[101] :

A. L'INGENIERIE SOCIALE

Cette méthode consiste couramment, de la part des acteurs, de s'intéresser particulièrement à leurs futures victimes par des baratins, leur faisant miroiter un avenir somptueux, une générosité sans contrepartie.

[101] Ibidem.

Nous soumettons à la lecture de nos lecteurs un exemple personnel d'un mail que nous avions reçu dans l'une de nos adresses de messagerie. D'emblée, je leur avertis que ce mail contient toute une panoplie de fautes ! Je me refuse de les corriger. Il en est de même des autres exemples que j'évoquerai ultérieurement:

« Bonjour,
Je suis très ravis et contente de vous écrire en ce jour. Me rassurant que vous ayez avec moi un coeur ouvert, je vous répondrai si vous acceptez ma demande de correspondance malgré la différence qui existe entre nous. Je me nomme Jessica lapointe suis âgée de 32ans de nationalite cannadienne mais residente à OTAWA et je suis déléguée médicale.
Je veux bien correspondre avec vous dans une idée claire et saine, et ne rien vous cacher. Je voyage beaucoup, et peux un jour me rendre dans ton pays. Voila pourquoi j'aimerais correspondance avec vous, pour connaître mieux mes semblables et surtout échanger de cultures. Dit-on l'Afrique est riche en culture. En effet c'est après une longue recherche de mail sur les sites de correspondance que je suis arrivée à t'identifier parmi tant de personnes Je serai auusi fiere de te voire ici au Canada, car actuellement je suis en attente d'une conférence (CNUCED) des Nations unies sur le commerce et le développement avec le probleme d'environement Qu'organise la fondation FCD en partenariat avec les autres organisations internationales, aux Canada. N'est tu pas interressé par cette cette conférence car ce sera une oportunitée pour moi de te voire en personne.Si oui alors tu me faire signe pour que je te donne l'adresse à laquelle tu dois ecrire pour avoir de plus amples renseignements et pour savoir les conditions a remplir pour prendre part à cette edition . Sache que je ferai tout ce qui est en mon pouvoir pour que tu prenne part à cette conference une fois que tu as dejà la volonté .Voici l'adresse de l'organisation à l'aquelle tu vas ecrire pour avoir de plus amples renseignement : fcdcanadasiege@rocketmail.com .
Je veux que tu prenne soin de le lire et remplir les formalités et les conditions pour etre conforme à leur lois .Alors n'oublie pas de me mettre au courrant des demarches à suivre .
Je ferai tout pour toi pour le visa mais il suffit que tu sois sèrieux. Laisse moi un message apres avoir contacté l'organisation. Merci de m'écrire et de me faire connaître

votre pays et aussi de m'ajouter à mon contact: jesilepine1@yahoo.fr .Bisou à toi ».

Cet exemple frise tant soit l'ingénierie sociale.

B. LE SCAM[102]

Cette technique a pour but d'abuser de la crédulité des gens en utilisant les messageries électroniques (courriers principalement) pour leur soutirer de l'argent.

Je propose à mes lecteurs un spam (mail indésirable) reçu personnellement, pour essayer d'illustrer cette arnaque :

« Bonjour cher Ami,

Je sais que cette lettre vous parviendra telle une surprise, pour le simple fait que nous ne nous sommes jamais rencontré. Soyez en rassuré car ce sont de bonnes intentions.

Je suis Mr. USMAN DIALLO . Directeur du département d'audit d'une BANQUE au Burkina Faso. Pendant mes recherches à la banque, vers la fin de l'année dernière 2008, j'ai trouvé un montant énorme de Douze millions cinq cent mille dollars Américains (US12.5M) qui a été déposé dans un compte depuis 1999.

A partir d'une recherche approfondie, les résultats ont montré que le fond a été déposé par un Étranger qui a décédé avec toute sa famille au cours d'un accident d'avion en 2003.
Et depuis lors, le compte son compte est resté sans aucune réclamation de qui que ce soit, c'est à cet effet que je sollicite humblement votre aide et votre coopération afin de vous présenter à la banque en tant que bénéficiaire de ces fonds pour notre bien commun.

[102] Scam est le concept anglais désignant un type de fraude pratiqué sur Internet. Surnommé « arnaque à la nigériane ou à la zaïroise », cette méthode est née au XVIème siècle sous l'appellation « captive espagnole ». Elle consistait en l'envoi d'une missive provenant d'une personnalité d'un pays lointain qui prétendait avoir des ennuis avec la justice et cherchait de l'aide pour transférer ses fonds à l'étranger contre un pourcentage de sa fortune. Le stratagème a refait surface à la Révolution française sous la dénomination de « lettre de Jérusalem », les courriers émanant alors de riches prisonniers. Elle a pris le nom de scam 419 (scam pour « arnaque », le chiffre 4-1-9 correspondant à la section du code pénal nigérian qui criminalise cette pratique), lors de la seconde moitié du XXème siècle. [Source : Christophe CORNEVIN, **Explosion des arnaques à l'africaine sur Internet**, ©Le Figaro, 12 Juillet 2007 (extrait)]

Soyez sûr que toutes les procédures seront surveillées ici par moi jusqu'à ce que vous réceptionniez ces fonds dans votre compte bancaire.

Nous partagerons cette fortune comme suit : 35% pour vous, 5% pour toutes les dépenses effectuées au cours de ce transfert et 60% pour mon associé et moi.

Rassurez vous que ce transfert est sans risque, à 100%, car nous avons pris toutes les dispositions pour son bon déroulement.

Nous avons prévu un délai de 21 jours ouvrables pour amener la banque à procéder au transfert de ce fond dans votre compte bancaire.
En outre, cette transaction devrait être traitée avec la plus grande confidentialité pour la simple raison que je suis toujours en service dans cette banque.

Si vous êtes intéressé par cette affaire, donnez-moi une réponse afin que je vous envoie plus amples détails sur son déroulement.

Merci pour votre coopération.

A bientôt

M USMAN DIALLO. »

C. LE PHISHING OU HAMEÇONNAGE

Le hameçonnage, traduit de l'anglais phishing, désigne métaphoriquement le procédé criminel de vol d'identité par courriel. Il s'agit *d'aller à la pêche de renseignements personnels dans un étang d'utilisateurs Internet sans méfiance*[103].

Cette pratique consiste à amener par la ruse les utilisateurs Internet à dévoiler des informations personnelles ou financières par le biais d'un message électronique ou d'un site web frauduleux.

[103] SERRE Diane et CLUZEAU Anna, **La cybercriminalité : nouveaux enjeux de la protection des données**, in www.memoireonline.com

Ce type d'escroquerie est *généralement initié par un message électronique apparemment officiel en provenance d'une source de confiance, telle qu'une banque, une société de carte ou un commerçant en ligne qui a bonne réputation. Le message électronique conduit alors les destinataires vers un site web frauduleux où ils sont invités à fournir des informations personnelles, telles qu'un numéro de compte ou un mot de passe. Ces informations sont généralement exploitées à des fins de vol d'identité*[104].

Voici un exemple d'un mail qui frise le hameçonnage :

« Cher Membre,

En raison de la congestion de tous les utilisateurs de Hotmail et l'enlèvement de tous les comptes inutilisés Hotmail , Hotmail serait obligé de fermer votre compte, vous devrez confirmer votre e-mail en remplissant vos informations de connexion ci-dessous au cas où le formulaire n'est pas totalement rempli votre compte sera suspendu dans les 72 heures pour des raisons de sécurité.

Confirmation de votre identité. Vérification de votre compte Hotmail.

Nom:.....Prénom:.....

Date de Naissance :.....

Adresse Hotmail:.....

Mot de Passe:.....

Information

Région:.....

Pays:.....

Occupation:.....

Après avoir répondu au questionnaire et après vérification par nos services votre compte Hotmail continuera de fonctionner normalement. Tout refus de coopération entraîne la suppression systématique du compte Hotmail. Tout en nous excusant pour ces désagréments.

[104] Voir la définition de « Hameçonnage » dans le dictionnaire informatique DICO, sur http://dico.studiovitamine.com (consulté le 23 juillet 2010)

Sincèrement

Service Hotmail ».

D. LA LOTERIE INTERNATIONALE

Le concept de loterie désigne *le jeu de hasard où l'on tire au sort des numéros gagnants correspondant à des lots. Au sens figuré, il désignerait toute affaire de hasard*[105]. Le corollaire de cette pratique est le « pari » : *engagement mutuel entre des personnes qui soutiennent des choses contraires, de payer une somme fixée à celui qui aura raison*[106].

Le stratagème est le suivant[107] : la future victime reçoit un courrier électronique indiquant qu'elle est l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euros ou de dollars américains. Pour empocher le pactole, il suffit de répondre à ce courrier. Apres une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant que le concerné est bien le vainqueur, son interlocuteur lui expliquera que pour pouvoir toucher ladite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses, etc.

Nous invitons nos lecteurs à se pencher sur ce mail personnel qui illustre le commencement de cette pratique :

« Resultat.bill.gate à gagnant
Bonjour,
Nous avons le plaisir de vous annoncez que vous êtes l'un des heureux gagnants de la Fondation BILL GATE. Les résultats ont été libérés et vous fait bénéficier de 150.000 €. Nous vous recommandons de fournir au Huissier GUY LEROY les informations telles que : Nom - Prénom - Sexe-Date de naissance - Profession - Téléphone (fixe) - Téléphone (mobile) - Émail - Ville - Pays par email à l'adresse : huissier.guyleroy@yahoo.ca
Pour tous renseignements veuillez contacter la direction de revendication dirigé par JOHN COXTE A LONDRES : +44 70 111 74 524
Merci de vite faire diligence ».

[105] Voir la définition de « Loterie » dans le dictionnaire MEDIADICO, disponible sur www.mediadico.com
[106] Ibidem.
[107] Voir l'article « Arnaque par mail-loteries », sur http://www.commentcamarche.net/contents/attaques/loteries.php.3 (consulté le 23 juillet 2010).

III. LA CYBERCRIMINALITE ET LE DROIT PENAL CONGOLAIS

Au point précédent (II), nous avons, par un aperçu systématique et empirique, éclairé nos lecteurs sur le caractère polymorphe de la cybercriminalité qui se présente comme une délinquance aux multiples facettes. Toutes les différentes inconduites que nous avons passées en revue, portent atteinte à plusieurs valeurs protégées par le code pénal congolais et à toutes les valeurs créées par les NTIC, à savoir : la confidentialité des systèmes informatiques, des réseaux et des données ; leur intégrité ; leur disponibilité ; et leur utilisation conforme ou licite.

Certains de crimes analysés au point précédent, sont déjà déplorés en République Démocratique du Congo, *la plupart des cas se dénombrant dans le chiffre noir de la criminalité*[108] ; bien évidemment parce que, estimons-nous, nombre de congolais usagers des NTIC sont peu enclins à signaler aux autorités compétentes les atteintes dont ils sont victimes, considérant qu'il s'agit d'un épiphénomène ou que leur plainte resterait lettre morte parce que les acteurs (cyberdélinquants) agissent souvent à partir d'un *pays tiers*[109].

Par ailleurs, la non incrimination par le code pénal des différents crimes relevant de la cybercriminalité, est du aux obstacles que celui-là rencontre sur le chemin de celle-ci. Dans le présent titre, nous fixerons nos lecteurs sur certains points d'anachronisme du droit pénal congolais et l'inadéquation entre celui-ci et la cybercriminalité, tout en envisageant une opportunité d'adaptation de celui-là à l'évolution galopante de celle-ci.

En effet, le droit pénal obéit à certains principes cardinaux qui fondent son rigorisme ; parmi eux, nous pouvons inventorier les principes ci-après : **la légalité criminelle** ; **l'interprétation stricte de la loi pénale** ; **l'autonomie du droit pénal** ; **l'In dubio pro reo** ; **la territorialité**, **la personnalité et l'universalité de la loi pénale**. A ceux-ci, nous pouvons joindre les principes relatifs à la **qualification des faits**, au **concours d'infractions**, à la **qualification d'infraction** et à la **tentative punissable**.

Tous les principes sus énumérés, précieux au droit pénal congolais, sont –hélas !- battus en brèche par la cybercriminalité qui, par sa nature complexe, ne peut être embobinée par lesdits principes.

Les règles de procédure pénale relatives aux **organes chargés de la répression**, aux **pouvoirs et procédures reconnus aux autorités judiciaires**, à la **preuve**, à l'**extradition** et à la **coopération internationale** contre le crime sont mis en mal par la cybercriminalité…

[108] MANASI NKUSU, **Op.cit**., in idem
[109] La fréquence a démontré que la quasi-majorité des bourreaux des congolais, réside en Europe et en Afrique de l'ouest.

A présent, nous allons procéder à une légère démonstration de l'inadéquation entre quelques principes fondamentaux du système pénal congolais sus énumérés et la cybercriminalité :

III.1. Le principe de la légalité criminelle face à la cybercriminalité.

Traduit du latin « nullum crimen, nulla poena sine lege » (pas de crime, ni de peine sans loi), le principe de la légalité des délits et des peines, conceptualisé au XVIIème siècle[110], dispose qu'*on ne peut être condamné pénalement qu'en vertu d'un texte pénal, précis et clair*[111]. En d'autres termes, un acte ne peut être considéré comme infractionnel que s'il était déjà prévu et qualifié comme tel par le code pénal antérieurement à son exécution. Ainsi donc, *une action ou une abstention, si préjudiciable soit-elle à l'ordre public, ne peut être sanctionné par le juge que lorsque le législateur l'a visée dans un texte et interdite sous la menace d'une peine*[112].

A. Vitu note ce qui suit au sujet du principe sous analyse : « *Le principe de la légalité criminelle, clef de voûte du droit pénal et de la procédure pénale, impose au législateur, comme une exigence logique de sa fonction normative, la rédaction de textes définissant sans ambiguïté les comportements qu'ils érigent en infractions, et les sanctions qui leur sont attachées. La loi criminelle ne peut assurer pleinement et véritablement son rôle de protection contre l'arbitraire possible des juges et de l'administration, sa mission pédagogique à l'égard des citoyens soucieux de connaître le champ de liberté qui leur est reconnu, et son devoir de prévention générale et spéciale à l'encontre des délinquants potentiels, que si elle détermine avec soin les limites du permis et de l'interdit(…)».*[113]

Le principe de la légalité criminelle, consacré par des *instruments juridiques internationaux*[114], a été transposé dans l'*ordre normatif congolais*[115], notamment dans la constitution et dans le code pénal. Il constitue un rampart contre l'arbitraire des acteurs judiciaires et garantit une justice équitable…

---

[110] Le principe de légalité des délits et des peines était appliqué probablement depuis des temps fort anciens. Il n'a cependant été identifié et conceptualisé qu'au Siècle des Lumières; il est généralement attribué à Cesare Beccaria qui publia anonymement en l'été 1764 à Livourne, l'ouvrage « *Dei delitti e delle pene* » (*Des* délits et des peines).

[111] Lire l'article « Principe de légalité en droit pénal » sur Wikipédia, l'encyclopédie libre disponible sur http://dictionnaire.sensagent.com/principe+de+l%C3%A9galit%C3%A9+en+droit+p%C3%A9nal/fr-fr/ (consulté le 30 juillet 2010

[112] Parvèz A.C. DOOKHY, **Le comité judiciaire du conseil privé de la reine Elizabeth II d'Angleterre et le droit mauricien**, in www.memoireonline.com (consulté le 29 juillet 2010)

[113] A.VITU, **Le principe de la légalité criminelle et nécessité des textes clairs et précis** (Observations sous Cass.crim. 1er février 1990, Rev.sc. crim. 1991 555), disponible sur http://ledroitcriminel.free.fr/la_science_criminelle/penalistes/la_loi_penale/generalites/vitu_principe_legalite.htm (consulté le 30 Juillet 2010).

[114] Notamment la déclaration universelle des droits de l'homme de 1948 dans ses articles 9,10 et 11

[115] Voir l'article 17 de la Constitution de RD Congo du 18 Février 2006, ainsi que l'article 1 du Décret du 30 janvier 1940 portant code pénal.

La quasi-majorité d'inconduites naissantes de la cybercriminalité, c'est-à-dire celles qui sont liées à l'essence même des NTIC, restent méconnues de notre arsenal juridique pénal. Logiquement, ces crimes échapperaient à toute poursuite judiciaire parce qu'elles ne sont pas encore érigées en infractions ! Cette anachronisme substantiel du droit pénal congolais face à l'évolution des NTIC et des dangers y afférents, est de nature à cautionner l'impunité, car qu'on se le dise, la cybercriminalité est déjà une réalité en république démocratique du Congo. Une adaptation du code pénal congolais s'avère imminemment nécessaire et impérieuse. La *commission permanente de réforme du droit congolais*[116] a donc du pain sur la planche ; mais surtout, attention à l'arriéré technologique !

III.2. Le principe d'interprétation stricte de la loi pénale et la cybercriminalité

Traduit du latin « poena sunt restringendam » (littéralement : les peines sont à restreindre), le principe d'interprétation stricte de la loi pénale est le corollaire[117] direct du principe de la légalité des délits et des peines sus évoqué. Il peut se définir comme « rien que la loi pénale, mais toute la loi pénale »[118].

ROUX note : « Interpréter la loi pénale, c'est en déterminer la signification, afin d'en permettre ou d'en donner l'application exacte. L'interprétation des lois est une nécessité, parce qu'il est impossible, et d'ailleurs peu désirable, que la loi renferme l'indication de toutes les hypothèses particulières, susceptibles de se présenter, et règle chacune d'elles par une disposition spéciale. Pour demeurer claire, la loi doit rester concise, et contenir simplement l'énonciation des règles générales, en laissant à l'interprétation le soin d'adapter ces règles aux espèces concrètes »[119].

Le principe d'interprétation stricte de la loi pénale dispose que les textes pénaux sont d'interprétation stricte. D'ailleurs, selon Beccaria et Montesquieu[120], les juges devraient appliquer mécaniquement la loi pénale sans pouvoir l'interpréter.

Par ailleurs, l'interprétation stricte de la loi pénale s'oppose à *l'interprétation analogique* et à *l'interprétation restrictive*. La première consiste à étendre une règle de droit d'une situation prévue par elle à une situation voisine. La seconde, inversement, ferait échapper à la loi pénale des cas prévus par le législateur.

---

[116] Créée par la LOI 76-017 du 15 juin 1976 relative à la création d'une Commission permanente de réforme du droit zaïrois.

[117] Voir Stefanie(Gaston) et Ali, **Droit pénal**, 13ème édition, Dalloz, Paris, p.193 ; J.C. SOYER, **Op.cit**., p.59

[118] Voir la signification du principe de l'interprétation de la loi pénale sur http://fr.wikipedia.org (consulté le 21 juillet 2010)

[119] ROUX J.-A., **De l'interprétation des lois pénales (suivant la science rationnelle)**, in Cours de Droit Criminel, 2ème édition, 1927, disponible sur http://ledroitcriminel.free.fr

[120] Cité dans l'article « Principe de légalité », sur http://www.etnoka.fr/qualified/attachment/101739/LE%20PRINCIPE%20DE%20LEGALITE.doc (consulté le 29 juillet 2010).

La prohibition de ces deux modes d'interprétation n'est pas comparable : *l'interprétation analogique viole ouvertement la prévisibilité de la loi pénale et la sécurité juridique. L'interprétation restrictive, quant à elle, ne contrarie que la séparation des pouvoirs, dans un sens favorable aux intérêts de la personne poursuivie*[121].

C'est effectivement au sujet du principe de l'interprétation de la loi pénale qu'il nous parait opportun d'ouvrir le débat en rapport avec les infractions classiques de la cybercriminalité, dont les auteurs se servent de l'internet pour parvenir à leurs fins. Prenons particulièrement pour cible les infractions du code pénal congolais contre les propriétés, et singulièrement l'infraction de « vol ».

En effet, le code pénal congolais dispose à son article 79 : « quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol ». Il transpire de cette disposition que le vol est la soustraction frauduleuse d'une chose appartenant à autrui dans le but de s'en approprier. Cette acception est largement retenue par la *doctrine*[122]. Les éléments constitutifs de cette infraction, se rapporte donc à la *chose*, à la *soustraction*, et à la *fraude*. La matérialité de cette infraction comprend la *soustraction de la chose d'autrui* ; sa moralité, la *fraude* qui en est le mobile.

Dans le cadre de cette étude, nous limitons notre analyse à la matérialité de l'infraction du vol, c'est-à-dire la soustraction de la chose d'autrui. C'est ici toute une épineuse question d'incompatibilité entre le droit pénal congolais et la cybercriminalité. En effet, comme tous les systèmes de droit pénal traditionnel, le droit pénal congolais vise surtout à protéger des biens tangibles clairement définis contre les attaques menées par des individus. En revanche, *les délits informatiques violent fréquemment de nouvelles valeurs intangibles dépendant d'un équilibre délicat d'intérêt et se prêtant peu à peu à une définition par le biais de termes et des dispositions généraux*[123].

Revenons donc à la matérialité de l'infraction de vol pour illuminer la compréhension de nos lecteurs. Elucidons tout d'abord le concept de « chose » pour ensuite s'attaquer à celui de « soustraction ». En effet, le législateur emploi le terme « chose » sans pour autant en donner une définition juridique. C'est donc vers la doctrine qu'il faut se tourner pour essayer de trouver des tentatives de définition juridique.

D'emblée, il sied de relever qu'une confusion plane au sujet de la différence entre une *chose* et un *bien*. Frédéric ZENATI et Thierry REVET écrivent que « les biens sont des choses qu'il est utile et

[121] http://fr.wikipedia.org (consulté le 21 juillet 2010).

[122] Voir René GARRAUD, **Traité de droit pénal**, 3ème édition, Tome VI, n° 2371, Paris, 1935, p.102 ; LIKULIA, **Droit pénal spécial zaïrois**, Tome I, 2ème édition, LGDJ, Paris, 1985, p.375.

[123] Nacer LALAM, **Op.cit.,** p.79

possible de s'approprier ; tout ce qui n'est pas une personne peut être une chose »[124]. François Terré et Philippe Simler donnent quant à eux une définition intéressante de la *chose* quand ils mentionnent que « la chose ne se limite pas à ce qui tombe sous le sens, ce qui ne se conçoit physiquement, mais il peut s'agir de « toute affaire, tout ce dont il en va de telle ou telle manière(…) »[125]. *La chose n'a donc forcement pas une réalité physique, tout comme le bien*[126]. Par cette logique, l'on admettrait donc que la définition du vol, rappelons-le, la soustraction frauduleuse de la chose d'autrui, *inclurait les choses immatérielles, c'est-à-dire celles qui n'ont pas d'existence physique, telles que les forces de la nature*[127]. Ceci constitue une exception au principe.[128] C'est ainsi que le vol d'électricité a été admis par les différents cours et tribunaux de par le monde[129].

Et puisque, à la lumière de l'argumentaire précédent, les choses immatérielles sont intégrables dans la définition de l'infraction de vol telle que définie par la loi, le vol de données ou d'informations numériques le serait aussi par ricochet.

Mais il nous semble que ce raisonnement ne soit pas juridiquement soutenable ; parce que *le Droit pénal appréhende correctement le vol d'information à travers le vol de son support, qu'il s'agisse d'une soustraction de la chose permanente ou qu'il s'agisse d'une appréhension frauduleuse pendant le temps nécessaire à la reproduction de l'information ; mais le vol d'information, lui, est encore inconnu car le vol ne s'applique qu'à une chose « matérielle susceptible d'appréhension (physique) par l'auteur du vol » et le « vol d'information »* (y compris donc celui des données) *ne peut être appréhendé par la loi qu'à travers le vol de son support matériel*[130].

Le second (plutôt le premier) élément mis en relief par la matérialité de l'infraction du vol consiste en une *soustraction.* C'est à la fois une appréhension et un enlèvement. Garraud constate que *le vol ne peut avoir pour objet qu'une chose mobilière. En effet, écrit-il, l'enlèvement d'une chose suppose nécessairement que cette chose peut être transportée d'un lieu dans un autre, qu'elle peut être appréhendée et déplacée. Les immeubles ne peuvent pas être déplacés (…).Les choses*

[124] F. ZENATI et T. REVET, cités par Raphael RIVIERS, « Définition du bien », in Encyclopédie juridique des biens informatiques, 3 Aout 2004, disponible à http://encyclo.erid.net/document.php?id=173 (consulté le 18 juillet 2010)

[125] F.TERRE et P. SIMLER, cités par Raphael RIVIERS, **Art.cit**., in idem.

[126] Raphael RIVIERS, idem.

[127] CORLAY et IR, **Bulletin de la criminologie**, N° 13, Dalloz, Paris, 1979, p.509

[128] LIKULIA, **Op.cit**., p.381.

[129] Italie : C.Cass., 13 Juillet 1898, cité par René GARRAUD, **Op.cit.,** idem. ; *Jurisprudence congolaise* Elis.27 février 1940, Revue Juridique, 1943, p.103

[130] C.A. Grenoble, 4 Mai 2000, cité par Fréderic DUFLOT, **Op.cit.,** p.26 ; *Jurisprudence congolaise* : Elis.22 Fév.1944, Revue Juridique, 1944, p.133 ; 1ère Inst.app.Coq.21 aout 1958, Revue Juridique du Congo-Belge de 1958..

incorporelles, tels que les droits, les pensées, les idées, ne sont pas plus que les immeubles, susceptibles de déplacement, d'enlèvement et dès lors, elles ne peuvent être soustraites. Mais souvent, le droit est constaté par un titre. Ce titre est un objet corporel qui devient matière à soustraction. Alors, le vol ne porte pas sur le droit, mais uniquement sur le titre qui est effectivement une chose corporelle. D'autre part, la pensée peut être imprimée : lettre, manuscrit, livre, etc., sont susceptibles de vol, en tant qu'objets corporels et abstraction faite de ce qu'ils contiennent[131].

Ainsi donc, l'effet de dérober des données ou des informations numériques contenues ou consignées sur Internet, ne donnerait pas lieu à l'application des dispositions du code pénal sur l'infraction du vol. Ceci est une conséquence très logique du principe de la stricte interprétation de la loi pénale, un principe général de droit qui, rappelons-le, découle du principe de la légalité des délits et des peines consacré dans l'ordre normatif congolais.

III.3. Le principe de la territorialité de la loi pénale et la cybercriminalité

Le système de droit pénal congolais se fonde sur l'idée de la souveraineté nationale, de sorte que la portée directe des décisions judiciaires qu'il génère soit limitée au territoire national congolais[132].

Le principe de la territorialité de la loi pénale dispose que *celle-ci ne peut s'appliquer que dans les limites du territoire national de l'Etat auquel elle appartient, c'est-à-dire de l'Etat qui a édicté cette loi*[133].

Néanmoins, Internet est un media véritablement universel. Les aspects géographiques (tels que l'emplacement où l'information est physiquement stockée) revêtent une importance mineure. Les données transférées transitent par différents pays et régions en ignorant les frontières et les lignes de démarcation…

Un questionnement suscite une attention particulière : sur base du principe de la territorialité, quelle suite le Droit pénal congolais réserverait-il à un sujet étranger résidant dans son pays, qui, par le truchement d'Internet, escroquerait à partir de là un sujet congolais résidant au Congo au moment de faits, une somme colossale d'argent transférée via une compagnie de transfert de fonds ; magot transféré en échange d'un service prétendument légitime ? Quoi qu'il en soit, dans cette hypothèse, il me semble que le code pénal congolais serait pris en étau…

---

[131] R. GARRAUD, **Op.cit**., p.26

[132] En effet, les articles 149 de la Constitution et 2 du Code pénal sont relativement clairs à ce sujet. L'article 149 alinéa 2 de la Constitution de 2006 dispose : « La justice est rendue sur l'ensemble du territoire national au nom du peuple », alors que l'article 2 du code pénal dispose à son tour : « l'infraction commise sur le territoire de la république est punie conformément à la loi nationale ».

[133] Frédéric DESPORTES et Francis LE GUNEHEC, **Droit pénal, Principe de la territorialité de la loi pénale**, in http://www.oodoc.com/93389-territorialite-loi-penale-articles.php (consulté le 30 juillet 2010).

III.4. Le principe de la légalité de la preuve en droit pénal congolais et la cybercriminalité

Selon une expression de Merle et Vitu, La preuve a, en droit criminel, « une importance fondamentale : c'est autour d'elle que la procédure pénale gravite »[134]. La preuve a pour objet la commission d'une infraction. A cet effet, il s'agit de *rassembler les preuves de l'infraction et d'en rechercher le ou les auteurs. Cette infraction doit être prouvée dans tous ses éléments constitutifs : matériel, moral et légal*[135] .

Dans une procédure pénale, les auteurs d'une infraction doivent être identifiés et des solides preuves de leur culpabilité doivent être produites. Ces exigences compliquent les poursuites intentées contre les auteurs des délits informatiques commis à l'aide de réseaux dans la mesure où, surtout, Internet est difficile à contrôler et garantit –du moins aux utilisateurs avertis- un niveau élevé d'anonymat. *Les réseaux informatiques internationaux (dotés de relais de messagerie anonymes ou de dispositifs d'accès libre aux fournisseurs d'accès Internet) assurent aux contrevenants un anonymat qui ne pourra être levé que si tous les pays que la communication traverse décident de coopérer*[136].

Le droit congolais qui régit la preuve, en donne la nature et les modes. Le principe est celui de la *légalité et de la hiérarchisation de la preuve*[137]. Sur pied de l'article 198 du code civil congolais livre III, les modes de preuve sont énumérés dans un ordre précis.il s'agit de : la preuve littérale, la preuve testimoniale, les présomptions, les aveux des parties, et les serments. Cette législation ne semble pourtant dire quelque chose concernant la preuve électronique. Par ailleurs, S'agissant de la preuve en matière pénale, elle est, pour l'essentiel, *fondée sur la jurisprudence faisant application des principes généraux du droit*[138]. Sans doute, qu'il est malséant dans un droit qui se veut légaliste, comme le déplore Sohier, « de recourir aux principes généraux pour suppléer à l'absence de dispositions législatives, lorsque le législateur a omis de traiter une matière, non pour laisser libre jeu à l'interprète, mais au contraire pour écarter délibérément cette matière de son droit »[139]. Au reste, d'une manière générale, en Droit de procédure pénale, les différentes preuves

---

[134] Merle & Vitu, cités par Conte, P. & Maistre du Chambon, **Procédure Pénale**, 4è Ed. Armand Colin, Paris, 2002, p.31.

[135] Fourment F., **Procédure Pénale**, Manuel 2004-2005, 5è Ed. Paradigme, Orléans, 2004, p.24, 28

[136] Nacer LALAM, **Op.cit**., p.96

[137] KATUALA KABA KASHALA, **La preuve en droit congolais**, Ed. Batena Njambua, Kinshasa, 1998, p.43

[138] T. NGOY, **Op.cit.**, p.311

[139] Cité par RUBENS, **Op.cit**., p.53

sont les suivantes[140] : l'aveu ; le témoignage ; les constations matérielles ; les présomptions ou indices ; et les écrits…

Avec la dématérialisation de l'écrit par Internet qui a apporté des supports intangibles, donc une certaine dématérialisation de la preuve devenue électronique, la notion de preuve implique une nouvelle définition, un nouveau mode d'élaboration et des nouveaux effets juridiques. La signature électronique, en tant que preuve, elle devra juridiquement être définie par le législateur congolais pour permettre au juge et aux parties de s'en servir dans un procès mettant en évidence une inconduite perpétrée via ou contre des réseaux informatiques en générale et Internet en particulier...

ELEMENTS DE CONCLUSION

Mais il est temps de conclure. Je dois tout de même avouer que cette tâche me semble très délicate ! De mon étude, j'ai tiré les enseignements suivants :

1. la cybercriminalité est une nouvelle forme de délinquance qui se commet généralement sur des réseaux informatiques, en particulier sur le réseau Internet. Grace à l'éclosion et à la vulgarisation de ce dernier, non seulement des nouveaux actes antisociaux ont vu le jour, mais aussi des vieilles inconduites, déjà déplorées et réprimées dans différents systèmes pénaux, se sont perfectionnées. C'est ce polymorphisme (ambivalence) qui constitue le particularisme de cette délinquance électronique, et rend ambigüe toute tentative de sa conceptualisation : ni le législateur, ni la doctrine, aucun de deux ne parvient à contenir la cybercriminalité dans un cadre définitionnel précis pouvant permettre de cerner scientifiquement tous ses contours…

   Un nombre non moins important d'acteurs dangereux (cyberdélinquants) aux motivations assez diverses compétitionnent ingénieusement dans le cyberespace, en usant d'une gamme de techniques ou méthodes que l'on peut catégoriser en : (a) infections informatiques ; (b) attaques cybernétiques ; et (c) arnaques. Les deux premières sont constituées généralement des atteintes contre les réseaux informatiques en général et contre Internet en particulier ; tandis que la troisième catégorie est constituée de tromperies et escroqueries diverses commises via lesdits réseaux.

2. Toutes les inconduites couvertes par la cybercriminalité portent atteinte à certaines valeurs déjà protégées par le Code pénal congolais. D'ailleurs, un arsenal considérable desdites inconduites, notamment celles qui utilisent Internet seulement comme moyen de perpétration, ont déjà été érigées en infractions ; Ce ne sont alors que des « vieilles

[140] J.C. SOYER, **Op.cit.,** p.228.

marmites qui ont été embellies à la nouvelle cire» ; parmi elles, je peux citer par exemple le « vol ». Les variations dans la commission sur Internet de cette infraction, pourraient échapper aux prévisibilités du Code pénal, notamment à cause de l'orthodoxie de certains principes fondamentaux caractérisant le système pénal congolais ; nous citons entre autre le principe de la **stricte interprétation de la loi pénale**. Ainsi, pour cette infraction du vol, il importe seulement de la part du législateur congolais d'adapter notre Code pénal en essayant de redéfinir clairement l'un des ses éléments matériels, en l'occurrence la « chose » qui devrait concerner à la fois les choses matérielles et les choses immatérielles…

Dans l'état actuel de notre législation pénale, en ce qui concerne singulièrement le vol des données, renseignements et informations numériques, étant donné que la stricte interprétation de la loi pénale ne transige avec l'interprétation analogique, c'est-à-dire une possibilité d'intégration du « vol des données, renseignements et informations électroniques » dans les prévisions légales de l'infraction de « vol » telle que définie par l'article 79 du Code pénal congolais, je suggère donc au législateur :

3. L'institution au Code pénal d'une nouvelle incrimination, parmi les infractions dirigées contre les propriétés, qui aura pour intitulé : « De l'infraction du vol des données, renseignements et informations électroniques », serait un pas vers l'idéal poursuivi par ma présente étude. Cette solution aura pour avantage la qualification extensive de toutes les autres inconduites liées aux NTIC en infractions, en vue de leur éventuelle intégration au Code pénal. Il me semble que cette gymnastique legistique ne puisse être assez complexe pour notre législateur, car il suffirait de procéder par un « copier-coller » des cyberinfractions déjà traitées dans d'autres systèmes pénaux, pour les transposer dans notre Code pénal, comme cela a toujours été le cas –je révèle en effet ce secret de polichinelle- avec la quasi-majorité d'autres incriminations.

4. Somme toute, étant donné l'évidence de la délinquance électronique en République Démocratique du Congo, il appartient non solus au législateur de renforcer et moderniser les dispositifs législatifs sécuritaires en matières pénale et de télécommunications, sed etiam au gouvernement de ratifier des instruments juridiques de lutte contre la cybercriminalité et de multiplier des accords avec d'autres Etats dans le domaine de la coopération contre cette pandémie technologique qui, mettant en évidence un réseau transnational de communication, Internet, ne serait totalement neutralisée que par une politique internationale tous azimuts.

BIBLIOGRAPHIE DE REFERENCE

A. OUVRAGES, ARTICLES ET DOCUMENTATIONS DIVERSES

❖ *Sur la cybercriminalité et Internet :*

1) BENHAMOU B., « Petit essai de prospectives pour le cyberespace », Mars 2001, in www.homo-numericus.net
2) BENSOUSSAN A., **Les télécommunications et le Droit**, Paris, Hermès, 1996.
3) CAHEN (Murielle-Isabelle), « Internet et le droit d'auteur », Dossier SAM « Questions juridiques », Novembre 2000, in www.avocat-online.com
4) CHAWKI (Mohammed), « Essai sur la notion de cyber criminalité », IEHEI, Juillet 2006.
5) CORNEVIN (Christoph), « Explosion des arnaques à l'africaine sur Internet », Journal Le Figaro, 12 Juillet 2007.
6) FILIOL (Eric), **Le virus informatiques : théories, pratique et applications,** Springer, 2004.
7) LALAM (Naser), **La délinquance électronique**, Dossier problèmes politiques sociaux, Documents française, n° 953, Octobre 2008.
8) MARTIN D., **La criminalité informatique**, Paris, PUF, 1997.
9) MUKADI MUSUYI (Emmanuel), « La cybercriminalité est une réalité en République Démocratique du Congo », in http://www.digitalcongo.net
10) MUKADI MUSUYI (Emmanuel), « La cybercriminalité, le SIDA informatique », Revue LUBILA, N° 001 du 18 au 31 Janvier 2008, Kinshasa 2008.
11) MUKENDI WAFWANA (Emery), « Avocats congolais sur Internet : information ou publicité ? », 15 Juin 2000, in www.juricom.net
12) ONU : « Manuel pour la prévention et la répression de la criminalité informatique », Revue internationale de politique pénale, N° 43 et 44, 1995.
13) ROSE P., **Menaces sur les autoroutes de l'information**, Paris, Harmattan, 1996.
14) SERRE (Diane) et CLUZEAU (Anna), « La cybercriminalité : nouveaux enjeu de la protection des données », in www.memoireonline.com

❖ *Sur le Droit, la Criminologie et autres domaines connexes :*

1) CONTE P., et DU CHARBON M., **Procédure pénale**, 14ème édition, Paris, Armand-colin, 2002
2) CORLAY et IR, **Bulletin de la criminologie**, N° 13, Paris, Dalloz, 1979
3) DESPORTES (Fréderic) et LEGUNEHEC (Francis), « droit pénal, principe de la territorialité de la loi pénale », in www.oodoc.com
4) DURKHEIM (Emile), **Les règles de la méthode sociologique**, Paris, P.U.F., 1981

5) FERRI (Enrico), **La sociologie criminelle**, Paris, Alcam, 1905
6) FOURMENT F., **Procédure pénale**, Manuel 2004-2005, 5ème édition, Orléans, Paradigme, 2004
7) GARRAUD (René), **Traité de droit pénal**, 3ème édition, Tome VI, Paris, 1935
8) GASSIN (Raymond), **Criminologie**, 6ème édition, Paris, Dalloz, 2007
9) KATWALA KABA KASHALA, **La preuve en droit congolais**, Kinshasa, Batena Njambua, 1998
10) LAIGNEL LAVASTINE (Maxime) et STANGU(Vasil), **Précis de criminologie**, Paris, Payot, 1950
11) LEMAN-LANGLOIS, "Criminologie", vol 39, N° 1, 2006, in www.erudit.org
12) LIKULIA B., **Droit pénal spécial zaïrois**, Tome I, 2ème édition, Paris, L.G.D.J., 1985
13) PARVèZ DOOKHY, « Le comité judiciaire du conseil privé de la reine Elizabeth II d'Angleterre et le Droit mauricien », in www.memoireonline.com
14) ROUX J.-A., « De l'interprétation des lois pénales (suivant la science rationnelle) », Cour de Droit criminel, 2ème édition, 1927, in www.ledroitcriminel.free.fr
15) RUBBENS (Antoine), **Le droit judiciaire congolais : l'instruction criminelle et la procédure pénale**, Léopoldville-Bruxelles, Université Luvanium et Maison Larcier, 1965
16) SOYER (Jean-Claude), **Droit pénal et procédure pénale**, 10ème édition, Paris, L.G.D.J., 1993
17) STEFANI (Gaston), LEVASSEUR (Georges) et JAMBU MERLIN, **criminologie et science pénitentiaire**, 5ème édition, 1982.

B. MEMOIRES ET TRAVAUX SCIENTIFIQUES

1) DADJO (Cica Mathilda), **Les contrats dans le cyberespace à l'épreuve de la théorie générale : problèmes et perspectives**, Maitrise en Droit des affaires et carrières judiciaires, Université d'Abomey CALAVI-Benin, disponible sur www.memoireonline.com
2) GUILLEMARD S., **Le droit international privé face au contrat de vente cyberspatial**, Thèse de doctorat, Faculté des Etudes supérieures, Université CAVAL-Québec, Janvier 2003
3) MANASI NKUSU, **Le droit congolais et la criminalité de nouvelles technologies de l'information et de la communication**, Mémoire de D.E.A. en droit, Université de Kinshasa-RD Congo, 2006
4) NGOY (Théodore), **Le droit de la preuve dans l'avant procès en procédure pénale congolaise**, D.E.S., en Droit, Université de Kinshasa-RD Congo, 2006.

C. WEBOGRAPHIE

1) www.awt.be
2) www.bimarysec.fr

3) www.clusif.asso.fr
4) www.dfo-mpo.gc.ca
5) www.dicofr.com
6) www.fknet.fe
7) www.futura-sciences.com
8) www.itu.int
9) www.linux-france.org
10) www.louis-mpala.com
11) www.radisnoir.com
12) www.societecivile.cd
13) www.statistiques-mondiales.com
14) www.symantec.com

L'auteur vous remercie de l'attention que vous avez accordée à la lecture de cet essai de confrontation de la cybercriminalité au Droit pénal congolais.