ÉTUDE COMPARATIVE DE LA REPRESSION DE LA CYBERCRIMINALITE EN DROITS CONGOLAIS ET FRANÇAIS

Fiche pratique publié le **09/08/2014**, vu **77374 fois**, Auteur : Edmond MBOKOLO ELIMA

Les TIC apportent bel et bien des changements dans les sociétés partout dans le monde, elles améliorent la productivité des industries, révolutionnent les méthodes de travail et remodèlent les flux de transfert des capitaux, en les accélérant. Or, cette croissance rapide a également rendu possible des nouvelles formes de criminalité liées à l'utilisation des réseaux informatiques, appelées cybercriminalité, cyberbanditisme, cyberdéliquance, criminalité de hautes technologies ou criminalité des NTIC.

UNIVERSITE DE MBANDAKA

FACULTE DE DROIT

MEMOIRE DE LICENCE EN CYBERCRIMINALITE

(UNIMBA-RDC)/2013-2014

Sujet : « ETUDE COMPARATIVE DE LA REPRESSION DE LA CYBERCRIMINALITE EN DROITS CONGOLAIS ET FRANÇAIS »

Présenté par :

MBOKOLO ELIMA Edmond

Defenseur Judiciaire près le Tribunal de Grande Instance de Mbandaka

EPIGRAPHE

« Il y a près d'une trentaine d'années, une grande voix alertait les juristes. Dans son manuel de sociologie juridique, le Doyen CARBONIER observait que l'évolution des mœurs et des techniques donne matière à des nouvelles formes de délinquance. Aujourd'hui, cette observation résonne toujours avec autant de force et de gravité. Indéniablement, les nouvelles techniques d'internet ont changé radicalement nos civilisations. Elles ont bouleversé des pans entiers de la vie sociale, culturelle, économique, juridique et politique. Elles sont porteuses d'innombrables

avantages et opportunités. Mais les enjeux qui leurs sont attachés sont de nouveaux types de délinquance et suscité la commission de délits classiques. Cette délinquance d'un genre nouveau a pour nom la cybercriminalité ».

J. DJOGBENOU, *La cybercriminalité : enjeux et défis pour le Bénin*, disponible sur http://www.capod.org, consulté le 10/09/2013.

DEDICACE

Anotre mère **AMBA MOLA Marie Jeannette**, pour votre assistance et votre soutien combien adorable, inoubliable et extraordinairepour la relève de notre éducation et multiples sacrifices depuis le bas âge ; sans toi nous n'allions pas être ce que nous sommes aujourd'hui ; ainsi que pour le dévouement et le soutien financier manifesté à notre endroit. Vous n'avez pas voulu nous donner du poisson pour manger un jour, mais vous nous avez appris à pécher afin que nous mangions tous les jours en nous payant les frais pour nos études, et cela, nous restera inoubliable. Que le grand maitre de l'Univers puisse vous récompenser.

REMERCIEMENTS

Ce mémoire marque le couronnement d'un long processus de formation intellectuelle durant lequel nous avons consentis plusieurs sacrifices et privations. De ce fait, il ne serait pas réalisé sans l'aide ininterrompue, la compréhension et le dévouement d'un certain nombre de personnesqui, par leur disponibilité et leurs conseils, nous ont apporté tout leur soutien. Nous les en remercions et nous nous excusons de ne pouvoir toutes les citer.

A tout seigneur, tout honneur dit-on, nous adressons premièrement nos remerciements et de manière très respectueuse à notre Maître, Doyen de la Faculté, le Professeur Docteur Eddy MWANZO IDIN'AMINYE,pour avoir accepté non seulement à assurer la direction du présent mémoire mais aussi et surtout pour nous avoir encadré tout au long de notre cursus académique, ses orientations, son écoute et ses remarques, nous ont aidé à concevoir et finaliser ce travail avec modestie.

Nous réitérons les mêmes remerciements à l'endroit des Professeurs Docteurs Bienvenu WANE BAMEME et Raymond de Bouillon MANASI N'KUSU, respectivement pour sa disponibilité à assurer la première lecture de ce mémoire et nous avoir fourni les différentes sources nécessaires

pour la collecte des informations en rapport avec la cybercriminalité.

Nos sentiments s'adressent également à l'Assistant Sylvain ILONGA NZEE LOPANZA (mon frère bien-aimé), qui a bien voulu malgré ses multiples occupations assurer la co-directiondu présent mémoire.

Nos remerciements s'adressent également à toutes les autorités académiques, Professeurs, Chef de travaux et Assistant de la Faculté. Il s'agit du Recteur EKOKO BAKAMBO Gratien, Ivon MINGASHANG, Grégoire BASUE BABU KAZADI, José MUANDA, WESE, Jean Désiré INGANGE, Benjamin BOLITENGE LOPAKA, Georges NDJOLI, Jacques DJOLI, Albert KPANYA MBUNZU, AGR IKOBIA, Papy NZEKA, Willy LUANDA,Arseli MONGA MONGALA, Serge NZINGA, Bienvenu YAY, Dayiu WABI, Blaise ENYELA, Jeannot LIKILE, pour l'enseignement de qualité qu'ils n'ont cessé de nous dispenser pendant toutes ces cinq années de notre formation en Droit. Ils ont pu apporter chacun, sa contribution à la constitution de notre bagage intellectuel.

L'affection oblige d'adresser nos remerciements à tous nos frères germains à qui, nous avions traversé des moments épineux de la vie, en l'occurrence de l'Assistant Jérémie YELEMENGA, Thomas NZEE LOPANZA, Samson MOLA IHOMI et de notre assistant-informaticien Emmanuel BONKETO MBOKOLO, que Dieu vous patafiole.

Toute notre gratitude et reconnaissance vont directement à l'endroit de notre fiancée Esther BOMPOKO MBOYO (*Estha d'or*), pour l'amour et votre patience, que ce travail soit pour vous,un modèle à suivre tout au long de votre parcours universitaire à l'Institut Facultaire des Sciences de l'Information et de la Communication (IFASIC).

Nous nous sentons dans l'obligation de remercier tout particulièrement notre géniteur MBOKOLO ELIMA Edmond dont nous portons le nom et tous nosoncles paternels : à la personne de Mr MPUTU ELIMA Daniel ainsi qu'à sa femme Joséphine LOKUBAnotre maman de tous les jours età Papa Emmanuel BOLA.

Nous nous savons très redevable à tous nos frères et sœurs : Bébéta MBOKOLO, Denise AMBA NKENDO, Maître Dido NZEE, Pires ILONGA, Elie NGWELI, Huguette NZEE, Naomie NZEE, Coco NZEE, Yanick NGUBU, Daniel MPUTU, Noel BOLA, Nana MBOKOLO et Bienvenu IYELI ILANGA.

Nos remerciements s'adressent à notre belle famille BOMPOKO Emmanuel et à la Maman Théophile BOKELE qui nous ontbeaucoupassistés matériellement et moralement toutes les fois que nous étions dans le besoin.

Nous remercions confraternellement tous les avocats et défenseurs judiciaires du Cabinet BOSEMBE, à la personne de Maitre Philippe BOSEMBE, Maitre Teddy EKABELE, Maitre Afred BODJO, Maitre Didier LOTAWA, Maitre John ENDENGE et le Secrétaire Blaise ENGANGE, pour leur soutien intellectuel et leur encadrement professionnel.

Que le Révérend Pasteur MOBONGA LOBO Michée et le PDG Joseph INKUNE MBOYO, lisent également en ces lignes l'empreinte de notre redevance à la hauteur de leur soutien moral, financier, professionnel et spirituel.

Nos remerciements s'adressent également à la famille du Général José Alexandre BAKEMO ainsi qu'à sa femme Gertrude BOKOYA BANGOSEMA, notre amie de lutte, pour leur soutien combien immesurable.

Enfin, nous ne pouvons pas clore cette page de remerciements sans témoigner notre gratitude à

nos amis, connaissances et compagnons de lutte : Rebecca EKUMBAKI, Peter KOGERENGBO, Socrate ILONGA, Ovide MANZANGA, Michel MAKAILA, Platini IKWA, Faustin BATOLUKA, Anicet TOSUKU, Jules MAZOKO, Pitcho SINALA, Metuchelah NDOMBE, Barnabas LOOMA, Ruth EFOYA et tous ceux dont les noms ne sont pas repris ici qui, de près ou de loin, nous ont conduit à parfaire cette œuvre scientifique, cueillent à ce jour des fleurs d'une généreuse collaboration.

PRINCIPALESABREVIATIONS

- @ : Arobase
- § : Paragraphe
- AGR : Avocat Général de la République
- BE : Belgique
- BIOS : Basic In/Out System
- B.O. : Bulletin officiel
- CA : Canada
- CCL1 : Code civil livre premier
- CD : Congo Démocratique
- CH : Chine
- CLUSIF :Club de la Sécurité de l'Information Français
- COM : Commercial
- CPI : Code de la Propriété Intellectuelle
- D.E.A : Diplôme d'Etudes Approfondies
- D.E.S : Diplôme d'Etudes Supérieures
- DOS : Denial of Service (déni de service)
- Ed. : Edition

- EDVAC : Electronic Discret Variable Computer
- E-MAIL : Electronic Mailing (courrieléléctronique)
- ENIAC : Electronic numerical integrator and computer
- FR : France
- G2 : Deuxièmegraduat
- G3 : Troisièmegraduat
- GD : Grenade (pays)
- HTTP : Hypertext transfert protocol (protocole de transfert

des textes)

- INTERNET : Interconnected Network
- IP : Internet Protocol
- J.O.RDC : Journal Officiel de la République Démocratique du Congo
- J.O.Z : Journal Officiel du Zaïre
- L1 : Première année de licence
- LAN : Local Area Network
- L.G.D.J : Librairie Générale de Droit et de Jurisprudence
- MAN : MetropolitanArea Network
- MS : Microsoft
- Mr : Monsieur
- MS-DOS : Microsoft disk operating system
- N° : Numéro
- NET : Network
- NT : Nouvelle technologie
- NTIC : Nouvelles technologies de l'information et

de la communication

- Op.cit. : Operecitate (fait référence à une source déjà citée)
- ORG : Organisation
- OTAN : Organisation du traité de l'Atlantique Nord
- P. : Page
- PC : Personnal computer (ordinateur personnel)
- PDG : Président Directeur Général
- PUF : Presse universitaire française
- RDC : République Démocratique du Congo
- ROM : Read OnlyMemory (mémoire en lecture seule)
- S. : Suivant (s)
- SD : Sans date
- SL : Sans lieu
- SPAM : Spamming (pourriel)
- SQL :StructuredQueryLanguage
- T. : Tome
- TCP :Transmission control Protocol
- TIC : Technologie de l'Information et de la Communication
- UNIKIN : Université de Kinshasa
- UNILU : Université de Lubumbashi
- UNIMBA : Université de Mbandaka
- UPC : Université Protestante au Congo
- Voy. : Voyons
- WAN : Wide Area Network

- WWW : World Wide Web (toile d’araignéemondiale)

INTRODUCTION GENERALE

La cybercriminalité soulève tant des problèmes qui ne sont pas toujours bien cernés par le droit. Dans le cadre de ce mémoire, nous nous proposons d’analyser ***l’étude comparative de la répression de la cybercriminalité en droits congolais et français***, sujet intéressant qui exige pour être bien abordé que soit posée son état de la question (A), saproblématique (B), formulée son hypothèse (C), ressorti son intérêt (D), délimité le champ de son investigation (E), déterminées les différentes méthodes et techniques de recherches utilisées (F), et enfin, élaboré un plan sommaire (G).

A. Etat de la question

Il est dit que le domaine scientifique, particulièrement celui de la recherche, reste un champ où règnent la complémentarité, la réformation, les suggestions, les critiques et les remarques.Ainsi, « il peut arriver à un chercheur de trouver que, même si sa recension initiale des théories et recherche ne l’a pas amené à penser à un problème qui se prête à une investigation scientifique, après avoir découvert un certain nombre des travaux antérieurs peuvent se révéler pertinents »[1].

Par ailleurs, « même si la problématique est posée de façon pertinente, il est recommandé de vérifier les résultats de la recherche antérieure ainsi que toutes documentations sur la théorie qui pourraient se rapporter au thème sous examen »[2].C’est dans cette logique que nous n’avons pas la prétention d’être le premier à consacrer une étude de portée scientifique en rapport avec ce thème de recherche. En effet, il y a d’autres chercheurs qui l’ont abordé sous d’autres cieux et de manière approchée ; et dont les avis seront par nous repris.

Ainsi dit, SERRES DUANNE et CLUZEAU Anna, dans leur mémoire de maîtrise intitulé "la cybercriminalité nouveaux enjeux de la protection des données" abondent que « le développement des nouvelles technologies de l’information et de la communication et la vulgarisation d’internet ont provoqué des bouleversements majeurs, tant au niveau de la communication, à l’échelle mondiale qu’au niveau du droit applicable. On voit émerger de nouveaux modes de

communication, révolutionnées par cette possibilité de connecter le monde entier en permanence et notamment de nouveaux modes d'échanges, comme le commerce en ligne. Néanmoins, ce développement a aussi ses revers, et ont permis l'apparition d'une nouvelle menace : la cybercriminalité. Celle-ci est une notion polymorphe qui peut concerner les infractions classiques commises par le biais de nouvelles technologies, comme des nouvelles infractions nées de l'essence même de ces nouvelles technologies »[3].

FISTEL MEKONGO BALLA opine dans le même sens que ses prédécesseursen estimant que « le développement des nouvelles technologies de l'information et de la communication ouvre un nouvel espace. L'espace informationnel vient désormais s'ajouter aux espaces terrestre, maritime et aérien dont la protection et la sécurité entrent naturellement dans le champ de compétences régaliennes de l'Etat. Ainsi, toute activité humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. La cybercriminalité est l'une des nouvelles formes de criminalité et de délinquance, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective. La cybercriminalité est définie comme l'ensemble des infractions pénales susceptibles de ses commettre sur les réseaux de télécommunication »[4].

ERICK LEVI LIBENDE MIBOLU affirme quant à lui que, « la cybercriminalité est une notion large qui regroupe toutes infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau »[5].

GATIEN HUGO allègue pour sa part que « la plupart des grandes découvertes technologiques ont engendré, à côté des progrès économiques, sociaux et culturels qui en sont la finalité sociale, des retombées négatives diverses, parmi lesquelles figurent au premier chef la délinquance. L'invention de l'information et son développement fulgurant au cours des quarante dernières années ont en effet engendré une délinquance qui n'a cessé de se multiplier »[6].

En ce qui nous concerne, nous amorcerons notre sujet dans un angle comparatif. C'est pour cela qu'il nous sera important de faire une étude comparative de la répression de la cybercriminalité en droits congolais et français.

Toutefois, à en croire le Professeur Sylvain SHOMBA KINYAMBA lorsqu'il précise que « après avoir choisi un thème, le chercheur doit être capable de formuler un problème spécifique qui prête à l'investigation scientifique… »[7]. Il s'agit en clair, de bien poser la problématique du sujet de recherche.

B. Problématique du sujet

Une problématique « c'est l'art de poser les problèmes. Problématiser, c'est donc être capable d'interroger un sujet pour en faire sortir un ou plusieurs problèmes. Au-delà, l'élaboration d'une problématique suppose la capacité à articuler et hiérarchiser ces problèmes »[8]. En fait, c'est l'art de poser des questions pertinentes, qui est l'une des caractéristiques de toutes activités scientifiques.

Pour le Professeur Sylvain SHOMBA KINYAMBA, «la problématique signifie problème à résoudre par des procédés scientifiques. La problématique désigne l'ensemble de question posée dans un domaine de la science, en vue d'une recherche des solutions. C'est en outre, un ensemble d'idées qui spécifient la position du problème suscité par le sujet d'étude»[9].

Ainsi donc, dans cette étude, notre problème majeur va s'articuler autour de la cybercriminalité, l'objet principal de notre investigation.

En effet, « la révolution de l'information et de la communication promet d'être aux XXIème siècle ce que la révolution industrielle fut au XIXème. Ce phénomène nouveau qui nous propulse aux portes du cybermonde, dans une ère nouvelle, dont les projets d'autoroutes de l'information, internet, les multimédia, la télévision numérique ou la réalité virtuelle, sont les nouveaux outils d'une communication et d'une information à l'échelle planétaire »[10].

Certes, « les changements potentiels charriés par cette nouvelle ère sont si profondes, qu'ils posent des questions fondamentales sur l'organisation de nos sociétés, le devenir de l'homme et du citoyen »[11].

A vrai dire, beaucoup de découvertes techniques ont aussitôt suscité de nouvelles formes de criminalité et le problème se pose alors de savoir comment les juges vont réagir, compte tenu des textes qu'ils ont à leur disposition alors que ces textes ont été écrits par un législateur qui ne pouvait imaginer les découvertes postérieures à son action. En effet, « le problème se pose également pour l'informatique. L'existence et l'utilisation des ordinateurs peuvent bien évidement être source de comportements nuisibles aux tiers »[12].

Par conséquent, « l'apparition du *"personnel computer"* (PC), il y a une vingtaine d'années, et, depuis une dizaine d'années, l'interconnexion mondiale des ordinateurs, grâce à l'internet, ont créé dans la société un rapport tout autre à l'information. La technologie de l'information avance à pas de géant et internet connait une croissance exponentielle : on assiste à une véritable révolution de l'information »[13].

Ceci étant, « la société moderne est tributaire d'infrastructure de l'information sensibles. L'information et la communication, les banques, l'approvisionnement en énergie, électricité hydrocarbure et gaz, le transport et la logistique, de même que la santé et le secours, dépendent tous de l'informatique et des télécommunications. Ces structures qui nécessitent des technologies de plus en plus sophistiquées et complexes, n'en deviennent que plus vulnérables »[14].En fait, « ces progrès ont rapidement rendu obsolètes les mesures de protection des technologies de l'information et de la communication, pourtant sujettes aux pannes, erreurs et agressions électroniques. Le rôle essentiel que joue l'informatique dans les domaines les plus nécessaires à la société et l'interconnexion des infrastructures de l'information sur le plan national et international, peuvent potentiellement être sources de dommages non négligeables »[15].

Par ailleurs, « les technologies de l'information et de la communication (TIC) apportent des changements dans les sociétés partout dans le monde :elles améliorent la productivité des industries traditionnelles, révolutionnent les méthodes de travail et remodèlent les flux de transfert des capitaux en les accélérant. Or cette croissance rapide a également rendu possible de nouvelles formes de criminalité liées à l'utilisation des réseaux informatiques »[16].

Somme toute, il est difficile de bien saisir ou de conceptualiser où commence la criminalité liée à l'informatique. On considère souvent qu'elle continue une conduite proscrite par la législation et/ou la jurisprudence et qui nécessite l'utilisation des technologies numériques dans la commission du délit ; qui est dirigée contre les technologies de traitement des données et de communication elles-mêmes ; ou qui fait intervenir l'utilisation accessoire d'ordinateurs en vue de la perpétration d'autres délits. De toute évidence, « les réseaux numériques, singulièrement l'internet, peuvent être l'instrument d'abus relativement spécifique, en ce qu'ils ont pour cibles des biens de l'informatique. On parle, dans ce cas, *de "criminalité informatique",* à moins d'utiliser un néologisme dans le vent tel que cybercriminalité ou cyberterrorisme »[17].

En clair, les comportements répréhensibles sont diversifiés. Mais l'internet est aussi le support d'infractions tout à fait conventionnelles, qui peuvent se commettre par d'autres moyens.Cela

étant, « le côté 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, appelée aussi cyberdélinquance, délinquance électronique, etc… »[18].

A en croire MITONGO KALONDJI, « la cybercriminalité est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité humaine. La cybercriminalité est la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires »[19].

En conséquence, « la cybercriminalité est l'une des nouvelles formes de criminalités et de délinquance, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective, pour notre économie et bien sûr, pour les citoyens qui peuvent être personnellement atteints, dans leur dignité et dans leur patrimoine »[20]. En effet, la cybercriminalité est une notion large qui regroupe toutes les infractions susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau. Il s'agit donc d'une nouvelle forme de criminalité et délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel appelé le cyberspace.

« Depuis quelques années, la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du cybercrime »[21]. Trésor Gauthier MITONGO estime que « parler de la cybercriminalité est assez délicat, puisqu'il s'agit d'une notion émergente, dont la conceptualisation est assez complexe. Cette notion est polymorphe, car elle peut concerner aussi bien des infractions classiques ou conventionnelles commises par le biais d'internet, que des nouvelles infractionsnées de l'essence même de cet outil informatique »[22]. 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 ? »[23].

De ce qui précède, et dans le but de construire un raisonnement logique autour de notre sujet de recherche, nous avons trouvé utile de s'interroger sur l'étude comparative de la répression de la cybercriminalité en Droits congolais et français. Raison pour laquelle, pour aboutir et arriver à atteindre tous les objectifs que nous nous sommes assignés et pour mener à bon port notre étude scientifique, nous avons trouvé aisé de soulever plusieurs questions, qui constituent la quintessence de notre préoccupation, à savoir :

1. *Quelle place occupe le principe de la légalité criminelle vis-à-vis de la cybercriminalité en RDC ?*
2. *Que peut-on entendre par nouvelles technologies de l'information et de la communication (NTIC) ? Il y a –t-il des comportements nuisibles dans leur usage ? Si oui, quid la cybercriminalité ?*
3. *Existe-t-il un système juridique efficient pour la répression de la cybercriminalité au Congo(RDC) et en France ? Si oui, quels en sont les mécanismes de droit prévus par les législateurs de ces deux pays pour faire face à cette nouvelle forme de criminalité?*

Dès lors, il sera de notre devoir dans ce travail de mener une analyse minutieuse, en vue de porter réponses aux six questions de départ, qui pour répondre aisément aux nécessités d'ordre scientifique, une suite des réponses provisoires méritent d'être retenues à titre d'hypothèse, car dit le Professeur Sylvain SHOMBA : « toute bonne problématique part d'un état de la question et

débouche sur des hypothèses »[24].

C. Hypothèse du travail

D'entrée de jeu, une hypothèse est entendue comme « une proposition de la réponse à la question posée »[25].Abondant dans le même sens, le Doyen Maurice DUVERGER estime quant à lui que « une hypothèse, est une réponse dont la recherche a pour but de vérifier le bien ou le mal fondé de la question que l'on se posé »[26]. A vrai dire, l'hypothèse cherche à établir une vision provisoire du problème soulevé en évoquant la relation supposée entre les faits sociaux dont le rapport constitue le problème et en indiquant la nature de ce rapport.

Ainsi comprise, la question de la définition de l'hypothèse n'a pas concilié plusieurs doctrinaires, tel que démontré supra, mais pour franchir cette polémique doctrinale, nous avons trouvé bon de se prosterner face à l'opinion du Professeur Sylvain SHOMBA, lorsqu'il dit que « l'hypothèse est une série de réponses qui permettent de prédire la vérité scientifique, vraisemblable au regard des questions soulevées par la problématique et dont la recherche vérifie le bien-fondé ou le mal fondé »[27].

Cela étant, face aux questions que nous nous sommes posées dans la problématique, nous formulons les hypothèses ci-après

***Primo** :*

Le principe de la légalité criminelle est pris en otage car, « 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 dansl'arsenal juridique pénal. Logiquement, ces crimes échapperaient à toute poursuite judiciaire parce qu'elles ne sont pas encore érigées en infractions. Cet 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 »[28].

Dans son mémoire de D.E.A./D.E.S en cybercriminalité, le Professeur MANASI N'KUSU KALEBA Raymond de Bouillon dit que « les recherches menées ont relevé que le concept NTIC nageait dans un flou sémantique exemplaire qui rendait pénible l'effort de sa définition. Au but de cet effet, il s'est avéré, que les nouvelles technologies de l'information et de la communication font partie des technologies de l'information et de la communication en sigle TIC, définies comme l'ensemble d'appareils nécessaires pour manipuler de l'information, et particulièrement des ordinateurs et programmes nécessaires pour la convertir, la stocker, la gérer, la transmettre et la retrouver »[29].

« Les technologies de l'information se caractérisent par les développements technologiques récents dans les domaines des télécommunications et du multimédia. Ainsi que par la convivialité accrue des produits et services qui en sont issus et qui sont destinés à un large public de non spécialistes »[30].

Le concept de nouvelles technologies de l'information et de la communication est apparu pour marquer l'évolution fulgurante qu'ont connu les techniques de l'information avec l'avènement des autoroutes de l'information (notamment l'utilisation de l'internet) et l'explosion du multimédia. C'est l'interpénétration de plus en plus grande de l'informatique, des télécommunications et de l'audiovisuel qui est à l'origine des changements rapides sur les plans techniques, conceptuel et terminologique.

Secundo :

« Le développement des nouvelles technologies de l'information et de la communication et la vulgarisation de l'internet ont provoqué des bouleversements majeurs. Ce développement a aussi des revers et parmi eux on note l'apparition d'une nouvelle menace : la cybercriminalité »[31]. Ainsi, toute invention humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. Il s'agit d'une nouvelle forme de criminalité et de délinquance qui est liée, facilité et spécifique aux technologies de l'information et de la communication.

Tertio :

La cybercriminalité est une notion large qui regroupe « toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau »[32]. Elle peut être définieautrement comme étant : « l'ensemble des infractions pénales commises via le réseau internet. Plus précisément, la cybercriminalité est constituée par des délinquants qui utilisent les systèmes et les réseaux informatiques soit pour commettre des infractions spécifiques à ces systèmes et réseau informatique, soit pour développer ou faciliter des infractions qui existaient avant l'arrivée de l'internet »[33].

Eu égard à tout ce qui précède, la cybercriminalité est composée stricto sensu des infractions pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit. Il s'agit ici de la nature des technologies utilisées d'une part, dont l'on retrouve les infractions liées à la télécommunication, infractions liées à la téléphonie cellulaire et les infractions informatiques.D'autre part, les infractions pour lesquelles l'internet est le moyen de commission ou la facilite. Il s'agit de la criminalité de droit commun, de nature juridiquetraditionnelle. L'on rencontre ici les infractions prévues par le Code pénal et les infractions prévues par des textes spécifiques.

Quarto :

En confrontant la cybercriminalité au droit pénal congolais, Le Professeur MANASI estime que : « autant affirmer d'entrée de jeu que cette confrontation a révélé une réalité triste »[34].En effet, « jusqu'ici, la législation pénale congolaise relative aux NTIC est composée d'une loi, en l'occurrence la loi-cadre n°13/2002 du 06 octobre 2002 sur les télécommunications et d'une ordonnance, l'ordonnance n°87/243 du 22 juillet 2987 portant règlementation de l'activité informatique au Zaïre»[35].

Dans sa thèse de doctorat, le Professeur MANASI précise que : « cette triste réalité est exacerbée par : l'inexistence en droit congolais de toutes les règles de coopération internationale contre le crime impulsée par la nécessité de réprimer la cybercriminalité, la non adoption des lois susceptibles de régir les technologies de l'information et de la communication et toutes leurs implications ; la non adhésion de la RDC à la convention sur la cybercriminalité ; l'inefficacité des sanctions en vigueur en droit pénal congolais pour les crimes qu'il punit et l'absence de la formation requise pour la lutte contre la cybercriminalité dans le chef des autorités judiciaires »[36].

De ce fait, « le droit pénal congolais révèle son inefficacité à réprimer la cybercriminalité »[37].

A notre humble avis, le code pénal congolais, sans le savoir pénalise quelques infractions informatiques facilitées par les nouvelles technologies de l'information et de la communication. Il s'agit entre autre du vol, de l'escroquerie, des injures publiques et diffamation ; et de ne citer que ceux-là.

Contrairement au système de répression congolais de la cybercriminalité, le droit français marque des avancées significatives. A en croire Jean PRADEL : « l'informatique est apparue comme un moyen de commettre des infractions, le législateur intervient une première fois par une loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. Quelques années après, la fraude informatique fut prise en considération par le législateur. Notamment par la loi du 5 janvier 1988 relative à la fraude informatique, appelée LOI GODFRAIN. Cette loi crée 6 incriminations qui s'intègrent au code pénal dans un chapitre III, intitulé *"De certaines infractions en matière informatique"* »[38].

De la sorte, « en droit français actuel, les incriminations relatives à l'informatique se composent de deux ensembles : l'un sur les atteintes à la vie personnelle et l'autre sur la fraude »[39].

De ce qui précède, la lutte contre la cybercriminalité est en pleine évolution et elle fait l'objet de nombreuses réflexions en France. Notamment, l'adoption par les pays membres du conseil de l'Europe, de la convention sur la cybercriminalité du 23 novembre 2001. Ainsi, en 2003, a été ouvert à la signature, le protocole additionnel à la convention sur la cybercriminalité.

Ceci étant dit, une pareille étude est le fruit d'une observation de longue haleine du fait de l'expansion de l'informatique, et cela nous oblige en tant que chercheur, de démontrer l'intérêt que nous portons au présent sujet.

D. Choix et intérêt du sujet

La fin de notre formation de juriste pointant à l'horizon, étant du droit privé, particulièrement passionné du droit privé et judiciaire, nous avons souhaité porter notre analyse sur l'étude comparative de la répression de la cybercriminalité en droits congolais et français, pour afin, trouver les solutions aux épineux problèmes qui se passent dans la société congolaise et française sur l'utilisation des nouvelles technologies de l'informatique et de la communication, et des menaces qui y sont liées.

Ainsi, l'importance que comporte notre sujet est formulée en double intérêts : théorique et pratique.

Sur le plan théorique, cette étude se veut une majeure documentation sur les nouvelles technologies de l'information et de la communication ainsi que des menaces qui les entourent appelées cybercriminalité.

Par ailleurs, à l'heure où prime l'informatique, bon nombre de personnes sont moins informées sur cette nouvelle forme de criminalité qui se commet au moyen électronique et virtuel. Cette étude va exposer clairement, la quintessence de la notion de la cybercriminalité et qui permettre aux assoiffés scientifiques et aux profanes, de s'imprégner de cette forme de crime qui angoisse l'humanité en général et la RDC en particulier. Bref, nous voulons que ceuxqui viendront après nous, trouvent une documentation fiable, nécessaire et utile qui les aidera à parachever leurs investigations, car nous ne voulons pas qu'ils commencent dans le vide, comme cela est pour nous à l'université de Mbandaka.

S’agissant de l’intérêt pratique, nous croyons par notre travail faire une étude comparative entre les droits congolais et français sur la répression de ce fléau moderne. Il s’agit, en fait, d’approcher les deux législations afin de dégager leurs insuffisances à réprimer les délits de NTIC. Concrètement, cette recherche aura pour but, de démontrer l’inefficacité du législateur congolais vis-à-vis de la criminalité informatique et de son homologue français ; et ensuitesoulever les avancées significatives constatéesen droit français dans la lutte contre cette nouvelle forme de criminalité.

Enfin, cette étude se promet de suggérer au législateur congolais d’adopter des mesures efficaces et efficients comme est le cas en droit français, dans le but de bien normaliser l’activité informatique, qui à l’heure actuelle, revêt un caractère international du fait de la mondialisation.

Une telle étude nécessite d’être délimitée pour que nous nous ne perdions pas dans un labyrinthe de pensée.

E. Objet et délimitation du sujet

Certes, « on ne peut prétendre étudier l’univers jusqu'à ses confins, dit le savant REZSOHAZI» [40].

En conséquence, la circonscription de notre thème de recherche dans un cadre limité serait aussi le vider de sa substance dans la mesure où les théories développées dans les lignes qui suivent tiennent de l’international et particulièrement du droit comparé.

La réponse à la question de savoir pourquoi délimiter le sujet, est donné par le Professeur Sylvain SHOMBA KINYAMBA, lorsqu’il soutient que : « conformément à la tradition de recherche universitaire en RDC, quand on aborde le débat sur les dimensions de la délimitation du sujet, on se limite à mettre en évidence les facteurs temps et espaces »[41].

Ainsi donc, dans le temps, nous allons nous limiter à analyser les dispositions législatives et règlementaires de la RDC et de celles de son homologue la France, relatives aux nouvelles technologies de l’information et de la communication, notamment la délinquance qui en est attachée.

Par ailleurs, nous ne considérons que la période allant de 1940 à ce jour, pour le territoire congolais, du fait que c’est à cette année-là qu’il y a eu l’adoption et la promulgation du décret du 30 janvier 1940 portant code pénal ; et la période allant de 1978 et 1994 successivement la date à laquelle la loi sur l’informatique, les fichiers et les libertés a été promulguée et la date à laquelle le nouveau code pénal français est entré en vigueur en mars 1994 pour remplacer le code pénal de 1810.

En outre, l’espace étant annoncé ci-haut, cette étude couvre deux territoires, en l’occurrence du territoire congolais et français. Toutefois, même si la cybercriminalité revêt à l’heure actuelle un caractère mondial, nous nous aborderons uniquement cette notion dans les deux pays, la coopération internationale et régionale y compris.

Par rapport à la matière, cette étude va aborder les notions du droit pénal général combinées avec celles du droit pénal spécial. Il s'agira de confronter la portée du principe de la légalité criminelle face à la cybercriminalité d'une part, et d'autre part, étudier le système de répression des infractions se rapportant à l'utilisation des NTIC.

Ainsi, pour mieux purifier notre démarche scientifique, il est impérieux de recourir à un ensemble des méthodes et techniques appropriées afin d'atteindre les objectifs que nous nous sommes assignés.

F. *Méthodes et techniques de recherche utilisées*

Il est évident de partager le même avis avec ceux qui pensent que tout travail scientifique doit répondre à un objet et obéir à une certaine méthodologie. En clair, est-il question d'énumérer ici les différentes méthodes que nous avons fait usage pour mener à bon port notre étude et les techniques auxquelles nous avons recourues pour mieux en saisir l'objet.

1. Méthodes de recherche utilisées

D'après MUKANA MUTANDA et TSHIPAMA, « une méthode est un ensemble de démarches rigoureuses, raisonnées que suit l'esprit afin de mieux observer scientifiquement par le canal de sens humains, la raison, la sagesse ou par l'instruction en vue de recouvrir la vérité vraie des apparences et prédire une loi universelle »[42].

Toutefois, il est mieux de comprendre que le concept "méthode" revêt plusieurs sens et n'a pas concilié les différents auteurs qui s'y sont penchés. Mais dans le cadre de ce travail, nous allons outrepasser cette polémique tout en demeurant fidèle à M. GRAWITZ qui la définit comme étant : « un ensemble des opérations par lesquelles une discipline cherche à atteindre les vérités qu'elle poursuit, les démontrer, les vérifier ; elle dicte surtout de façon concrète d'envisager la recherche, mais ceci de façon plus au moins impératives, plus au moins précise, complète et systématisée »[43].

C'est suite à cette définition, et pour bien effectuer nos recherches et arriver à savoir les notions entourant notre sujet, nous avons utilisé les méthodes exégétique, sociologie et comparative.

1.1. La méthode juridique ou exégétique

La méthode juridique consiste « à rechercher les textes juridiques et les confronter avec les faits et le droit »[44].

C'est une méthode qui consiste « à analyser et à exposer les textes de loi et divers documents relatifs à la matière traitée en recherchant sans cesse le droit applicable au cas d'espèce »[45].

Effet, dans le cadre de cette étude, cette méthode juridique amènera à analyser les différents textes juridiques qui ont organisé le secteur de la cybercriminalité en particulier et du droit pénalen général jusqu'à ce jour. Il s'agit des instruments juridiques tant nationaux qu'internationaux, à l'interprétation des textes officiels organisant et protégeant l'usage des nouvelles technologies de l'information et de la communication en RDC et en France.

1.2. La méthode comparative

La méthode comparative est définie par REUCHELIN comme : « une démarche cognitive par laquelle on s'efforce à comprendre un phénomène par la confrontation des situations différentes » [46].

A en croire Madeleine GRAWITZ, la méthode comparative est « l'opération par laquelle on relie plusieurs objets dans un même acte de penser pour en dégager les ressemblances et les différences »[47].

Cette méthode nous a permis de comparer la législation congolaise et française quant à leur système de répression de la cybercriminalité. Elle nous a aidé d'identifier les similitudes et les différences qui existent par rapport à la règlementation des nouvelles technologies de l'information et de la communication et de la délinquance qui en découle.

1.3. La méthode sociologique

Cette méthode « consiste à fait appel à l'observation pure et simple. Elle est tributaire des faits et se propose moins de les apprécier que de les expliquer »[48].

Cela étant, elle nous a permis de confronter les textes juridiques et les faits sociaux, c'est-à-dire faits actuels en rapport avec a cybercriminalité en vue d'avoir la compréhension effective de notre sujet de recherche.

2. Techniques de recherche utilisées

Selon MULUMA MANANGA, la technique est entendue comme étant : « un ensemble des moyens et procéder qui permettent de rassembler les informations originales sur un sujet donné » [49].

Quant à Madeleine GRAWITZ, « la technique est l'ensemble des procédés opératoires rigoureux bien définis, transmissibles et susceptibles d'être appliqués à nouveau dans les mêmes conditions, adaptés au genre des problèmes et des phénomènes sous l'étude »[50].

Pour atteindre nos objectifs dans cette étude, nous nous sommes servis de la technique documentaire. Elle nous a permis d'interroger les différentes doctrines et documents pouvant nous éclairer sur les questions de droit nous concernant, notamment, par la lecture quotidienne des ouvrages, revues, travaux scientifiques, diverses publications officiels et surtout l'internet en rapport avec notre sujet de recherche.

G. Plan sommaire

Le thème de cette recherche étant relatif à *" l'étude comparative de la répression de la cybercriminalité en droits congolais et français",*

il nous a paru judicieux de prévoir, hormis la présente introduction générale, deux parties ayant chacune deux ou trois sections.Ensuite, suivront quelques perspectives d'avenir ainsi qu'une conclusion générale qui viendra clore notre réflexion. Ainsi donc, l'ossature de la présente étude se présente de la manière suivante :

Première partie : Le principe de la légalité criminelle face à la cybercriminalité

Titre premier : Le principe de la légalité des incriminations et de peines ; et l'application de la loi pénale

Titre deuxième : considération générale sur l'infraction

Deuxième partie : Les technologies de l'information et de la communication ainsi que leur usage

Titre premier : Description des technologies de l'information et de la communication

Titre deuxième : Les infractions des nouvelles technologies de l'information et de la communication : la cybercriminalité

Titre troisième : Considération comparative de la répression de la cybercriminalité en droits congolais et français.

PREMIERE PARTIE : LE PRINCIPE DE LA LEGALITE CRIMINELLE FACE A LA CYBERCRIMINALITE

Depuis la révolution française, certains pays vivent dans une société d'Etat de droit au sein de laquelle organes administratifs et organes judiciaires sont tenus de respecter des textes posés par la constitution et par la loi. Cela implique qu'un juge ne peut rendre la justice, c'est-à-dire juger et condamner une personne, si la personne en question n'a pas commis une infraction qui ne soit prévue et référenciée par un texte. La cybercriminalité, doit être prévue et punie conformément à la loi.(Je pense qu'il faille commenter ici en insistant sur le principe de la légalité des peines : un principe général de droit)

Cette première partie, qui aborde les notions du droit pénal général applicable en matière de cybercriminalité, comprend deux principaux titres, traitant respectivement du principe de la légalité des incriminations et de peines ; et l'application de la loi pénale (titre 1) et des considérations générales sur l'infraction (titre 2).

TITRE PREMIER : PRINCIPE DE LE LEGALITE DES INCRIMINATIONS ET DE PEINES ET L'APPLICATION DE LA LOI PENALE

Dans ce titre, il va falloiraborder les composantes de la légalité pénale (chapitre 1), avant d'attaquer l'application de la loi pénale dans le temps et dans l'espace (chapitre 2).

CHAPITRE PREMIER : COMPOSANTES DE LA LEGALITE PENALE

Dans le présent chapitre, il sera question d'étudier minutieusement le principe de la légalité ainsi que sa justification (section 1ère) et ensuite s'articuler sur son contenu (section 2).

SECTION 1ère : ETUDE DU PRINCIPE DE LA LEGALITE PENALE ET SON CONTENU

§1. Enoncé du principe

Dans le droit moderne, il n'y a pas d'infraction ni des peines sans un texte légal : "*nullumcrimen, nullapoena sine lege".* C'est le fameux principe de la légalité criminelle.

En effet, « ce principe a été énoncé pour la première fois par le législateur révolutionnaire, dans la déclaration des droits de l'homme et du citoyen de 1789. L'article 5 dispose que tout ce qui n'est pas défendu par la loi ne peut être empêché et nul ne peut être contrait de faire ce qu'elle n'ordonne pas et l'article 8 prévoit que nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliqué »[51].

Pour histoire, « ce principe a été développé par le pénaliste italien Cesare BECCARIA aux 18ème siècle. Il s'est imposé comme une règle fondamentale à tous les criminalistes du 19ème siècle et les législations de tous les pays l'ont à leur tour consacré »[52].

Selon le Professeur NYABIRUNGU mwene SONGA, « le principe de la légalité criminelle est sans doute le principe le plus important du droit pénal : seuls peuvent faire l'objet d'une condamnation pénale les faits déjà définis et sanctionnés par le législateur au moment où l'accusé a commis son acte, et seuls peuvent leur être appliquées les peines édictées à ce moment déjà par le législateur »[53].Ce principe est compris comme une garantie contre l'arbitraire du pouvoir judiciaire. Il interdit bien sûr au juge d'inventer une infraction ou d'en étendre le champ d'application. Le principe de la légalité s'est répandu et fait l'objet d'une certaine reconnaissance au niveau international.

En France, « ce principe avait été consacré par le code pénal de 1810, dont l'article 4 disposait : nulle contravention, nul délit, nul crime, ne peuvent être punis des peines qui n'étaient pas prononcées par la loi avant qu'ils fussent commis »[54]. En outre, toujours en France « le nouveau code pénal réaffirme son attachement à la légalité dans l'article 111-3, qui veut que : nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi ou pour une contreventions dont les éléments ne sont pas définis par le règlement »[55].

Ce principe de la légalité pénale est prévu en République Démocratique du Congo par trois textes. Il s'agit de l'article 1èrde décret du 30 janvier 1940 portant code pénal tel que modifié et complété à ce jour et qui prévoit que : « nulle infraction ne peut être punie des peines qui n'étaient pas portées par la loi avant que l'infraction fut commise »[56].

L'article 17 alinéa 3 de la Constitution du 18 février 2006 telle que révisée à ce jour dispose que : « nul ne peut être poursuivi pour une action ou une omission qui ne constitue pas une infraction au moment où elle est commise et au moment des poursuites »[57]. L'alinéa 4ème du même article prévoit que : « nul ne peut être condamné pour une action ou une omission ne constitue pas une infraction à la fois au moment où elle commise et au moment de la condamnation »[58].

Enfin, l'article 11 de la Déclaration universelle de droits de l'homme du 10 décembre 1948 dispose que : « nul ne sera condamné pour des actions ou omissions qui au moment où elles ont été commises ne constituent pas un acte délictueux d'après le droit national et international. De même, il ne sera pas infligé aucune peine plus forte que celle qui était applicable au moment où l'acte délictueux a été commis »[59].

A en croire le Professeur Bienvenu WANE BAMEMEle principe de la légalité des peines« signifie que les règles du droit pénal sont exprimées dans la loi : seuls peuvent faire l'objet d'une

condamnation pénale les faits déjà définis et sanctionnés pat le législateur au moment où l'accusé a commis son acte, et seuls peuvent leur être appliquées les peines édictées à ce moment déjà par le législateur »[60].

Le criminaliste FEUERBACH, cité par le Professeur WANE a résumé au 19ème siècle ce principe par la forme « *"nullumcrimen, nullapoena sine lege"*, c'est-à-dire nul crime, nulle peine sans loi » [61].

MERLE et VITU cités par le même doctrinaire considèrent que : « quoique savante, cette formule est néanmoins incomplète parce qu'elle ne vise que le droit pénal de fond (qui gère les crimes et les peines) ; alors que le principe de la légalité s'applique également à la procédure, au droit pénal de forme. Pour ce faire, ces deux auteurs complètent la formule : *" nullumcrimen, nullapoena, nullumjudicium sine lege"* »[62].

§2. Justification du principe

La justification du principe de la légalité des délits et des peines ne peut être mieux appréhendée que si l'on expose son fondement (2.1) ainsi que les conséquences de ce principe par rapport au juge et ses limites (2.2).

2.1. Le fondement du principe de la légalité

Le principe légaliste, jugé par certains insuffisant et même dangereux pour la défense de la société puisqu'il ne permet pas de punir les actes contraires à l'ordre social qui ne rentrent pas dans le champ précis des prévisions légales non plus que les actes ou les états menaçant la sécurité, tant qu'une infraction n'a pas été commise, se justifie du point de vue juridique par des considérations d'intérêt public que privé. En effet, « la première considération, propre au droit pénal stricto sensu est tirée d'une nécessité de la POLITIQUE CRIMINELLE »[63]. Il s'agit ici que « la loi avertisse avant de frapper, de manière que le citoyen sache avant d'agir, ce qui est permis et ce qui est interdit ; par sa préexistence la loi pénale exerce sur la volonté humaine une contrainte psychologique qui contrebalance les tendances délictuelles possibles de l'individu, sous ce rapport, la loi pénale remplie une fonction intimidant et en une certaine mesure un rôle éducatif »[64].

Le Professeur NYABIRUNGU renchérit en disant que : « la loi pénale exerce aussi une certaine influence sur la psychologie de l'agent qu'elle informe du danger encouru par la commission de l'infraction. Elle joue un rôle éducatif et préventif. Ce rôle sera d'autant mieux assuré que la loi aura été claire, précise et sans ambiguïté »[65].

La deuxième considération, qui est celle de la LIMITATION DU DROIT DE PUNIR, est d'ordre purement politique. Ainsi, « la société ne peut punir sans borne et sans mesure. Ce pouvoir de la société de maintenir l'ordre doit être contenu dans certaines limites qui garantissent et respectent la liberté, la sécurité et l'indépendance individuelle »[66]. De ce fait, « les hommes vivent en société et celle-ci est une réalité indispensable, mais il importe que la collectivité n'abuse pas les prérogatives qu'elle possède sur les êtres qui la composent : son pouvoir doit être contenu dans certaines limites, qui garantissent la liberté et l'indépendance de chacun »[67].

La troisième considération est que « le principe de la légalité est le rempart contre l'arbitraire du pouvoir »[68]. Il constitue par ailleurs, « l'une des garanties essentielles de la liberté individuelle, le citoyen est protégé contre l'arbitraire du juge, car il peut connaitre à l'avance ce qui est défendu et à la peine à laquelle il s'expose en ce faisant »[69]. Le principe de la légalité criminelle a aussi une valeur constitutionnelle. Ce principe s'impose au législateur lui-même ; en conséquence celui-ci

saurait violer la légalité par exemple en promulguant des lois expressément rétroactives ou ne laissant aux tribunaux d'organiser la procédure. Ce principe s'impose non seulement au juge ou à l'administration mais aussi au législateur lui-même.

Par ailleurs, « la justification du principe est un élément important car elle résume les idées créatrices de ce principe et explique ses fondements. Elle met en détail de manière précise les attentes par rapport à cette règle »[70].

2.2. Conséquences du principe de la légalité pour le juge et ses milites

Il s'agit de la qualification des faits (A) et de l'interprétation de la loi pénale par le juge (B).

A. La qualification des faits

D'après le Professeur Pierre AKELE ADAU, «la qualification est une question primordiale en droit pénale spécial à cause du principe de la légalité des délits et des peines. Le juge doit tenir compte des incriminations et des sanctions prévues par la loi »[71]. Pour cela, « il doit respecter certaines règles pour qualifier les faits. C'est ainsi qu'il doit rechercher la qualification exacte des faits poursuivis. Autrement dit, il doit confronter les faits avec le texte qui incrimine pour vérifier et établir que les éléments constitutifs de l'infraction se trouvent bien réunis dans le cas d'espèce » [72].

Donc, « les juges, avant de prononcer une peine, doivent dans leur décision de condamnation constater l'existence d'un texte répressif antérieur aux faits poursuivis et vérifier que sont réunis les éléments constitutifs exigés par la loi pour que le fait soit punissable. Il importerait peu qu'aux yeux du juge, le comportement de l'individu poursuivi apparaisse immoral ou socialement dangereux, en dehors de toute infraction caractérisée, le juge ne peut prononcer aucune sanction pénale »[73].

Ainsi, il est aussi interdit de donner aux textes de lois une portée rétroactive (sauf, dans l'hypothèse de la rétroactivité in mitius), d'appliquer des peines non prévues par la loi, ou de prononcer une peine supérieure au maximum ou inférieure au minimum fixés par la loi, ou de faire application des peines portés non par une loi, mais par un acte du pouvoir exécutif et hors le cas d'une délégation législative régulière.

B. L'interprétation de la loi pénale par le juge

« L'opération de qualification qui permet de cristalliser le texte incriminateur correspondant à l'entreprise criminelle donnée ne constitue qu'une phase de l'œuvre du juge répressif car il doit encore donner à ce texte applicable sa portée réelle, c'est-à-dire dégager son vrai sens, son sens exact en vue d'en assurer une application correcte. Tel est l'objet de l'interprétation »[74]. En effet, « l'interprétation des lois par le juge, ou à la recherche de leur vrai sens constitue une nécessité. Le magistrat est tenu de statuer sur chaque cas qui lui est présenté »[75].

En conséquence, « la loi pénale est d'interprétation stricte. Elle n'autorise pas le juge à créer des infractions ou des sanctions, ni à prononcer des peines supérieures ou maximum prévues par les textes »[76].

SECTION 2ème : CONTENU DE LA LEGALITE CRIMINELLE

Cette section oppose la légalité des infractions (§1) à la légalité des sanctions (§2), et formule le

recul que connait ce principe (§3).

§1. La légalité des incriminations

Les incriminations représentantles actes qui troublent l'ordre public, sont en vertu du principe de la légalité définies préalablement par le pouvoir législatif.

A vrai dire, « les incriminations sont établies par la loi, seuls tombent sous le coup de la loi, les faits qui, au moment où ils sont commis, sont déjà comme constituant une infraction par le législateur. Ce principe de l'antériorité obligatoire des définitions des infractions est une garantie de la liberté et de la sécurité juridiques, car on peut valablement supposer que, dans ce cas, ces définitions ont été élaborées sous parti pris, dans l'ignorance des personnes qui tomberont éventuellement sous leur application »[77].

§2. La légalité des peines

Au niveau du législateur, « seul ce dernier peut déterminer la nature et le taux de la peine, c'est-à-dire seules peuvent être appliquées des peines et des mesures édictées par le législateur au moment où l'accusé a commis son acte »[78]. Autrement dit, « le principe légaliste impose au législateur l'obligation de fixer les sanctions de manière précise dans le texte même des incriminations, c'est-à-dire, à chaque infraction doit être rattachée une sanction précise »[79].

A contrario, au niveau du juge :

- « il ne peut prononcer des peines si le texte n'en prévoit pas ;
- il ne peut prononcer une peine supérieure au maximum ni inférieure au minimum »[80] ;
- « il ne peut refuser de prononcer la peine prévue par la loi, sauf s'il y a cause d'exonération » [81].

§3. Le recul du principe de la légalité

« Le recul du principe de la légalité des délits et des peines s'est manifesté sur plusieurs aspects, notamment à l'égard du juge où ce déclin s'observe avec l'attribution du juge le pouvoir d'individualiser la peine et par le biais des sentences indéterminées »[82]. D'abord, « en mettant l'accent sur l'individualisation de la sanction par le biais des notions de soins, de rééducation, de resocialisation, les idées nouvelles ont contribué au recul du principe de la légalité criminelle. Le juge ayant obtenu du législateur le pouvoir de fixer la peine en dessous du minimum légal, grâce au jeu des circonstances atténuantes, il est paru souhaitable de libérer de l'obligation de respecter le maximum légal »[83].

Par ailleurs, « c'est surtout le mécanisme des sentences indéterminées qui porte gravement atteinte au principe de la légalité. Il existe deux types d'indétermination de la sentence : quand la décision judiciaire ne précise pas à l'avance la durée de la peine prononcée, l'indétermination dela sentence est dite absolue ; elle est seulement relative lorsque le juge fixe un maximum et un minimum entre lesquels la peine varie selon l'appréciation portée concrètement par les organes pénitentiaires d'exécution sur l'amendement du condamné »[84].

CHAPITRE DEUXIEME : DE L'APPLICATION DE LA LOI PENALE

Le problème de l'application de la loi pénale va se poser dès lors qu'un acte délictueux va se commettre. En effet, le premier souci va être de vérifier si les faits reprochés à la personne correspondent bien à une infraction prévue par un texte de la loi pénale. Toutefois, il faut aussi que les faits soient réprimés par un texte de qualification. Dans ce chapitre, il va falloir traiter d'abord du champ d'application de la loi pénale dans le temps (section 1) avant d'atterrir sur l'application de la loi pénale dans l'espace (section 2).

SECTION 1ère : LE CHAMPS D'APPLICATION DE LA LOI PENALE DANS LE TEMPS

D'après G. STEFANI et alii, « la nécessité d'un élément légal pour l'existence d'une infraction entraîne comme conséquence : l'impossibilité d'appliquer une loi pénale des faits antérieures à sa promulgation ou à sa date d'entrée en vigueur fixée par la loi promulguée. C'est la question de l'application de la loi pénale dans le temps »[85].

Ainsi donc, l'on distingue l'application de la loi pénalede fond (§1) de l'application de la loi pénale de forme (§2).

§1. L'application dans le temps des lois pénales de fond

Une loi pénale de fond, à en croire le Professeur Bienvenu WANE, « est celle qui définit les infractions et détermine les sanctions »[86].

1.1. La non-rétroactivité des lois pénales de fond

Sans doute, le principe de la non-rétroactivité n'est-il pas particulier au droit pénal ; il existe aussi en droit civil. Le juge répressif doit donc soumettre à la loi nouvelle les faits antérieurs à sa promulgation, dès lors que cette loi a été déclarée rétroactive par le législateur. En effet, « pour les lois de fond, c'est-à-dire celles qui déterminent les actes qui tombent sous le coup de la loi pénale et qui fixent les conditions dans lesquelles les actes peuvent être punis des peines qu'elles édictent, la non-rétroactivité est vraiment la règle (A), et la rétroactivité l'exception (B) »[87].

A. La non-rétroactivité est la règle

« Lorsque deux lois pénales de fond sont en conflit, le principe de solution est celui de la non-rétroactivité de la loi pénale de fond. Cette loi ne rétroagit pas ; elle dispose pour l'avenir, c'est-à-dire, elle ne régit que l'avenir et non le passé »[88].

De cette évidence, « une loi pénale qui crée une incrimination nouvelle, ou qui élève la peine applicable à une infraction antérieurement définie ne s'applique pas aux faits accomplis avant son entrée en vigueur »[89].

B. La rétroactivité est l'exception

Le deuxième principe est considéré par la doctrine comme une exception au principe de la non-rétroactivité. Il s'agit donc, « la loi pénale nouvelle rétroagit si elle est plus douce »[90]. En effet, « lorsque un texte présente des dispositions de fond plus douces, la situation diffère et peut s'appliquer immédiatement. C'est ce que l'on appelle la rétroactivité *in mitius* »[91].

Ceci étant dit, lorsque le législateur déclare lui-même une loi rétroactive, le juge répressif est tenu de l'appliquer même à des faits antérieurement à la promulgation de cette loi, dans les conditions fixées par cette dernière. C'est le cas de l'article 112-1 alinéa 3 du nouveau code pénal français, qui dispose que : « toutefois, les dispositions nouvelles s'appliquent aux infractions commises avant leur entrée en vigueur et n'ayant pas donné lieu à une condamnation passée en force de chose jugée lorsqu'elles sont moins sévères que les dispositions anciennes »[92].

La rétroactivité *in mitius*, des lois plus douces se justifie finalement au point de vue de l'intérêt de la société. Dès lors, la disposition ancienne estimée trop rigoureuse a été modifiée, la société n'a plus d'intérêt à l'appliquer. Sur le plan individuel du délinquant reconnu coupable d'une infraction qui était punie d'une peine déterminée au moment où il l'a commise, ne sera plus puni de cette peine, mais de celle prévue par la loi nouvelle en vigueur au moment où il sera jugé, si elle est moins rigoureuse. Il serait contraire à bon sens de lui appliquer, au nom du principe de la non-rétroactivité des lois qui ont été édictées pour le protéger, la loi plus sévère, pour la seule raison qu'elle était en vigueur au jour de la commission de l'infraction.

En somme, il va falloir pour cela opérer une comparaison en se plaçant soit sur le plan de l'incrimination, soit sur le plan de la répression, car il se pose une question de savoir comment apprécier le caractère plus doux ou plus sévère d'un texte ?

B.1. Sur le plan de l'incrimination

Selon le Professeur NYABIRUNGU, « une loi est plus sévère si elle soumet le fait poursuivi à une répression plus rigoureuse. Il en sera ainsi si une loi crée une nouvelle incrimination, si elle supprime une cause de justification, si elle institue une circonstance aggravante, ou encore si elle réduit le nombre des éléments constitutifs d'une infraction »[93].

Par ailleurs, « une loi est plus douce si elle abroge l'infraction, crée une cause de justification, supprime une circonstance aggravante ou augmente le nombre des éléments constitutifs de l'infraction »[94]. Il faut rappeler ici que, « un nouveau texte intervenant en supprimant l'incrimination existante est considérée comme adoucissant le texte initial. Il en est de même lorsqu'une loi supprime une circonstance aggravante »[95].

B.2. Sur le plan pénalité

D'après le Professeur WANE, « en comparant les légalistes, l'autorité chargée de l'application de la loi tiendra compte de la hiérarchie des peines prévues à l'article 5 du code pénal. D'après cet article, la peine de mort est la peine la plus grave, le châtiment suprême. Après cette peine, viennent les travaux forcés ; la servitude pénale (d'abord à perpétuité, ensuite à temps) même la plus faible l'emporte sur la peine d'amende, quel que soit son montant »[96].

François DURIEUX, quant à lui estime que : « quand la loi supprime une peine, elle est plusdouce. De même qu'une loi qui allège les sanctions antérieurement encourues pour une infraction.Il en est de même lorsqu'un nouveau texte supprime la peine principale initialement appliquée »[97].

De même, dans un texte peuvent coexister des dispositions plus douces et des dispositions plus sévères que la loi ancienne. Par exemple, une loi nouvelle peut tout à fait réduire le champ d'une incrimination tout en augmentant la sanction, la peine. En tel cas, que va donc devoir être la marche à suivre par le juge ? La réponse est donnée par François DURIEUX qui préconise que : « le juge va alors devoir examiner si le texte est divisible ou fait rétroagir uniquement la partie favorable au prévenu. Dans le cas où le texte n'est pas divisible, le juge doit se référer à la disposition principale de la nouvelle loi »[98].

Somme toute, « si cette disposition principale est considérée dans son ensemble comme plus douce, le juge fera rétroagir ce texte nouveau, y compris dans ses dispositions les plus dures. A contrario, si la disposition principale est plus sévère, même comportant les dispositions beaucoup plus douces, le juge ne fera pas rétroagir le nouveau texte »[99].

§2. L'application dans le temps des lois pénales de forme

« Les lois pénales de forme sont celles qui définissent le déroulement de la procédure, avec la compétence des juridictions, les voies de recours, les délais, la prescription, … »[100]. En d'autres mots, les lois pénales de forme sont celles qui organisent la compétence, la procédure, l'organisation judiciaire, l'exécution des peines et la prescription.

Ainsi, « à la différence des lois de fond dont la rétroactivité n'est qu'exceptionnelle, les lois qui ne modifient ni les caractéristiques de l'infraction, ni la responsabilité de l'auteur, ni la fixation de la peine, mais qui sont relatives à la constatation et à la poursuite des infractions, à la compétence et à la procédure, sont considérées comme les lois de forme et à ce titre s'appliquent immédiatement, même au jugement de faits commis avant leur promulgation »[101].

2.1. Principe de l'application immédiate des lois de procédure

Dès lors, une loi nouvelle qui modifie les règles de compétence, de procédure ou de prescription, pourra-t-elle s'appliquer immédiatement à des faitsaccomplis sous une loi ancienne ? Pour les lois pénales de forme, il y a application immédiate de la nouvelle loi, celle-ci « conduit à ce que jusqu'à sa promulgation, les instances sont régies par la loi ancienne, et aucun effet de celle-ci n'est mis en cause. Mais dès sa promulgation, la loi nouvelle s'applique aux instances en cours et à toutes celles qui naîtront par la suite »[102]. Par ailleurs, « l'application immédiate ne veut pas dire rétroactivité parce que la nouvelle loi qui entre en vigueur n'annule pas ce qui a été élaborée avant sa mise en vigueur »[103].

Ainsi tel est le sens de l'effet immédiat de la loi nouvelle. Faite pour une meilleurs administration de la justice et dans l'intérêt de la collectivité et de l'individu, la loi nouvelle ne peut ni attendre, ni rétroagir, à moins que le législateur, de manière expresse, n'en décide autrement. La loi nouvelle reçoit application immédiate en ce qui concerne l'exécution des peines et des mesures de sûreté » [104].

2.2. Exceptions ou quelques aménagements

Tout comme les lois pénales de fond, le principe d'application immédiate des lois pénales de forme souffre de quelques aménagements, ceux-ci vont dans le sens de la cohérence de la

procédure et du traitement légalement le plus juste pour le délinquant. Il s'agit ici de la question de la compétence (A), des voies de recours (B), de la prescription (C), de la preuve (D) et des poursuites (E).

A. Lois de compétence

Le Professeur NYABIRUNGU admet que : « en ce qui concerne les lois de compétence, la loi nouvelle ne peut recevoir application immédiate, lorsque l'affaire a déjà fait l'objet d'un jugement sur le fond en premier ressort »[105]. En d'autres termes, si un jugement au fond a déjà été rendu lors de la survenance de la loi nouvelle, la procédure ultérieure obéit à la loi antérieure, ce dans un but de cohérence de l'ensemble de l'affaire.

En outre, « lorsqu'une lois nouvelle intervient pour modifier une compétence d'une juridiction d'appel alors que l'affaire a déjà été jugée au premier degré sur le fond, cette loi nouvelle de compétence ne peut s'appliquer »[106].

B. Les voies de recours

En ce qui concerne la loi sur les voies de recours, signalons que « les recours obéissent aux lois en vigueur au jour où ils sont formés. Une loi postérieure modifie leur forme n'aura aucun effet sur les recours déjà formés. L'application immédiate se restreint ici aux recours entamés postérieurement à la promulgation de la loi »[107]. Certes, une loi nouvelle qui supprime une voie de recours ne peut pas s'appliquer immédiatement, car elle remet en cause les droits acquis des parties au procès.

C. Lois sur les prescriptions

En considérant la prescription comme relevant du fond ou de la forme, l'on pense qu'il faut appliquer la loi nouvelle si elle est favorable au prévenu, ou alors qu'il peut immédiatement appliquer la loi nouvelle qu'elle soit favorable ou non.

En effet, nous partageons le même avis avec G.MINEUR lorsqu'il dit que « en cas du changement de la durée de la prescription, le texte le plus favorable au prévenu doit être appliqué »[108]. Ainsi, « le texte sera considéré comme favorable lorsqu'il réduit la durée de la prescription »[109]

D. Lois sur les modes de preuve

En ce qui concerne les lois relatives aux modes de preuve, il y a toujours une controverse doctrinale, du fait que certains pensent que les lois ayant trait aux modes de preuve ne sont pas de forme mais plutôt de fond et par conséquent, il serait mieux d'appliquer la loi nouvelle si elle est favorable au prévenu. En effet, pour les uns, notamment LEVASSEUR et S.BOUZAT pensent qu'une loi « sera favorable si elle prévoit un mode de preuve plus facile pour le prévenu ou si elle est plus exigeant à l'égard du Ministère public »[110].

D'autres, par contre estime que : « le droit de la preuve est régit par la loi en vigueur au moment où la preuve doit être établie. Ce qui consacre l'application immédiate de la loi nouvelle. D'où, les lois relatives à la preuve sont considérées comme de forme »[111].

Abondant dans le même ordre d'idée, le Professeur Bienvenu WANE BAMEME estime quant à lui que : « en ce qui concerne les lois relatives aux modes de preuve, la solution consacrée aux lois de prescription s'applique également aux lois relatives aux modes de preuve »[112].

E. Lois sur les poursuites

Les lois sur les poursuites s'orientent vers la mise en mouvement ou l'exercice des poursuites. En conséquence, « elles sont assimilées aux lois de fond et la loi nouvelle en la matière suit les règles déjà étudiées, à savoir : principe de non rétroactivité et application de la loi nouvelle plus douce »[113].

SECTION 2ème : L'APPLICATION DE LA LOI PENALE DANS L'ESPACE

Le grand problème qui se pose dans cette section, est la question de savoir, quelle loi doit-on appliquer lorsque l'auteur d'une infraction est appréhendé au moment des poursuites dans un pays autre que celui dans lequel l'infraction est commise ? Ou encore quelle attitude doit avoir le juge lorsqu'une infraction a été perpétrée dans plusieurs pays différents et successivement ? Ou encore quelle loi applicable lorsque l'infraction commise dans un autre territoire porte atteinte aux intérêts vitaux de l'Etat ?

La réponse à ces trois questions, fait l'objet de la présente section. C'est ainsi qu'en premier lieu nous allons aborder les systèmes doctrinaux (§1), avant de s'attarder sur les systèmes applicables en droits positifs congolais et français (§2), et enfin, exposer quelques mécanismes de coopération internationale contre le crime (§3).

§1. Les systèmes doctrinaux

Pour la doctrine, l'application d'une norme pénale peut se concevoir en trois systèmes. Appelés aussi principes, dont nous parlerons tour à tour de la territorialité de la loi pénale (1.1), de la personnalité (1.2), et enfin, l'universalité de la loi pénale (1.3).

1.1. La territorialité de la loi pénale

A. Définition

La territorialité de la loi pénale, « est un principe qui veut que la loi pénale d'un pays déterminé s'applique et de ce fait, les juridictions de ce pays soient compétentes à toutes les infractions commise sur tout le territoire de ce pays quelle que soit la nationalité de l'auteur et celle de la victime »[114]. C'est-à-dire, la loi pénale applicable sera celle du lieu de commission de l'infraction, peu importe la nationalité de l'auteur des faits *« lex locus delicticommissi* »[115].

Il sied de préciser que « l'infraction est considérée comme ayant été commise sur le territoire de l'Etat quand un acte d'exécution a été tenté ou accompli sur ce territoire ou quand le résultat de l'infraction s'est produit sur ce territoire »[116].

Donc, « il peut s'agir des actes préparatoires, des conditions préalables à l'existence d'une infraction, mais aussi des effets produits par l'infraction ainsi que des éléments strictement constitutifs. La compétence sera établie dès lors que l'un de ces faits constitutifs ne sera produit sur le territoire de la République »[117].

B. Avantages de ce système

L'avantage du principe de la territorialité est de quatre ordres, à savoir : « l'intérêt social, une meilleure justice, le respect du principe de la légalité, l'exercice de sa souveraineté par l'Etat de la

commission de l'infraction »[118].

C. Inconvénients de ce système

Ce système appliqué de manière rigoureuse peut conduire à la paralysie de la justice et dont l'impunité de certains délinquants. Raison pour laquelle François DURIEUX préconise que : « l'inconvénient de ce système est de faire du territoire de chaque Etat un refuge pour tous les ressortissants nationaux ayant pu commettre des actes pénalement sanctionnables à l'étranger »[119].

1.2. La personnalité de la loi pénale

A. Définition

Le système de la personnalité de la loi pénale « signifie que la loi pénale n'est plus liée à un territoire mais s'attache aux personnes et les suit en tous lieux où elles se rendent. La loi pénale applicable sera donc celle de l'Etat national duquel ressort un auteur d'infraction ou bien une victime »[120].

A en croire Bienvenu WANE BAMEME, « c'est un principe qui veut que la loi d'un Etat déterminé s'applique à toutes les infractions commises per ses nationaux soit à l'intérieur soit à l'extérieur du territoire. Le délinquant est jugé d'après sa loi d'origine et relève des tribunaux de son pays »[121]. Ainsi, « le système se dédouble selon que les personnes sont des délinquants ou des victimes : on parle alors de personnalité active, et de personnalité passive »[122], et aussi « du principe de la réalité de la loi pénale »[123].

B. La personnalité active

Ce principe veut que « la loi d'un Etat s'applique à toutes les infractions commises par ses nationaux soit à l'intérieur soit à l'extérieur du territoire. Le délinquant est jugé d'après sa loi d'origine et relève des tribunaux de son pays. Il se fonde sur l'idée que la loi nationale est mieux adaptée à la personne du délinquant et que le juge national sera plus juste qu'un juge étranger » [124].

C. La personnalité passive

A l'inverse de la personnalité active, s'il s'agit de la personnalité de la victime, on parle de la personnalité passive. Selon ce principe, la loi pénale suit les ressortissants de l'Etat où elle est en vigueur et s'applique à toutes les infractions dont ils sont victimes, où qu'ils se trouvent. La loi pénale d'un Etat s'applique à toutes les infractions qui victimisent ses nationaux. Il se justifie par l'idée que la loi pénale de la victime est la plus à même d'assurer sa protection.

D. *La réalité de la loi pénale*

Une particularité, cependant, s'il s'avère que la victime soit l'Etat, on parle du principe de la réalité. Ce système ne peut jouer que pour des infractions relativement limitées, donc il entend sur le plan de fond, assurer la protection des intérêts essentiels de l'Etat.

1.3. L'universalité de la loi pénale

En vertu de ce système « c'est le tribunal du lieu d'arrestation du délinquant qui est compétent

pour connaître l'infraction »[125]. C'est un système de la compétence universelle de la loi pénale. Il s'agit de la compétence juridictionnelle et non législative.

§2. Systèmes applicables en droits congolais et français

2.1. En droit français

La particularité du droit interne français est qu'il combine tous les systèmes avec cependant une préférence pour la territorialité.

A. Les infractions commises ou réputées commises sur le territoire de la République

La justification essentielle du principe tient dans la souveraineté de l'Etat dont il est la manifestation. Ainsi, la référence au principe de territorialité est clairement affirmée par l'article 113-2 du nouveau code pénal français et qui dispose que : « la loi pénale française est applicable aux infractions commises sur le territoire de la République »[126]. Toutefois, « l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire »[127].

Par ailleurs, il est question de déterminer lequel de territoire dont on fait allusion. Il s'agit bel et bien de l'espace terrestre, maritime et aérien. Il convient de préciser que : « ce principe de territorialité a été étendu aux navires et aux aéronefs français ainsi qu'aux actes de complicités » [128]. En conséquence, les articles 113-3 à 113-5 du code pénal français précisent que lorsqu'une infraction est commise à bon d'un navire ou aéronef français, quel que soit le lieu où ils se trouvent, seule la loi française est applicable.

B. Les infractions commises hors du territoire de la République

L'infraction étant commise à l'étranger, le principe de territorialité est abandonné. La nécessité de réprimer efficacement la criminalité internationale et celle de protéger les intérêts de la France au-delà de ses frontières ont conduit à reconnaitre la compétence de la loi française pour un nombre toujours plus grand d'infractions commises à l'étranger. Cette compétence est prévue par les articles 113-6 à 113-12, soit en raison de la nationalité française de l'auteur ou de la victime

B.1. L'application de la loi française en raison de la nationalité française de l'auteur ou de la victime

En tout état de cause, c'est le principe de la personnalité de la loi pénale qui va être mis en œuvre selon lequel la loi pénale ne s'applique qu'à l'égard de ses nationaux qu'ils soient d'une infraction (personnalité active) ou qu'ils en soient les victimes (personnalité passive) et les atteinte à des intérêts supérieurs français.

C. La compétence universelle des juridictions française par l'effet des conventions internationales

La compétence universelle ne peut résulter que d'une convention internationale et ne vaut que pour les infractions désignées par celle-ci. La règle non bis in idem s'applique en cas de compétence universelle : les poursuites devant les juridictions français sont exclues lorsque l'intéressé a déjà été jugé pour les mêmes faits[129].

En effet, « aucune plainte ou dénonciation préalable n'est ici nécessaire. Les cas de compétence

universelle tendent à se multiplier. Les principaux d'entre eux figurent aux articles 689-2 à 689-9 du code de procédure pénale : acte de torture (convention de New York, 1984), terrorisme (convention de Strasbourg, 1977 ; convention de New York, 1998 & 2000), etc… »[130].

2.2. En droit congolais

A. Principe de territorialité

Le principe de territorialitéest consacré en droit congolaisdans trois dispositions légales distinctes: l'article 2 du code pénal, l'article 67 de la loi organique portant organisation, fonctionnement et compétence des juridictions de l'ordre judiciaire et l'article 14 du code civil livre premier.

- L'article 2 du code pénal dispose que : « l'infraction commise sur le territoire de la République est punie conformément à la loi »[131].
- L'article 67 alinéa 1 de la loi organique portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire prévoit que : « en matière répressive, le Ministère public recherche les infractions aux actes législatifs et règlementaires qui sont commises sur le territoire de la République »[132].
- L'article 14 du code civil livre premier stipule que : « les lois pénales ainsi que les lois de police et de sureté publique obligent tous ceux qui se trouvent sur le territoire de l'Etat »[133].

Ainsi donc, « relève de la compétence des tribunaux congolais, toute infraction dont l'un des éléments constitutifs a été réalisé au Congo à condition qu'aucun jugement définitif n'ait été rendu à l'étranger pour les mêmes faits et à l'endroit du même infracteur parce que le Congo consacre le principe de non bis in idem »[134].

En revanche, ce principe de territorialité reçoit des exceptions qui n'en sont qu'en apparence. Cependant, « en vertu de l'immunité dont ils bénéficient sur le plan international, les diplomates étrangers, les ministres, représentants diplomatiques, attachés d'ambassades et leurs personnels ne peuvent pas être poursuivis et condamnés en RDC pour les infractions qu'ils commettraient sur le territoire congolais et même dans l'enceinte de leurs ambassades respectives »[135].

B. Les corrections au principe de territorialité

B.1. Correction relevant de l'universalité

L'universalité du droit de punir est visée par le législateur congolais à l'article 3 alinéa 1^{èr} du code pénal congolais, qui prévoit expressément que : « toute personne qui, hors du territoire de la République Démocratique du Congo, s'est rendue coupable d'une infraction pour laquelle la loi congolaise prévoit une peine de servitude pénale de plus de deux mois, peut être poursuivie et jugée en République Démocratique du Congo, sauf application des dispositions légales sur l'extradition »[136].

En clair, les cours et tribunaux congolais sont compétents pour juger toute personne, quelle que soit sa nationalité ou celle de sa victime, qui se sera rendue coupable, à l'étranger, d'une infraction présentant une certaine gravité. Ainsi, « la gravité de l'infraction sera appréciée selon deux critères : il faut que la loi congolaise prévoie aussi l'infraction (principe de la double incrimination) et il faut que cette infraction soit punissable par la loi congolais d'une peine supérieure à deux mois »[137].

A en croire le Professeur NYABIRUNGU, « la poursuite et le jugement du délinquant qui s'est rendu coupable d'une infraction à l'étranger sont soumis à certaines conditions : il faut que l'infraction présente une certaine gravité ; il faut que l'inculpé soit trouvé au Congo au cours de l'instruction au moins (sauf pour les infractions d'atteintes à la sûreté de l'Etat et à la foi publique ; il faut que l'inculpé n'ait pas encore été jugé définitivement à l'étranger et en cas de condamnation, n'ait pas subis ou prescrit sa peine ou obtenu sa grâce car le droit congolais tient compte de l'application du principe de non bis in idem ; il faut une requête du Ministère Public ; lorsque l'infraction lèse un particulier et qu'elle est punissable de 5 ans au moins par la loi congolaise, il faut ou bien que la partie offensée dépose plainte, ou bien que l'autorité du pays où l'infraction a été commise la demande officiellement à l'autorité judiciaire du Congo»[138].

B.2. Correction relevant de la personnalité

B.2.1. ***L'infraction commise à l'étranger par un congolais : la personnalité active***

Selon le Professeur WANE BAMEME, « à l'évidence, il y a application du système de la personnalité active. Ce système veut que la norme congolaise puisse s'appliquer lorsqu'il est établi que les faits infractionnels commis sur un territoire étranger ont été l'œuvre d'un congolais. C'est l'interprétation du premier alinéa de l'article 3 du Code pénal congolais qui peut constituer partiellement le fondement de cette compétence active. La loi pénale congolaise applicable dans tous les cas de commission d'une infraction, par un congolais hors du territoire de la République » [139].

B.2.2. L'infraction commise à l'étranger contre un congolais : la personnalité passive

Cette compétence personnelle passive voudrait que la loi pénale congolaise soit applicable à toute infraction commise par un congolais ou par un étranger hors du territoire de la République, lorsque la victime est de nationalité congolaise.

B.2.2. L'infraction commise à l'étranger contre les intérêtsde la RDC : personnalité réelle

Il y a atteinte aux intérêts fondamentaux de la nation lorsqu'une infraction commise porte atteinte à son indépendance, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense et de sa diplomatie, à la sauvegarde de la population aussi bien sur le territoire national qu'à l'étranger, à l'équilibre de son milieu naturel et de son environnement, à des éléments essentiels de son potentiel scientifique, économique et patrimoine culturel.

De ce fait, « une norme pénale congolais peut également se révéler compétente à s'appliquer sur des infractions commises par des étrangers au-delà des frontières nationales lorsqu'il est établi que les dites infractions ont porté atteinte aux intérêts fondamentaux de la République Démocratique du Congo »[140]. Il s'agit néanmoins, des atteintes à la sûreté de l'Etat regroupant la trahison, l'espionnage, les attentats et complots contre le chef de l'Etat, les attentat, complots et

autres infractions contre l'autorité de l'Etat et l'intégrité du territoire, les attentats et complots tendant à porter le massacre, la dévastation ou le pillage, la participation à des bandes armées, la participation à un mouvement insurrectionnel et autres.

§3. Mécanisme de coopération internationales contre le crime

A l'heure actuelle, la criminalité tant moderne que traditionnelle acquiert une dimension internationale voire même mondiale de par l'apparition de World wide web. Et cela mobilise les Etats à manifester une certaine collaboration pour combattre ou éradiquer ce fléau. Pour y parvenir, les Etats mettent en place une procédure appelée extradition (3.1) et d'autres formes de collaboration internationale (3.2).

3.1. L'extradition

A. Notions

En tant qu'une procédure internationale, l'extradition consiste pour « un Etat (dit Etat requis) d'accepter de livrer un individu se trouvant sur son territoire à un autre qui en a fait la demande (Etat requérant) afin que celui-ci puisse le juger ou s'il est déjà condamné, lui fasse purger sa peine »[141]. De cette évidence, lorsque l'extradition est faite en faveur du pays où l'infraction fut commise, elle permet une justice plus efficace, car le délinquant est jugé par le pays qui dispose de plus d'atouts pour la recherche et découverte de la vérité.

Il sied de signaler que, l'extradition se base juridiquement sur les traités que les Etas concluent entre eux afin de se livrer mutuellement les délinquants les plus dangereux.

B. Conditions d'extradition

L'effectivité de ce mécanisme, requiert la réunion d'un certain nombre des conditions, se rapportant notamment à l'Etat requérant, à l'Etat requis et à l'individu recherché (le délinquant).

- ***L'Etat requérant***

Les Etats qui peuvent requérir sont : l'Etat sur le territoire duquel l'infraction a été commise ; l'Etat dont est ressortissant la personne recherchée; et l'Etat dont l'infraction a mis en cause les intérêts essentiels.

- ***L'Etat requis***

Il s'agit bel et bien du pays où la personne recherchée se trouve actuellement.

- ***L'individu recherche***

C'est l'auteur, coauteur ou complice d'une infraction consommée ou tentée que l'Etat requérant à compétence de réprimer.

C. Infractions extraditionnelles

Les infractions extraditionnelles doivent présenter une certaine gravité. Ainsi, pour déterminer cette gravité, deux techniques sont possibles : soit l'énumération des faits pouvant donner lieu à l'extradition dans le corps même du traité, soit la référence à la gravité de la peine encourue ou effectivement prononcée pour l'infraction dont il s'agit. C'est-à-dire, les conventions d'extradition

signées entre Etats précisent la gravité de l'infraction dont les auteurs peuvent faire l'objet d'extradition.

D. Infraction non extraditionnelles

Les infractions militaires et celles politiques ne peuvent faire l'objet d'une extradition.

1. Les infractions militaires

L'article 40 alinéa 1^{èr} du Code pénal militaire dispose que : « les infractions d'ordre militaire sont celles qui ne sont commises que par des militaires ou assimilés. Elles consistent en un manquement au devoir de leur Etat »[142]. En effet, ces infractions sont réparties en quatre catégories :

- « Des infractions tendant à soustraire leur auteur de ses obligations militaires (de l'insoumission, de l'absence irrégulière, des désertions, de la mutilation volontaire et de la lâcheté »[143] ;
- « Des infractions contre l'honneur ou le devoir (de la capitulation ou de défaitisme, du complot militaire, des pillages, des destructions, des faux, falsifications, concussions et corruptions, de l'usurpation d'uniformes, décorations, signes distinctifs et emblèmes, de l'outrage au drapeau ou à l'armée, de l'incitation à commettre des actes contraires au devoir ou à la discipline »[144] ;
- « Des infractions contre la discipline (de la révolte militaire, de la rébellion, du refus d'obéissance, des voies de fait et outrages envers les supérieurs, des violences ou insultes à sentinelle, des violences envers les populations civiles, du refus d'un service dû légalement, des voies de réquisition, du détournement des objets saisis, de la constitution illégale d'une juridiction répressive »[145] ;
- « Des infractions aux consignes »[146].

2. Les infractions politiques

L'on rencontre trois catégories d'infractions politiques : les infractions politiques pures, les infractions politiques complexes ou mixtes et les infractions annexes à des délits politiques.

a. Les infractions politiques pures

C'est tout simplement « les infractions qui ne portent atteinte qu'à l'ordre politique. Il s'agit de la haute trahison ou du complot »[147].

b. Les infractions politiques complexes ou mixtes

Ce sont les infractions qui, selon le Professeur NYABIRUNGU « existent lorsqu'un seul et même fait à caractère double, viole à la fois le droit commun et le droit politique »[148].

c. Les infractions connexes a des délits politiques

Ce sont des infractions de droit commun inhérentes à une action politique. Elles se commettent à l'occasion d'une guerre civile ou d'une insurrection. A titre exemplatif, nous pouvons évoquer les destructions méchantes des monuments des adversaires.

3.2. Autres mécanismes de collaboration internationale

A. La coopération avec la cour suprême de justice

Le traité de la CPI a été signé à Rome le 17/07/1998. La République Démocratique du Congo était le 60ème Etat qui ratifiait ce traité par le décret n°0013/2002 du 30/03/2002, et celui-ci est mis en vigueur le 1èr juillet 2002. En effet, l'article 86 du statut de la CPI (statut de Rome) exige que tous les Etats parties coopèrent pleinement avec la Cour dans les enquêtes et poursuites qu'elle mène pour les crimes relevant de sa compétence.

De ce fait, la CPI a la compétence de connaitre les crimes les plus graves qui touchent l'ensemble de la communauté internationale. Il s'agit du crime de génocide, des crimes contre l'humanité, des crimes de guerre et du crime d'agression. Aussi, « la Cour n'est compétente que si l'une des trois conditions suivantes est remplie »[149]. Il s'agit de :

- L'accusé est ressortissant d'un Etat partie au statut ou qui accepte la juridiction de la CPI en l'espèce ;
- Le crime a été commis sur le territoire d'un Etat partie ou qui accepte la juridiction de la CPI en l'espèce ;
- Le conseil de sécurité a saisi le Procureur en vertu du chapitre VII de la charte des nations-unies.

Il est loisible de signaler que, « en vertu du principe de subsidiarité, les Etats conserveront à titre principal la responsabilité de poursuivre et juger les crimes les plus graves : la CPI ne sera compétente qu'en cas de défaillance ou de mauvaise volonté des Etats »[150].

Néanmoins, « la CPI ne peut être saisie que par un Etat partie, c'est-à-dire qui a signé le statut de Rome, le Procureur ou le conseil de sécurité des Nations-Unies »[151].

B. La collaboration policière internationale

Il s'agit ici, « des polices nationales surtout celles des pays partageant les frontières, collaborent entre elle et s'échangent des informations, voir des délinquants. Mais la forme la plus élaborée de la collaboration policière contre les criminels internationaux, c'est assurément l'organisation internationale de la police criminelle (OIPC), communément appelée INTERPOL »[152].

C. Lemandat d'arrêt européen

D'après le Professeur WANE, « l'Union Européenne a adopté une décision cadre du 13/06/2002 qui prévoyait de remplacer la procédure d'extradition, par une nouvelle procédure qui est celle de Mandat d'Arrêt Européen »[153].

TITRE DEUXIEME : CONSIDERATIONS GENERALES SUR L'INFRACTION

L'infraction est l'élément de base de la loi pénale, raison pour laquelle le présent titre se bornera sur les éléments constitutifs de l'infraction (chapitre unique).

CHAPITRE UNIQUE : LES ELEMENTS CONSTITUTIFS DE L'INFRACTION

Il va falloir analyser tour à tour la définition et l'élément légal de l'infraction (section 1), des éléments matériels de l'infraction (section 2) avant de se focaliser sur l'élément intellectuel de l'infraction (section 3).

SECTION 1ère : DEFINITION ET ELEMENT LEGAL DE L'INFRACTION

§1. Définition

Le code pénal congolais est silencieux quant à la définition de l'infraction. Ainsi, pour rendre fécond cette étude, il nous a été d'une grande nécessité de recourir à la définition de l'article 1382 du Code civil belge, qui la définit comme : « est une infraction, tout fait quelconque de l'homme auquel la loi a attaché une sanction pénale »[154].

Quant à HAUS, l'infraction « une violation d'une loi pénale, l'action ou l'inaction que la loi frappe d'une peine »[155].

De notre côté, l'infraction est entendue comme une violation d'une loi de l'Etat, résultant d'un acte externe de l'homme, positif ou négatif, socialement imputable, ne se justifiant pas par l'accomplissement d'un devoir ou l'exercice d'un droit et qui est frappé d'une peine prévue par la loi.

Abordant la même matière, Pierre de QUIRINI S.J., estime que : « pour qu'il ait infraction, deux éléments doivent exister : il faut qu'il ait violation d'une loi de l'Etat ou d'un règlement d'une part, et d'autre part il faut que cette omission soit sanctionnée par une peine »[156].

Bref, une infraction est un fait imputable à l'homme et sanctionné par la loi.

§2. Elément légal de l'infraction

L'élément légal de l'infraction est constitué de l'article qui régit l'infraction, car il n'y a pas d'infraction qui ne soit punie par la loi. C'est ce qui ressort du principe de la légalité des délits et des peines consacré au premier titre.

SECTION 2. ELEMENTS MATERIELS DE L'INFRACTION

TOPUSULA IPANZA Geoffrin soutient que : « aucune infraction ne peut être punie sans la constatation d'un élément matériel »[157]. Ainsi donc, il va falloir analyser dans cette section, la notion générale d'un élément matériel de l'infraction (§1), cerner les notions de l'élément général (§2) et spécifique de l'infraction (§3), et enfin, s'attarder sur la tentative punissable (§4).

§1. Notions de l'élément matériel

François DURIEUX estime qu'un élément matériel « peut-être un fait ou un ensemble des faits décrits par le texte d'incrimination »[158].

Pour BOUZAT, cité par le Professeur NYABIRUNGU, « l'élément matériel, c'est le fait extérieur par lequel l'infraction se révèle et, pour ainsi dire, prend corps »[159].

Surabondamment, le Professeur WANE opine dans le même sens, et estime que : « l'élément matériel de l'infraction constitue l'acte par lequel, l'auteur extériorise ou fiat extérioriser sa pensée criminelle »[160]. Il s'agit en fait, d'un comportement que le législateur juge anti-social, et par conséquent, il est susceptible d'être constaté à l''extérieur. C'est ce que NYABIRUNGU désigné de *« corpus delicti »*[161].

La notion de l'élément matériel de l'infraction implique l'étude du cheminement criminelle, appelé *"Itercriminis"* (A) ainsi que des stades du processus criminel (B).

A. Itercriminis

Il constitue le cheminement par lequel devra passer l'infraction. Il comprend non seulement la conception et la résolution criminelle mais aussi la manifestation de la cogitation criminelle. Autrement dit, c'est le processus de formation du crime qui trouvera son aboutissement dans la réalisation criminelle qui l'on qualifie ainsi d'élément matériel requis.

B. Stades du processus criminel

Lorsque nous parlons des stades du processus criminel, c'est la question de voir comment l'infraction se consomme, soit encore comment elle se prépare. En effet, la consommation d'une infraction sous-entend, la réunion de tous les éléments exigés pour l'existence d'une infraction. La préparation de l'infraction présume que la phase de la préparation contient la manifestation et les actes préparatoires. Ce sont des actes extérieurs par lesquels l'agent se procure, apprête et dispose les moyens dont il attend se servir pour mener à bon port son plan criminel.

Par ailleurs, « le droit pénal requiert l'accomplissement d'un acte, c'est-à-dire une réalisation-manifestation, un événement dans le monde extérieur »[162], car « les intentions qui ne se manifestent par aucun acte extérieur, n'offrent pas de prise à une accusation humaine »[163].

En définitive, un acte préparatoire constitutif de l'infraction est entendu comme « tout acte matériel posé par un délinquant déterminé qui, suite à une cause reconnue et incontrôlée par l'agent et qui a occasionné l'abandon de ce projet criminel sans atteindre le seuil de la tentative punissable »[164].

§2. Elément matériel général

Tel que dit supra, aucune infraction ne peut être punie sans la constatation d'un élément matériel. Celui-ci manifeste l'acte par lequel, l'auteur extériorise ou fait extérioriser sa pensée criminelle. C'est un comportement constatable à l'extérieur. C'est la cristallisation ou mieux la matérialisation d'une infraction.

§3. Elément matériel spécifique

Il s'agit ici d'un aspect concret à travers lequel se présente dans un cas particulier une infraction. En clair, « les éléments spécifiques de l'infraction sont ceux qui la différencient des autres infractions de la façon la plus concrète, ils forment l'objet propre et principal du droit pénal spécial » [165]

. C’est par exemple le meurtre qui se distingue de l’assassinat. Ces deux incriminations préconisent l’intention de donner la mort mais, une mort avec préméditation constitue l’assassinat. Donc la préméditation est un élément matériel spécifique.

§4. La tentative punissable

En principe, une infraction doit être consommée pour entrainer une sanction. Or, une infraction n’est consommée que si le résultat initialement visé par le texte de qualification est concrètement atteint. Afin de prévenir à un tel résultat, le contrevenant doit accomplir toute série d’actes, d’agissement, situation, appelée par les pénalistes "le processus criminel". Ce processus va englober les actes préparatoires, le commencement d’exécution et la consommation de l’infraction, or le problème auquel on va être confronté est celui des infractions dites impossibles, tentées et manquées.

Selon l’article 4 du Code pénal congolais combiné avec l’article 4 du Code pénal militaire congolais, qui disposent que : « il y a tentative punissable lorsque la résolution de commettre l’infraction a été manifestée par des actes extérieurs qui forment un commencement d’exécution de cette infraction et qui n’ont été suspendues ou qui n’ont manqué leur effet que par des circonstances indépendants de la volonté de l’auteur. La tentative est punie de la même peine que l’infraction consommée »[166].

Par conséquent, lorsque l’exécution a été suspendue ou interrompue par une cause extérieure à l’agent, l’on parle de l’infraction tentée, mais lorsqu’elle a manqué son effet alors que tous les actes d’exécution ont été accomplis, dans ce cas c’est l’infraction manquée, enfin, lorsque le résultat recherché par l’argent ne peut être atteint soit par manque d’objet, soit par inefficacité des moyens utilisés, l’on parle de l’infraction impossible.

SECTION 3. ELEMENT INTELLECTUEL DE L’INFRACTION

Pour qu’un délinquant soit déclaré pénalement responsable, il faut qu’il ait commis matériellement un acte proscrit par la loi, c’est l’élément matériel mais il faut également que cet acte puisse lui être reproché, c’est-à-dire qu’il faut qu’il ait commis une faute, et que cette faute soit intentionnelle, soit non intentionnelle.

En effet, c’est le lien entre l’acte matériel et l’auteur qui constitue l’élément moral ou intellectuel de l’infraction que l’on appelle " MENS REA " ou " LA VOLONTE CRIMINELLE ". Donc, l’élément moral de l’infraction intervient pour mieux juger la responsabilité d’une personne.

De cette évidence, il faut dire que toute infraction n’est constituée et n’est punissable que si son auteur a eu la volonté ou la conscience de violer la loi pénale. Toutefois, cette volonté ne joue pas le même rôle u n’a pas la même étendue dans toutes les infractions. Car, dans certaines infractions, la volonté ne porte que sur l’acte lui-même. Dans d’autres, elle porte à la fois sur l’acte et sur ses conséquences.

En effet, constant la diversité des infractions dans l’arsenal juridique congolais et français, il convient d’étudier dans les lignes qui suivent leur classification.

DEUXIEME PARTIE : DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION ET LEUR USAGE

Les technologies de l'information se caractérisent par les développements technologiques récents dans les domaines des télécommunications et du multimédia ainsi que par la convivialité accrue des produits et services qui en sont issus et qui sont destinés à un large public de non spécialistes. Elle englobe des domaines assez variés, tels que les biotechnologies ou encore les nanotechnologies.

Ainsi donc, nous avons bien restreint notre étude aux domaines qui nous intéressent dans le cadre de l'électronique, l'informatique et les télécommunications. Il s'agit là, des nouvelles technologies de l'information et de la communication.

Dans cette partie, nous allons tout d'abord présenter la description des technologies de l'information et de la communication (titre 1). Ensuite, nous nous imprégnerons à étudier les infractions des nouvelles technologies de l'information et de la communication : la cybercriminalité (titre 2). Et enfin, une considération comparative de la répression de la cybercriminalité en droits congolais et français viendra mettre fin au vif de notre étude (titre 3).

TITRE PREMIER : DESCRIPTION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Le présent titre aborde tour à tour l'analyse conceptuelle (chapitre 1) et l'usage des technologies de l'information et de la communication (chapitre 2).

CHAPITRE PREMIER. ANALYSE CONCEPTUELLE ET CONTENU DES NTIC

Dans ce chapitre, nous parlerons successivement de l'analyse conceptuelle (section 1) ainsi que du contenu des NTIC (section 2).

SECTION 1ère. ANALYSE CONCEPTUELLE

La présente section abordera la technologie (§1), l'information (§2), la communication (§3), les nouvelles technologies (§4), technologie de l'information et de la communication (§5), et enfin, les nouvelles technologies de l'information et de la communication (§6).

§1. La technologie

D'après le dictionnaire le Petit Robert illustré, le concept technologie est défini comme étant « une étude des outils, des machines utilisées dans l'industrie. Ensemble des savoirs et de pratiques, fondé sur des principes scientifiques, dans un domaine technique »[167].

Celle-ci est prise comme : « un ensemble de procédés ordonnés, scientifiquement mis au point, qui sont employés à l'investigation et à la transmission de la matière »[168].

A en croireMICROSOFT ENCARTA 2009, lorsqu'il définit le terme technologie comme étant « ensemble de savoir, de procédés ou d'outils qui mettent en œuvre les découvertes et les applications scientifiques les plus récentes »[169]. Pour WIKIPEDIA, une technologie désigne «l'étude des outils et des technologies »[170].

§2. L'information

En informatique, une information « est un ensemble de données pouvant être traitées par un système informatique »[171]. Elle peut aussi être définie comme un élément de connaissance susceptible d'être codé pour être conservé, traité ou communiqué. Il s'agit d'un élément ou système pouvant être transmis par un signal ou une combinaison de signaux.

§3. La communication

Par communication, il faut entendre « l'ensemble des moyens et des techniques permettant la diffusion de messages écrits ou audiovisuels auprès d'un public plus au moins vaste et hétérogène »[172]. C'est en fait, toute opération de transfert ou d'échange d'informations entre un émetteur et un récepteur.

§4. Nouvelles technologies (NT)

Selon le petit Larousse Illustré, les nouvelles technologies ou technologies de pointe « sont des moyens matériels, organisations et structurels qui mettent en œuvre les découvertes et les applications scientifiques les plus récentes »[173].

Somme toute, le dictionnaire électronique ENCARTA renchérit en définissant les nouvelles technologies en tant que « ensemble de savoirs, de procédés et d'outils qui mettent en œuvre les découvertes et les applications scientifiques dans les domaines de l'informatique et de la

communication »[174].

§5. Technologie de l'information et de la communication (TIC)

Expression aux contours assez flou, apparue avec le développement des réseaux de communication, désignant tout ce qui tourne autour d'internet et du multimédia. Elle recouvre également la notion de convivialité accrue de ces produits et services destinés à un large public de non spécialistes.

Il s'agit d'un ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des télécommunications, qui ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information. En effet, « les TIC, sont un ensemble des technologies parmi lesquelles figure souvent l'ordinateur et qui, lorsqu'ils sont combinés ou interconnectés, permettent de numériser, de traiter, de rendre accessible et de transmettre, en principe à n'importe quel endroit, une quantité quasi illimité et très diversifiée de données »[175].

HEBERT Simon les définit comme étant « un ensemble des technologies d'informatique et de télécommunication, ils sont les résultats d'une convergence entre technologie. Elles permettent l'échange des informations ainsi que leur traitement. Elles offrent aussi des nouveaux moyens et méthodes de communication »[176].

Quant à CHARPENTIER : « Les TIC sont un ensemble des technologies utilisées pour traiter, modifier et échanger de l'information, plus spécifiquement des données numérisées. La naissance de ces TIC est due notamment à la convergence de trois activités. Au sens strict, les TIC sont composées :

- du domaine des télécommunications qui comprend lui-même les services et les équipements ;
- du domaine de l'informatique comprend le matériel, les services et les logiciels ;
- du domaine de l'audiovisuel qui comprend principalement la production et les services audiovisuels ainsi que l'électronique grand public »[177].

§6. Nouvelles technologies de l'information et de la communication (NTIC)

« Le concept NTIC est apparu pour marquer l'évolution fulgurante qu'ont connu les technologies de l'information avec l'avènement des autoroutes de l'information (notamment l'utilisation de l'internet) et l'explosion du multimédia. C'est l'interpénétration de plus en plus grande de l'informatique, des communications et de l'audiovisuel qui est à l'origine des changements rapides sur le plan technique, conceptuel et terminologique »[178].

Ainsi, « les premier pas vers une société d'information furent entamés lors de l'invention du télégramme électrique, du téléphone fixe, de la radiotéléphonie et de la télévision. L'informatique, la télécommunication, mobile-GPS et GSM-et la télévision numérique sont considérées comme de NTIC, parce qu'elles utilisent la haute technologie, la technologie numérique, le système binaire » [179].

SECTION 2. CONTENU DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Les NTIC sont constituées de trois secteurs relatifs à l'informatique (§1), de l'électronique (§2), et enfin, de la télécommunication (§3).

§1. L'INFORMATIQUE

Le dictionnaire le Petit Larousse illustré défini l'informatique comme étant « une science du traitement automatique et rationnel de l'information en tant que support des connaissances et des communications ; ensemble des applications de cette science mettant en œuvre des matériels (ordinateurs) et des logiciels »[180]. En effet, dans ce secteur, l'on a des machines de bureau, les ordinateurs personnels, grands ordinateurs, matériels de réseau, périphériques, serveurs, carte, etc…

§2. L'électronique

Dans le secteur électronique, l'on trouve les différents composants électroniques, semi-conducteurs, circuits imprimés, équipement de l'électronique grand public (télévision, récepteurs radio, lecteurs de disques, magnétoscopes, instruments de mesure, instruments de navigation, etc… C'est une catégorie d'outils et de biens de consommation obtenus par utilisation de l'électricité en vue de la transmission de l'information.

D'après MICROSOFT ENCARTA 2009, l'électronique « est le domaine de la physique appliquée qui exploite les variations de grandeurs électriques (courants, tensions, charges, etc..) pour capter, transmettre ou analyser des informations (signaux audio d'un récepteur radio, image d'un écran de télévision, données informatiques d'un ordinateur, etc… »[181].

§3. La télécommunication

La télécommunication « est un ensemble des procédés permettant de transmettre des informations à distance, tels que le téléphone, la radio, la télévision, et maintenant les réseaux informatique »[182]. De ce fait, elle constitue toute communication à distance. Suivant le type d'information transmise ou échangées, on distingue les procédés de télécommunication du son (téléphone, radiodiffusion), de l'image (vidéographie), du son et de l'image (télévision), des textes complétés ou non d'éléments visuels ou sonores (télégraphe, télécopie, courriel).

Toutefois, selon le mode d'échange, on différencie les moyens de télécommunication fonctionnant toujours à sens unique, d'un émetteur vers un ou plusieurs récepteurs (radiodiffusion, télévision) de ceux qui permettent d'instaurer un dialogue entre deux personnes ou deux groupes (téléphones) ou bien entre d'un côté une personne ou un groupe et de l'autre côté un fournisseur de service en ligne (site web).

CHAPITRE DEUXIEME : USAGE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Dans ce chapitre, il sera question d'analyser l'usage de l'informatique (section 1) et des télécommunications (section 2), qui sont les deux secteurs intéressant notre sujet d'étude.

SECTION 1ère. USAGE DE L'INFORMATIQUE

Trois principaux paragraphes constituent l'ossature de cette section. Il s'agit de l'historique de l'ordinateur (§1), des domaines d'application de l'informatique (§2), et enfin, des notions générales

et globales de l'informatique (§3).

§1. Historique de l'ordinateur

Le présent paragraphe aborde tour à tour la période avant l'ordinateur (A), pendant le premier ordinateur (B), et enfin, les générations des ordinateurs (C).

A. Avant l'ordinateur

Cette période couvre les automates (1), les machines à calculer (2), ainsi que les machines programmables[183].

A.1. Les automates

Par automate, nous entendons « un appareil présentant l'aspect d'un être humain ou d'un animal et capable d'en imiter les gestes. Il est équipé de dispositifs qui permettent l'exécution de certaines tâches sur l'intention de l'homme. Il s'agit des robots »[184].

A.2. Les machines à calculer[185]

Depuis le millénaire, l'homme a créé et utilisé des outils l'aidant à calculer pour réaliser des calculs complexes. Parmi ces outils, nous y trouvons :

- Les abaques ;
- Le boulier compteur ;
- L'horloge calculante ;
- La Pascaline ;
- Le multiplicateur de LEIBNIZ.

B. Premiers ordinateurs

Le développement de l'ordinateur est marqué par l'apparition effective de l'ElectronicNuméricalIntegrator and Computer (b.1.) et de l'Electronic Discret Variable Computer (b.2.).

B.1. Electronic numérical integrator and computer-ENIAC

D'après C. LUAMBA et Alii, l'ENIAC « est inventé par John MAUCHLY et Prosper ECKERT en 1945, qui fut une machine électronique universelle, programmable, numérique basée sur le système décimal. Commandée par l'armée des Etats-Unis en 1943 pour effectuer les calculs de balistique, il remplaçait 200 personnes chargées auparavant de calculer les tables de tir. Il occupait 23m3, pesait 30 tonnes, coûtait un demi-million de dollars et consommait presque 200 kilowatts »[186].

Toutefois, « bien qu'étant le premier calculateur électronique, l'ENIAC n'est pas considéré comme le premier ordinateur selon le sens donné aujourd'hui à ce terme »[187].

B.2. Electronic discret variable computer (EDVAC)

« Avant la fin de l'année 1945, JOHN VON NEUMAN, un mathématicien d'origine hongroise, associé comme consultant au projet ENIAC, franchit le dernier obstacle et proposa la construction de l'EDVAC, machine modèle de l'ordinateur tel qu'on le conçoit à présent, car il accomplit une abstraction géniale du système de commande de la machine en proposant d'enregistrer les programmes en mémoire »[188].

En effet, présentant l'aspect de l'ordinateur actuel, l'architecture ou structure d'un ordinateur selon VON NEUMAN est la suivante :

- La présence d'une unité arithmétique et logique (UAL) ;
- L'unité de commande ;
- La mémoire centrale ;
- L'unité d'entrée ;
- L'unité de sortie.

Ainsi, « EDVAC est le tout premier véritable ordinateur programmable »[189].

C. Générations des ordinateurs[190]

L'historique de l'ordinateur se présente en moult générations successives qui correspondent à des innovations majeures dans l'évolution du matériel et du logiciel.

Par conséquent, six générations sont à retenir. Il s'agit de :

- 1ère génération allant de 1945-1954 : Elle présente les caractéristiques suivantes : volume très grand, consommation élevée du courant électrique, beaucoup des pannes et calcul répétitif.
- 2ème génération allant de 1955-1965 : Qui a comme caractéristique la réduction du poids, réduction du volume, utilisation des circuits imprimés,…
- 3ème génération allant de 1966-1975 : Ces ordinateurs présentes les caractéristiques comme la miniaturisation des circuits d'où la réduction du volume des machines, accroissement de la vitesse d'exécution des opérations, réduction de plus en plus de la consommation de l'énergieélectrique.
- 4ème génération allant de 1970-1985 : C'est la génération des micro-ordinateurs.
- 5ème génération allant 1986-1991 : Génération caractérisée par la présence de la technologie des logiciels, traitement avancé des logiciels, bureautique, robotique, intelligence artificielle,…
- 6ème génération allant de 1991 – à nos jours : Dans cette génération, l'on trouve des supers ordinateurs dont la puissance de calculs donne accès au traitement d'images et de sons. Ils se développent aussi les ordinateurs portables en miniature, sans fils et/ou invisible à l'intelligence ambiante intégrée aux objets de la vie courante.

§2. Domaines d'application de l'informatique[191]

La présence des NTIC de par son intervention figurante dans certains domaines et au sein de la société. C'est-à-dire démontrer réellement la place qu'elles occupent dans la société.

En effet, il est question dans ce paragraphe, de mettre en évidence le rapport qui existe entre l'informatique et d'autres domaines. C'est ce que nous désignons de la TYPOLOGIE DE L'INFORMATIQUE. Ainsi, parmi une multitude des domaines auxquels intervient l'informatique, nous avions retenu ceux-ci :

- L'informatique juridique
- L'informatique éducationnelle ;
- L'informatique industrielle ;
- L'informatique médicale, qui englobe la télémédecine et l'e-santé.
- L'informatique commerciale ;
- L'informatique maintenance ;
- L'informatique réseau ;
- Le webmastering ;
- La bureautique ;
- etc…

§3. Notions de l'informatique

3.1. Sémantiques des concepts

A. Informatique

Le concept informatique a été proposé par l'Ingénieur Français Philippe DREYFUS et publié par l'académie française en 1965 pour désigner le traitement automatique de l'information. Le mot informatique est le résultat de la contraction de deux mots INFOR qui signifie INFORMATION et MATIQUE qui veut dire AUTOMATIQUE.

Ainsi comprise, l'informatique est définie comme : « la science du traitement raisonnable de l'informatique grâce à un système des machines automatiques appelé ordinateur dans presque tous les domaines (scientifique, technique, économique…) »[192].

B. Information

L'information désigne, l'élément conceptuel qui permet le traitement, le stockage et le traitement de connaissance. En d'autres mots, « tout ce qui peut être traité, stocké ou conserver dans l'ordinateur »[193].

C. Donnée

En informatique, une donnée « est une représentation d'une information sous forme conventionnelle, c'est-à-dire codée en caractère numérique, alphanumérique, alphabétique et ou en symboles ou signes »[194]. En d'autres mots, une information lisible par la seule machine en vue de son enregistrement, traitement, conservation et communication.

D. Science

La science, du latin scientia, signifie connaissance. C'est ce que l'on sait pour l'avoir appris. Elle est « un ensemble de connaissance, d'études d'une valeur universelle caractérisée par un objet (domaine) et une méthode déterminée, et fondée sur des relations objectives vérifiables »[195]. Autrement dit, la science est destinée à produire des connaissances scientifiques à partir des méthodes d'investigation rigoureuses, vérifiables et reproductrices.

E. Ordinateur

Le mot ordinateur a été inventé en 1950 par le Français Jacques PERRET à la demande de l'IMB France afin de doter la langue française d'un terme équivalent à son homologue anglo-saxon " computer ". En effet, un ordinateur « une machine électronique qui fonctionne par la lecture séquentielle d'un ensemble d'instructions qui lui font exécutées les opérations et arithmétiques sur les chiffres binaires »[196].

Selon C. LUEMBA et Alii, « l'ordinateur est une machine ou un ensemble des machines automatiques capables de traiter une information »[197]. Il est une machine électrique qui permet de traiter les informations d'une façon automatique grâce aux programmes préenregistrés.

F. Programme

En informatique, le programme désigne une suite d'opérations prédéterminées, destinées à être exécutées de manière automatique par un appareil informatique. C'est un ensemble d'instructions relatives à des traitements des informatiques automatiques.

3.2. Structure d'un système informatique

Un ordinateur est appelé système, car il est structuré d'un ensemble d'éléments interconnectés en vue de produire un résultat. Ainsi donc, l'ordinateur est composé de deux grandes parties, en l'occurrence de la partie matérielle appelée "HARDWARE" (3.2.1) et de la partie immatérielle appelée "SOFTWARE" (3.2.2).

3.2.1. Le hardware

En Français quincaillerie, le Hardware est « la partie visible palpable, touchable de l'ordinateur » [198]. C'est la partie « matérielle »[199]. En effet, le Hardware est divisé en deux parties, d'une part l'unité centrale (A) et les unités périphériques (B) d'autre part.

A. L'unicité centrale

L'unité centrale recouvre, le boitier central du système contenant tous les organes vitaux de l'ordinateur. Elle est composée de plusieurs éléments, entre autres la carte mère, le processeur, les mémoires, etc.…

A.1. La carte mère

La carte mère, est une carte sur laquelle on branche ou soude les composants sur un circuit imprimé et sur lequel on greffe les connecteurs des périphériques.

A.2. Le processeur ou micro-processeur

Appelé aussi unité centrale de traitement, est le cerveau de l'ordinateur, car « il est le composant de l'ordinateur qui a pour mission d'analyser et d'exécuter les instructions du programme »[200]. Il est à la base de tous les calculs, c'est-à-dire il réalise toutes les opérations analogiques et numériques de l'ordinateur et après le traitement, il transfère le résultat à la mémoire centrale.

A.3. Les mémoires

Une mémoire est un dispositif ayant pour mission d'enregistrer l'information, de la conserver et de la restituer. Ainsi, dans un ordinateur, l'on retrouve la mémoire ROM, RAM et la mémoire de masse (unité centrale).

A.4. La carte d'extension

Elle permet de brancher tous les composants externes pour être reliés à la carte mère. Généralement, elle est placée derrière l'unité centrale, et contient des orifices appelé ports.

B. Les unités périphériques

B.1. Définition

Un périphérique est, « tout dispositif matériel que l'on peut brancher à l'ordinateur pour communiquer avec »[201]. Il faut préciser que, les échanges entre l'homme et l'ordinateur se fond à partir des organes de communication, d'entré ou de sortie, appelés périphériques.

B.2. Typologie des périphériques

Il existe quatre types de périphériques, à savoir :

1. Périphériques d'entrée (clavier, souris, scanneur, ect…) ;
2. Périphériques de sortie (écran, imprimante, haut-parleurs, etc…) ;
3. Périphériques d'entrée-sortie (modem, switch, etc…) ;
4. Périphériques de stockage (disque dur, flash disk, cd-rom, bande K7, carte mémoire, carte sim, ect…).

3.2.2. Le software

Le Software « est la partie immatérielle, intelligible de l'ordinateur. Il est constitué d'un ensemble de programmes ou logiciels »[202]. En effet, il existe trois types de programmes, à savoir :

A. Le programme résident ou de base- BIOS

Le Basic in/out put system, est le programme de base incorporé à l'intérieur de l'unité centrale, au niveau de la mémoire ROM de l'ordinateur par le fabricant. C'est le programme de démarrage qui fait fonctionner la carte mère.

B. Le système d'exploitation

C'est un programme qui gère tout le fonctionnement de l'ordinateur. Il sert d'intermédiaire entre l'opérateur et l'unité centrale. Il permet à l'utilisateur d'exploiter toutes les ressources de la machine. A titre exemplatif, nous avons le MS-DOS, MS-WINDOWS, etc.…

C. Le programme d'application

C'est un programme qui aide l'utilisateur à réaliser ses travaux spécifiques. Nous pouvons citer le cas de Ms-Word, Ms-Excel, Internet, etc…

3.3. Différents systèmes informatiques

Depuis l'apparition du véritable ordinateur programmable en 1945, il existe plusieurs familles

d’ordinateurs regroupées en trois, à savoir :

3.3.1. Les ordinateurs centraux

Ce sont les ordinateurs possédant une grande puissance de calculs, des capacités d’entrée-sortie gigantesques. Ils sont appelés Mainframes et pesaient au moins 30 tonnes.

3.3.2. Les mini-ordinateurs

« Les mini-ordinateurs est à l’origine une catégorie d’ordinateurs entre les ordinateurs centraux et les micro-ordinateurs »[203]. Ces ordinateurs avaient une moindre puissance que les précédents.

3.3.3. Les micro-ordinateurs (PC)

Ce sont les ordinateurs actuels, appelés ordinateurs personnels. Ils sont au nombre de trois, à savoir :

- Les ordinateurs de bureau (Desktop) ;
- Les ordinateurs portables (Lap top) ;
- Les ordinateurs de poche (Pocket pc).

3.4. Les réseaux informatiques

3.4.1. Définition et typologie des réseaux

A. Définition

Le terme générique réseau définit « un ensemble d’entités (objet, personne, etc…) interconnectés les unes avec les autres. Il permet de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon les règles bien définies »[204]. En informatique, le réseau appelé en Anglais NETWORK[205], « est un ensemble des ordinateurs et périphériques connectés les uns aux autres »[206]. Il pour intérêt l’échange des informations et permet de :

- Partager de ressources (fichier, connexion internet,….) ;
- La communication entre processus (industriel) ;
- La communication entre personne ;
- La garantie de l’unicité et de l’universalité de l’accès à l’information (base de données en réseau) ;
- Etc…

B. Typologie de réseaux[207]

Généralement, il existe trois catégories de réseaux informatiques. Il s’agit du réseau LAN, MAN et WAN.

B.1. Le réseau Lan (local area network)

Le réseau local est un ensemble d’ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l’aide d’une même technologie, la plus étant l’Ethernet.

B.2. Le réseau Man (metropolitan area network)

Le réseau métropolitain, est un réseau qui regroupe plusieurs LAN géographiquement proches.

B.3. Le réseau wan (wide area network)

Le réseau étendu interconnecte plusieurs LAN à travers de grandes distances géographiques. Le plus connu de WAN est l'internet.

3.4.2. L'internet

A. Définition[208]

L'Internet est un système d'interconnexion des machines qui constitue un réseau informatique mondial, utilisant un ensemble standardisé de protocoles de transfert de données. C'est un réseau des réseaux. Le terme d'origine américaine, il est le dérivé du concept "INTERNETING", qui signifie interconnecté des réseaux. Son apparition remonte vers les années 83.

B. Services de l'internet[209]

Les services de l'internet sont nombreux, mais dans le cadre de cette étude, nous retiendrons que quatre, à savoir : le web, le courriel, la messagerieélectronique et les forums.

B.1. Le web (toile d'araignée)

C'est un outil qui permet de naviguer sur internet, sur des pages multimédia, entre des documents reliés entre eux par des liens hypertextes.

B.2. Le courriel (e-mail[210])

Le courriel permet aux internautes de s'échanges des documents, photos, liens, textes, etc…

B.3. La messagerie instantanée-chat

C'est une communication synchronisée, qui constitue une communication réelle entre deux personnes, de manière instantanée qui permet d'établir des dialogues en temps réels. On y utilise le son et la webcam[211].

B.4. Les forums ou discussion

C'est une communication asynchrone. Les forums sont des espaces où des groupes d'internautes discutent en différé, en déposant des messages sur un serveur. Les forums regroupent généralement des discussions centrées autour des mêmes centres d'intérêt.

SECTION 2ème. USAGE DES TELECOMMUNICATIONS

Deux paragraphes constituent l'ossature de cette section. Il s'agit de l'application des télécommunications (§1) et des différents services des télécommunications (§2).

§1. Application des télécommunications

Le contenu d'une télécommunication peut donc être pratiquement de n'importe quelle nature, mais le moyen de transmission doit être de type électromagnétique. Il s'agit en fait, de tout transmission, émission ou réception des signes, des signaux, d'écrits, d'images, des sons ou des renseignements de toute nature par fil, radioélectricité, optique ou autres systèmes électromagnétique.

Ceci étant dit, trois types d'application sont à retenir, s'agissant de la transmission de la voix et du son (A), de la transmission de l'image et de la vidéo (B), et de la transmission du texte et de données (C).

A. La transmission de la voix et du son

Le transfert de la voix par le téléphone, fut la première avancée des télécommunications, juste après les premiers télégraphes.

En effet, « la téléphonie qui repose sur le réseau téléphonique permet également des services plus avancés tels que la messagerie vocale, la conférence téléphonique ou les services vocaux » [212]. A côté de la téléphonie, l'on trouve la radiotéléphonie, c''est-à-dire la communication à distance sans fil. Elle est le moyen principal de communication du contrôle aérien, des liaisons maritimes et des liaisons de sécurité.

Par ailleurs, la voix et le son sont également transmis à l'aide de la radiodiffusion, qui consiste la distribution du programme à partir d'un émetteur vers les auditeurs d'un récepteur. Toutefois, la téléphonie mobile est la possibilité de téléphoner sans connexion filaire soit par une solution terrestre basée sur les zones de couverture hertzienne d'antenne relais, soir par satellite.

Eu égard à ce qui précède, soulignons que, la voix et du son sont transmis par :

- Téléphone ;
- Messagerie vocale ;
- Conférences téléphoniques ;
- Informations téléphoniques (horloge parlante, météo,…) ;
- Radiodiffusion ;
- Téléphonie mobile.

B. La transmission de l'image et de la vidéo

La transmission de l'image et de la vidé est surtout l'œuvre de la télévision. Toutefois, d'autres mécanismes sont à la base, à savoir :

- Transfert d'images fixes ;
- Télévision

- Visiophonie
- Vison conférence
- Etc.…

C. La transmission du texte et des données

Le télégraphe est l'ancêtre des transmissions de données et la première application des télécommunications : transmettre les caractères, donc un message, par signaux optiques, puis une ligne et par ondes radio. Les mécanismes utilisés ici sont :

- Télex, télétex ;
- Courrier électronique ;
- Documentation électronique ;
- Vidéotex ;
- Télécopie.

§2. Services des télécommunications

« Un service des télécommunication peut être vu sous deux aspects, selon que l'on prend le point de vue de l'usage ou celui de l'exploitant du réseau :

- du point de vue de l'usage, le service est caractérisé par ses utilisations possibles, on parle alors de télé services ;
- du point de vue de l'exploitant, ce service est considéré selon son recours aux ressources offertes par le réseau, on parle alors de service support »[213].

TITRE DEUXIEME : INFRACTIONS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION : LA CYBERCRIMINALITE

Le présent titre consacré à l'étude des infractions cybernétiques, va analyser deux principaux chapitres, traitant tour à tour de l'analyse conceptuelle (chapitre 1) et des infractions des nouvelles technologies de l'information et de la communication ; et leurs techniques de perpétration (chapitre 2).

CHAPITRE PREMIER : ANALYSE CONCEPTUELLE

Il est question ici, de définir en premier lieu la cybercriminalité (section 1) et ensuite disséquer d'autres concepts associés au concept cybercriminalité (section 2).

SECTION 1. LA CYBERCRIMINALITE

D'entrée de jeu, disons que« la cybercriminalité ne définit pas à elle, seule une infraction, mais un ensemble d'atteintes aux biens ou aux personnes commises via l'utilisation des nouvelles technologies »[214].

Pour WIKIPEDIA, « la cybercriminalité est une notion large qui regroupe toutes infractions pénales

susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté sur le réseau »[215]. Il s'agit en fait, « d'une forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, appelé cyberspace »[216].

Quant à Emmanuel DADOUD, « la cybercriminalité regroupe les infractions anciennes, liées aux forme de criminalité traditionnelle qui ont pu et su évoluer avec les nouvelles technologies de l'information et de la communication et des infractions nouvelles, liées aux systèmes d'information et de traitement automatisé des données et qui sont apparues avec le développement des réseaux informatiques, et notamment d'internet »[217].

Selon l'Office Central de Lutte Contre la Criminalité liée aux technologies de l'information et de la communication, la cybercriminalité est un mot générique désignant « l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général et plus particulièrement sur les réseaux partageant le protocole TCP/IP, appelés communément internet »[218].

Il s'agit de toute infraction qui implique l'utilisation des technologies informatiques. C'est l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels. C'est une criminalité, ayant l'ordinateur pour objet ou pour instrument de perpétration principale.

« La cybercriminalité est la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale. »[219].

SECTION 2. AUTRES CONCEPTS

Il s'agit des concepts criminalité (§1), cyberspace (§2) cyberdélit(§5), cyberdelinquance (§3) et cybernaute (§4).

§1. Le cyberspace

Le terme cyberspace ou cybermonde désigne « un lieu imaginaire appliqué métaphoriquement au réseau internet et dans lequel les internautes qui naviguent s'adonnent à des activités diverses. C'est donc un environnement virtuel dans lequel se déroule la transmission des informations via internet, qui est considéré comme un moyen de communication »[220].

En effet, on appelle cyberespace «l'espace virtuel des ordinateurs reliés entre eux par des réseaux télématiques. Le droit considère le cyberespace comme un milieu global d'intérêt puisqu'il forme un environnement dans lequel se produisent des événements qui entraînent des conséquences juridiques diverses »[221].

§2. La criminalité

MITONGO KALONJI pense que : « le second concept mis en relief par ce vocable de cybercriminalité est celui de criminalité. Il n'est point utile de souligner ici les sempiternelles difficultés que la criminologie a pu avoir avec cette notion »[222]. En effet, elle désigne « l'ensemble des actes criminels commis dans un pays ou dans un groupe social donnés et à une période déterminée »[223].

Ainsi donc, dans le cadre de cette étude, nous nous limiterons à une conception juridique. C'est-à-dire, le crime est considéré comme un délit ou une infraction.

D'ailleurs, il importe de souligner que « généralement une infraction est considérée être un crime si elle porte atteinte au bien-être collectif de la société ou si elle déroge significativement des normes socio-culturelles qui dictent la conduite normale d'une personne »[224].

§3. La cyberdelinquance

La cyberdélinquance« englobe toute action illicite visant les systèmes informatiques soit comme formant l'objet du délit, soit comme constituant le moyen de commettre l'infraction »[225].

Ainsi, « le cyberdélinquant pourra utiliser l'ordinateur pour s'attaquer aux systèmes informatiques en utilisant l'ordinateur comme relais ou comme cible par des actes portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité des données, détruisant des données ou des sites, effectuant des intrusions, déposant des programmes pirates ou espions, envoyant des virus ou usurpant des adresses ou des noms de domaine »[226].

§4. Cybernaute

Le cybernaute « est la personne qui fait usage des réseaux de communication numériques et, dans un sens similaire, internaute celle qui utilise le réseau Internet (le Net, le Web, la Toile). Un cybernaute peut commettre un délit ou un crime en dévoyant le moyen de communication qu'est Internet ou en en faisant un mésusage illicite ou criminel. »[227].

§5. Le cyberdélit

Selon une acception courante, « un cyberdélit désigne toute activité mettant en jeu des ordinateurs ou des réseaux en tant qu'outil, cible ou lien d'une infraction »[228].

CHAPITRE DEUXIME : LES INFRACTIONS DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION ET LEURS TECHNIQUES DE PERPETRATION

Deux sections constituent la pierre angulaire de ce chapitre. Il s'agit d'une part des infractions des NTIC (section 1) ; et leurs techniques de perpétration d'autre part (section 2).

SECTION 1ère : LES INFRACTIONS DES NTIC : LA CYBERCRIMINALITE

Deux opinions se divergent quant aux catégories désignées sous le vocable de cybercriminalité. Pour les uns, en l'occurrence de l'encyclopédie universelle WIKIPEDIA, « on peut alors aujourd'hui regrouper la cybercriminalité en trois types d'infraction[229], à savoir :

- les infractions spécifiques aux technologies de l'information et de la communication ;
- les infractions liées aux technologies de l'information et de la communication ;
- les infractions facilitées par les technologies de l'information et de la communication.

Par contre, une autre opinion estime que : « la cybercriminalité comprend plutôt, d'une part, les crimes contre les NTIC, c'est-à-dire, les crimes dans lesquels les NTIC, dans leur essence

ontologique, sont l'objet même du délit et, d'autre part, les crimes facilités par les NTIC, c'est-à-dire, ceux dans lesquels les NTIC sont des moyens pour perpétrer les crimes avec facilité »[230].

Ainsi donc, dans le cadre de cette étude, et pour outrepasser cette controverse doctrinale qui demeure infinie, il est loisible de partager le même avis avec la deuxième opinion sur ledualisme des infractions des NTIC. En effet, il s'agit donc dans un premier temps d'aborder les infractions ontologiques aux NTIC (§1) ; et dans le second volet, se pencher sur les infractions dont la commission est seulement facilité par les NTIC (§2).

§1. Les infractions ontologiques ou directement liées aux NTIC

Il s'agit ici, « des infractions pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit »[231]. Elles ont comme caractéristiques, « la nature des technologies utilisées »[232]. En effet, les infractions directement liées aux NTIC regroupent « les infractions liées à la télécommunication, les infractions liées à la téléphonie cellulaire et les infractions informatiques »[233].

Par ailleurs, « dans cette sphère, la cybercriminalité recouvre un éventail d'inconduite dont l'existence est entièrement dépendante de celle des réseaux. Cette typologie vise toutes atteintes à la sécurité des systèmes et réseaux informatiques ou des données informatiques. Concrètement, ce sont des atteintes à la confidentialité, à l'intégrité, à l'authenticité et à la l'intégrité des systèmes et données informatiques »[234].

A en croire T-G. MITONGO et R-B MANASI lorsqu'ils précisent que, « plusieurs inconduites peuvent être relevées dans la catégorie sous analyse, à titre d'échantillon, nous en énumérons neuf (9) seulement »[235], à savoir :

1. l'accès illégal aux données et systèmes informatiques ;
2. l'interception illégale des données ;
3. l'atteinte à l'intégrité des données ;
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 communication ;
9. l'obstruction non intentionnelle aux correspondances par télécommunication.

A. L'accès illégal aux données et systèmes informatiques (piratage, craquage)

D'après la Convention Européenne sur la cybercriminalité, « l'accès intentionnel et sans droit à tout ou partie d'un système informatique »[236], constitue l'infraction d'accès illégal. Toutefois, « une partie peut exiger que l'infraction soit commise en violation des mesures de ou dans une autre intention délictueux, ou soit en relation avec un système informatique connecté à un autre système informatique »[237].

Selon l'Union Internationale des télécommunications : « le piratage (hacking) désigne l'accès illégal à un ordinateur »[238]. Cet accès initial est sanctionné comme suit :

- le système violé est protégé par des mesures de sécurités et/ou ;
- l'auteur de l'infraction a l'intention de nuire et/ou ;
- des données ont été collectées, modifiées ou corrompues.

B. Interception illégale des données

L'interception illégale des données consiste « à l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique. Y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques »[239].

En effet, pour obtenir des informations, les pirates peuvent également intercepter des communications ou de transfert des données. Les pirates sont susceptibles de viser tous les types d'infrastructure de communication et tous les types de service internet.Ils cherchent à identifier les points faibles du système.

C. L'atteinte à l'intégrité des données

L'atteinte à l'intégrité des données consiste par « le fait intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques »[240]. En effet, tout problème d'accès aux données peut aussi causer des dommages considérables. Les pirates peuvent vider l'intégrité des données de différentes façons :

- Par effacement ;
- Par suppression ;
- Par altération ;
- Par limitation de l'accès.

D. L'atteinte à l'intégrité des systèmes

Il sied de noter que « ce qui a été dit à propos des attaques visant les données informatiques s'appliquent également aux attaques visant le système informatique. Une façon de mener une attaque est de s'en prendre physiquement au système informatique, par destruction du matériel » [241].

En effet, selon l'article 5 de la Convention Européenne sur la cybercriminalité, l'atteinte à l'intégrité du système est « l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, l'altération ou la suppression de données informatiques »[242].

E. L'abus de dispositif ou utilisation abusive de dispositifs

Pour commettre un cyberdélit, un équipement relativement élémentaire suffit. Les infractions plus sophistiquées nécessitent l'utilisation d'outils logiciels spécialisés.

Ainsi, l'abus de dispositif, consiste à la commission intentionnelle et sans droit [243]:

1. La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :
    - d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;
    - d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils

soient utilisés afin de commettre l'une des infractions visées par les articles 2 à 5 ci-dessus.

2. La possession d'un élément visé ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées aux articles 2 à 5.

F. La falsification informatique

L'article 7 de la Convention européenne sur la cybercriminalité définit cette prévention comme : « l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit, de données informatiques, engendrent des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligible »[244].

G. la fraude informatique

La fraude informatique consiste par le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

1. par toute introduction, altération, effacement ou suppression des données informatiques ;
2. par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention frauduleuse, d'obtenir sans droit un bénéfice économique par soi-même ou par autrui.

Par ailleurs, la fraude informatique « est l'un des délits les plus courants sur interner, car elle peut être automatisée et réalisée avec des logiciels permettant au fraudeur de cacher son identité. Elle comprend la fraude aux enchères en ligne qui consiste à proposer la vente des produits qui n'existent pas et à exiger des acheteurs le paiement avant livraison ; et à faire un achat et à demander d'être livré, avec l'intention de ne pas payer, d'une part, et d'autre part la fraude aux avances sur commission qui consiste à envoyer des courriels qui sollicitent l'aide du destinataire pour transférer des grosses sommes d'argent vers des tiers »[245].

H. La fraude en matière de communication

La fraude en matière de communication consiste à [246] :

- l'exploitation sans autorisation ou sans déclaration préalable d'un moyen de communication ;
- exploitation d'un moyen de cryptologie[247] soit fourni ou fait fournir une prestation de cryptologie sans autorisation ou déclaration préalable ;
- etc.…

I. L'obstruction non intentionnelle aux correspondances par télécommunication

§2. Les infractions facilitées par le NTIC

Les infractions dont la commission est facilitées par les NTIC désigne « des cas où l'informatique n'est qu'un moyen de commission des certaines infractions classiques »[248]. Il s'agit de la criminalité de droit commun, de nature juridique traditionnelle. Ces sont « les infractions prévues par le code pénal et les textes spécifiques »[249].

Par ailleurs, LEMAN souligne que : « ce sont en fait des crimes relativement conventionnels dont les auteurs ont adopté des outils modernes pour arriver à leur fin. On peut s'approprier une infinité de biens physiques, de valeurs symboliques et d'informations confidentielles dans le monde tangible, et l'idée de le faire avec une technologie procurant de nouveau outils et de nouvelles cibles n'est particulièrement difficile à formuler, ni à émettre en pratique »[250].

Somme toute, dans cette hypothèse, l'on comprend que le réseau de télécommunication constitue « qu'un outil ou un moyen pour commettre l'infraction »[251].

Eu égard à ce qui précède, cette catégorie de cybercriminalité est composée de plusieurs infractions. Il s'agit des incriminations énumérées par MANISI[252] et consorts. A savoir :

1. La contrefaçon ;
2. Le faux en écriture ;
3. Le vol ;
4. L'abus de confiance
5. Les tromperies en matière de commerce ;
6. Le harcèlement (cyber-harcèlement) ou le chantage ;
7. Les injures, diffamation et d'attentat ;
8. Les appels téléphoniques malveillants ;
9. L'image contraire aux bonnes mœurs ;
10. Les infractions de presses ;
11. Les infractions militaires ;
12. L'escroquerie ;
13. La production de la pornographie enfantine ;
14. L'offre et la transmission de pornographie enfantine par le biais d'un système informatique ;
15. La diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;
16. La possession de pornographie enfantine dans un système informatique ou au moyen de stockage de données informatiques ;
17. Le fait de se procurer ou de procureur à autrui de la pornographie enfantine par le biais d'un système informatique ;
18. Les atteintes à la propriété intellectuelle ;
19. Les atteintes aux droits connexes à la propriété intellectuelle ;
20. La diffusion des matériels racistes et xénophobe par le biais des systèmes informatiques ;
21. La menace avec une motivation raciste et xénophobe ;
22. L'insulte avec une motivation raciste et xénophobe ;
23. La négation, minimisation grossière, approbation ou justification, du génocide ou des crimes contre l'humanité,
24. L'utilisation des NTIC pour le blanchiment des capitaux (cyber blanchiment) ;
25. L'utilisation des NTIC aux fins de trafic d'armes de destructions massive, trafic de drogue et crimes organisés ;
26. L'utilisation des NTIC à des fins terroristes ;
27. La manipulation de l'information ;
28. La diffusion de l'information dangereuse ;
29. L'utilisation des NTIC dans la fraude fiscale ;
30. Le recel des données.

SECTION 2. TECHNIQUES DE PERPETRATION DE LA CYBERCRIMINALITE

Il faut entendre par technique de perpétration de la cybercriminalité, « les différentes manières

d'actions fréquemment employées par les cyberdélinquants pour arriver à leurs fins »[253]. Ces techniques sont réparties aux infections informatiques (§1), les attaques cybernétiques (§2) et enfin, les arnaques (§3).

§1. Les infections informatiques

1.1. Définition

Les infections informatiques « sont des programmes ou de sous -ensembles de programmes malveillants qui, à l'insu de l'utilisateur, sont destinés à perturber, à modifier ou à détruire tout ou partie des éléments indispensables au fonctionnement normal de l'ordinateur »[254].

Quant à Eric FILIOL, Expert en sécurité informatique, une infection informatique peut être définie comme étant : « une 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 »[255].

Cette dernière définition semble être complète et par conséquent, nous renvoi à l'étude des différents types d'infections.

1.2. Les grandes familles d'infections

Les infections informatiques sont regroupées en deux grandes familles : les infections simples (A) et les infections auto-reproductrices (B).

A. Les infections simples

D'après le CLUSIF : « un programme simples contient une fonctionnalité malveillant caché qui se déclenche ou s'initialise lors de son exécution. Il n'y a pas propagation. En un simple exemplaire, ce programme doit être introduit dans l'ordinateur ciblé. C'est souvent l'utilisateur lui-même qui, par manque de discernement, introduit le programme. Ce processus peut également être le travail d'un virus »[256].

En fait, « l'action introduite peut avoir un caractère destructif ou simplement perturbateur. Elle peut être immédiate ou retardée dans le temps. Dans de nombreux cas, le programme appelé s'installe à l'insu de l'utilisateur et modifie les paramètres du système pour ensuite s'exécute à chaque démarrage de la machine. Il s'agit alors de manière discrète et continue »[257].

Les infections simples sont catégorisées de la manière suivante :

- Les bombes logiques ;
- Les cheveux de Troie ;
- Les portes dérobées ;
- Les outils de capture d'information ;
- Les outils d'attaque réseau ;
- Les outils d'appropriation de ressources.

1. Les bombes logiques

Une bombe logique, « une un programme contenant une fonction destructrice cachée et généralement associée à un déclenchement différé. Cette fonction a été rajouté de façon illicite à un programme hôte qui conservera son apparence anodine et son fonctionnement correct jusqu'au moment choisi par le programmeur malveillant »[258].

2. Cheveux de Troie et portes dérobées

Ce sont des programmes qui permettent d'obtenir un accès non autorisé sur les équipements qui les contiennent. Le terme cheval de Troie est utilisé pour une fonction cachée et rajoutée au sein d'un programme légitime quelconque. Par contre, la porte dérobée s'applique à tout programme malveillant spécifiquement dédié à cet effet.

3. Outils de capture d'information

Il s'agit ici des techniques de collecte d'information. Ainsi donc, nous pouvons classifier les outils utilisés en fonction de l'information recherchée.

A) Renifleur de clavier et de mot de passe

Un renifleur de clavier (Key loger) « est un programme permettant d'enregistrer les frappes au clavier. Son rôle ne se limite pas à l'enregistrement d'éventuels mots de passe »[259]. Il peut être sélectif ou enregistrer l'intégrité des informations qui transitent sur le périphérique de saisie. En effet, « les outils spécifiquement dédiés à la capture de mot de passe prennent souvent la dénomination anglaise de "passwordstealer-PWS" »[260].

b) *Publiciel et espiogiciel*

Ce sont des programmes qui sont installés à l'ordinateur lors de la navigation sur le site web, et ce, à l'insu de l'utilisateur. Ils sont communément appelés"ADWARE et SPYWARE". Celui-ci est un ADWARE qui installe sur le poste de l'utilisateur un logiciel espion et envoie régulièrement et, sans accord préalable, des informations statistiques sur les habitudes de celui-ci.

Par contre, l'ADWARE est un logiciel qui permet d'afficher des bannières publicitaires. La plupart des annonceurs sont juridiquement légitimes et leurs sociétés commerciales reconnues.

4. Outils d'attaque réseau

a) attaque en déni de service (Dos)

A en croire CLUSIF, « en terme de serveur et plus rarement de poste client, une attaque de type DOS, est une activité consistant à empêcher quelqu'un d'utiliser un service. Pour ce faire, l'attaquant utilise un programme qui cherche à rendre le système ciblé indispensable en le faisant suspendre ou en le surchargeant »[261].

Par ailleurs, « en terme de réseau, une attaque de type DOS consiste à submerger la victime d'un flot de trafic supérieur à sa capacité de traitement. La bande passante est alors saturée et le réseau devient indispensable »[262].

b) Attaque en déni de service distribuée (Ddos)

C'est une autre forme de l'attaque DOS, mais utilisant un grand nombre de machines à la fois.

5. Outils d'appropriation de ressources

5.1. Numérateur furtif

En anglais "DIALER", le numérateur furtif est u programme qui gère connexion réseau à distance. Il s'installe souvent de manière silencieuse lors de la navigation web et démarre en même temps que l'ordinateur sans que l'utilisateur en ait connaissance.

5.2. Relais de spam

C'est un programme qui est installé sur la machine à l'insu de son propriétaire. Il permet d'émettre des courriers non sollicités (spam) vers les victimes de spammeurs.

B. Les infections auto-reproductrices

Trésor Gauthier MITONGO pense que : « la famille 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, ce 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 »[263].

Par conséquent, seuls les vers (1) et les virus (2) forment à eux, les programmes auto-reproducteurs, qui constituent le premier niveau des infections informatiques.

1. Le ver (Worm en anglais)

Selon Peter DENNING, un ver « est un programme capable de fonctionner de manière indispensable. Il se propage de machine en machine au travers des connexions réseaux. Un ver ne modifie aucun programme, il peut cependant transporte avec lui des portions de code qui pourront, par la suite, effectuer une telle activité »[264].

2. Le virus

Un virus « est un programme capable d'infecter d'autres programmes en les modifiant de manière qu'ils contiennent une copie de lui-même, parfois évoluée. Il ne transporte pas nécessairement de données, n'est pas toujours délibérément invisible, et ne fonctionne pas obligatoirement de façon dissimulé. De plus, un virus se reproduit »[265].

Somme toute, le virus ne peut pas fonctionner d'une manière indépendante. L'exécution du programme hôte est nécessaire à son activation. En effet, il sied de rappeler que « tout code malveillant à même de se propager est souvent considéré comme un virus. Selon cette théorie, les vers ne sont alors qu'un sous-ensemble dans la famille des virus »[266].

Ainsi donc, nous pouvons catégoriser les virus en quatre types principaux, à savoir:

- Les virus programmes ;
- Les virus systèmes ;
- Les virus interprétés ;
- Les vers qui, comme nous l'avons dit ci-haut, sont des infections réseaux.

§2. Les attaques cybernétiques

2.1. Définition

MITONGO attend par attaques cybernétiques, « l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système, et généralement préjudiciable » [267].

2.2. Catégories d'attaques cybernétiques[268]

Quatre ordres des principales attaques cybernétiques sont retenus. Il s'agit des attaques cryptographiques (A), de déni de service (B), de techniques (C) et attaques web (D).

A. Attaques cryptographiques

Elles sont au nombre de trois, à savoir :

- L'attaque de mot de passe ;
- L'attaque main in the middle ;
- L'attaque par rejet.

B. Attaques déni de service

Ces attaques sont:

- 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 ;
- L'attaque SYN.

C. Attaques techniques

Nous distinguons huit attaques techniques, qui sont :

- L'usurpation de l'adresse IP ;
- Le vil de session TCP ;
- L'attaque du protocole APR ;
- L'analyse réseau ou écoute réseau ;
- Le balayage de ports ;
- L'attaque par débordement de tampon ;
- Le spam, spim ou pollupostage ;
- Le mail bombe.

D. Attaques web

Dans une page web, les attaques suivantes sont fréquentes, à savoir :

- L'attaque par falsification des données ;
- L'attaque par manipulation d'URC ;
- L'attaque cross- site Scripting ou injection de code malicieux ;
- L'attaque par infection de commande SQL.

§3. Les arnaques

Les attaquesconstituent une troisième façon que les cyberdélinquants se servent pour la perpétration de la cybercriminalité. En effet, une arnaque n'est rien d'autre qu'une série de tromperie, d'escroquerie généralement courant dans l'internet.

Cela étant, il existe quatre ordres d'arnaques selon MANASI N'KUSU[269], à savoir : l'ingénierie sociale (3.1), le Scam (3.2), le phishing ou hameçonnage (3.3) la loterie internationale (3.4) et la sextorsion (3.5).

3.1. L'ingénierie sociale

Par ingénierie social, il faut entendre : « une forme d'acquisition déloyale d'information et d'escroquerie utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations »[270]. Il s'agit en fait, « d'une méthode consistant couramment de la part des acteurs, de s'intéresser particulièrement à leurs futurs victimes pas des baratins leur faisant miroiter un avenir somptueux, une générosité sans contrepartie »[271]. Elle est une forme approfondie d'escroquerie.

Cela étant, nous vous proposons dans les lignes qui suivent, un exemple d'ingénierie sociale qui constitue cette arnaque et que nous-mêmes, étions victimes.

Objet : Re:Bonjour Bien Aimé En Christ

From: MOURTH MARINA

To: ***mboyo01@yahoo.fr*** ***(monadresseélectronique)***

Mar 5 at 2:14 AM

Bonjour,

Je me nomme MOURTH MARINA. Née le 31. /…05 /…1938 originaire de la France, hospitalisée dans un hôpital ici à Londres suite à une maladie incurable laquelle mon médecin m'a dit si je croie en Dieu je serais peut être sauvé. Je souffre de la tumeur du cerveau qui se traite depuis plus de 7 mois aujourd'hui. Je ne comprends plus rien de ma vie. Cela vous semblera un peu suspect. Je suis veuve et je n'ai pas d'enfant. Je recherche une âme frère et âme sœur à qui je peuxconfiertous mes biens. Pour qu'il a y aider les orphelins et aux sans-abri. J'ai en ce moment dans une mallette noire, une somme de 250.000,00 € que j'ai déposé dans une BANQUE en Afrique pour ces projets.

C'est un don de Dieu que je vous fais et sans rien vous demander en retour. Émail : (mourthmarina@yahoo.fr)

3.2. Le scam

Le scam est le concept anglais désignant « un type de fraude pratiquée sur internet. Surnommé d'arnaque à la nigérienne ou à la zaïroise. Cette méthode consiste 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 » [272].

Il s'agit d'une technique consistant à l'utilisation des messageries électroniques pour soutirer de

l’argent. Ces genres des messages sont toujours reçus à la boite aux lettre appelée SPAM (courriels indésirables).

Ainsi dit, pour être trop pratique, nous vous proposons le message suivant dont nous même étions victimes au mois de décembre 2013.

Objet : Répond moi s'il te plait

From: ROSE ADER

To: mboyo01@yahoo.fr

Dec 13 at 10:59 PM

Bonjour,

Je suis ROSE ADER, née le 12 Mai 1958.Je désire aider les enfants pauvres et démunies se trouvant dans une situation difficile, et aussi des orphelins. Je suis une patiente en sous observation médical au Centre d’hôpital Elisabeth Queens sise au Grande-Bretagne. J’ai toujours privilégié le service de ma nation au détriment de ma propre santé et voilà aujourd’hui cela me rattrape, mais je suis quand même fière d’avoir pu aider des gens autour de moi et je pense pouvoir continuer à le faire à travers vous. Mais je me demande parfois, Faut- il absolument une raison pour donner ? Et d'abord, que signifie donner ? Quel est le sens du don ? Pour ma part je donne ce que j’ai reçu de la vie et par moi d’autres seront aussi heureux. Ceux qui ne comprendront pas ce que je fais, donnent-ils ? Et que donnent-ils ? Oui je souhaite confier cette lourde responsabilité à une personne physique, anonyme, croyante à mon histoire. Je sollicite votre assistance pour la bonne gestion et bon usage de mes biens d'une somme de 3.025.000 £ (trois million vingt-cinq mille euros) se trouvant auprès d'une banque Béninoise. Je veux que vous m'accompagnez dans vos prières et surtout par mon image vous devenez le père ou la mère des enfants en situation critique, devenir également par mon image le bâtisseur de plusieurs temples de Dieu, des Mosquées, des écoles pour l'alphabétisation des enfants qui n'ont pas la chance d'aller à l'école..

Je vous laisse par ici mon adresse privée pour m’écrire directement.
Adresse E-mail: roseader@yahoo.fr

3.3. Le phishing ou hameçonnage

Pour obtenir des informations personnelles sur les utilisateurs, les cyberdélinquantsont mis aux points différents techniques, qui vont des logiciels espions aux attaques par hameçonnage. L’objectif du hameçonnage est d’amener les victimes à révéler des informations personnelles ou confidentielles. Il est définit comme : « une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer des usurpations d’identité. La technique consiste à faire croire à la victime qu’elle s’adresse à un tiers de confiance-banque, administration, etc…afin de la soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc… »[273].

Diane SERRE et Anne CLUZEAU préconisent que, 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 »[274].

A en croire Trésor Gauthier MITONGO, « ce type d'escroquerie est généralement initié par un message électronique apparemment officiel en provenance d'une source de confiance, 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 exploitées à des fins vol d'identité »[275].

En effet, nous vous proposons un hameçonnage, dont nous étions victimes.

Objet : offre de bourse suisse 2014-2015

*From:**switzerland scholarship***

To: mboyo01@yahoo.fr

Todayat 9:16 am

Par l'intermédiaire de la commission fédérale des bourses étrangères (CFBE-suisse), le secrétariat d'état à l'étude et à la recherche de la confédération lance un appel à la candidature pour 600 bourses d'études suisse au titre de l'année académique 2014-2015. Ces bourses sont destinées aux ressortissants des pays de la catégorie a (pays industrialises européens, et extra-européens) et ceux des pays de la catégorie b (pays en du développement, du tiers monde et extra -européens). Elles doivent leur permettre de poursuivre leurs études, de parfaire leurs connaissances pour les travaux de recherches dans les domaines auxquels les universités Londres accordent une attention particulière.

- avoir au maximum 16 ans a 64 ans ;
- comprendre et parler correctement l'une des langues d'enseignement en suisse (français, espagnol, allemand, anglais, Italie) ;
- avoir un diplôme équivalent au brevet d' étude de premier cycle d'enseignement, au baccalauréat ou au brevet d'aptitude professionnelle

Les candidats retenus recevront une attestation du secrétariat d'état à l'étude et à la recherche pour notification de la bourse. Les candidats désireux de participer aux bourses d'études 2014 – 2015 doivent retirer leur formulaire à remplir auprès de la cfbel: à leur adresse email: direction.boursesuisse@laposte.net

La date limite de dépôt des dossiers est d'une semaine.

3.4. La loterie internationale

La loterie désigne les jeux hasards où l'on tire au sort des numéros gagnants correspondants à des lots. En effet, cette arnaque consiste à la future victime de recevoir un courrier électronique indiquant qu'elle est l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs centaines de dollars.

Par ailleurs, il suffit seulement de réponde. Après une mise en confiance et quelques échanges de courriers, éventuellement avec des attachements aux pièces jointes représentant des papiers attestant que le concerné est bien le vainqueur ou le gagnant heureux, son interlocuteur lui expliquera la procédure à faire pour toucherladite somme, les frais administratifs, de douanes, des taxes diverses sont exigés.

Enfin, nous proposons dans les lignes qui suivent cette pratique dont nous étions victimes au mois de mars 2014.

Objet : Rep: VOTRE REPONSE

COMPAGNIE HEINEKEN

To: mdechavannes@ymail.com

Mar 5 at 11:26 AM

GRANDE TOMBOLA HEINEKEN WEB
1863 - 2013, PLUS DE 150 ANS D'EXISTENCE DE LA COMPAGNIE HEINEKEN
LA HEINEKEN

Le16 décembre 1863 HEINEKEN est créé avec une marque qui dispose d'une forte identité publicitaire, au Royaume-Uni, aux USA, au Canada et plus récemment en Afrique. Sur le marché des bières en Afrique, la marque HEINEKEN est dominante avec 50 % de parts de marché depuis 2000. La HEINEKEN, s'exporte aux quatre coins du globe. Ainsi, la marque HEINEKEN est désormais associée aux valeurs de force, de patience et de bon vivre. Dans le souci unique de faire découvrir et promouvoir son expansion à travers le monde entier depuis sa 150ème Anniversaire, la HEINEKEN organise une tombola pour vous chers internautes. A cet effet, nous avons le plaisir de vous annoncer que vous êtes l'heureux gagnant d'un prix forfaitaire d'une somme de (80000 Euros) à la PROMOTION HEINEKEN portant votre adresse email basé sur l'exercice de la sélection aléatoire des sites web, vous aviez été choisis au hasard parmi plus de 100.000 sites Internet. En outre il faudra confirmer votre identité complète et réclamer votre gain auprès de l'huissier de justice chargé de l'homologation du tirage et de la remise du prix, Maître ALAIN DECHAVANNE en lui envoyant vos informations à l'adresse Email: mdechavannes@rocketmail.com INFORMATIONS PERSONNELLES A ENVOYER A L'ADRESSE EMAIL DU CABINET

NOM : ……..
PRÉNOMS : ……..
SEXE: …… AGE: ……..
PROFESSION: ……..
ÉTAT CIVIL: ……..
PAYS : …… VILLE: ……..
ADRESSE COMPLÈTE /
E-MAIL:.....
N° DE TÉLÉPHONE (Inclure le code du pays) :……..
N° DE QUALIFICATION:.....
Adresse mail à contacter Me mdechavannes@rocketmail.com

Et aussi, il faudrait vous noter que votre Numéro de Qualification est le (CXY 007-0121-baf/2706-08) et peut être demandé dans les échanges de correspondance a effectué avec notre Compagnie HEINEKEN et le Cabinet jusqu'au retrait de votre gain. NB: Date limite d'envois de votre demande de revendication du prix: (01) SEMAINE
Bonne journée à vous.

3.5. La sextorsion : le racket numérique

« La sextorsion (terme né de la contraction de sexe et extorsion), ou encore ***chantage**** à la webcam , peut se définir comme le fait de soutirer de l'argent ou des images à connotation érotique ou pornographique à autrui, sous la menace d'une diffusion d'informations, de photos ou de vidéos personnelles. **Dans tous les cas, le sexe est utilisé pour un chantage »**[276]**.**

En fait, la sextorsion « est un crime qui est extorsion de faveurs sexuelles. Le sextorsion consiste à images à caractère sexuel »[277].

Par ailleurs, « elle appartient à la famille des arnaques à la nigériane, c'est-à-dire des escroqueries par l'intermédiaire de messageries électroniques, abusant crédulité des internautes et dont le but est d'obtenir del'argent ou des données personnelles. Les auteurs de ces abus sont souvent situés en Afrique de l'Ouest (Bénin, Côte d'Ivoire ou Nigeria) et se font appeler « brouteurs ». Les victimes, elles sont désignées sous le terme de *mugu (pigeon*). La grande majorité des victimes de sextorsion sont des hommes»[278].

Ainsi, « le mode opératoire de l'arnaque se déroule en deux étapes.

En premier lieu, la victime est contactée par le biais d'un site de rencontre ou de réseaux sociaux. L'escroc se fait passer pour une femme et propose une discussion intime sur une messagerie instantanée (type Skype), puis un déshabillage de webcam à webcam. Pour mettre en confiance son interlocuteur, l'escroc diffuse l'extrait préalablement volé à la place de l'enregistrement de sa propre webcam, faisant ainsi croire que les images vues par la victime montrent ce qui se passe au domicile de l'arnaqueur. Le prétexte d'un problème de son de la webcam est donné pour tromper la victime »[279].

Lorsque la victime montre des parties de son corps ou effectue certains actes, l'escroc sauvegarde ces images, puis met rapidement fin à la conversation.

En second lieu, « l'internaute reçoit des menaces, bien souvent par E-mail. L'escroc demande l'envoi d'argent par mandat cash, c'est-à-dire transfert de fonds par le biais des services postaux (Western Union ou Moneygram), sous peine de diffuser les images compromettantes qu'il a enregistré. Or, même si la somme demandée est versée, la vidéo est habituellement publiée sur le Net, et se retrouve référencée sur les moteurs de recherche, dont Google. L'extorsion va de quelques dizaines à plusieurs milliers d'euros »[280].

En outre, « si la victime ne coopère pas, de faux mails et documents de la police ou de la justice peuvent aussi être envoyés (par le biais d'adresses de messagerie en yahoo, gmail ou hotmail), avec demande de paiement d'amende. Afin de pousser la victime à céder au chantage, l'escroc peut mentionner la pédopornographie dans le titre de la vidéo qui sera diffusée. De plus, si les coordonnées Facebook de l'internaute sont connues, menace peut être faite de prévenir les proches »[281].

Enfin, il faut toutefois noter que, « cette escroquerie se fonde sur la peur et la honte. La victime craint souvent de passer aux yeux du monde et de ses proches pour un « pervers ». Du fait du caractère intime de l'extorsion, la situation n'est donc pas dénoncée. Cette inquiétude peut se transformer en angoisse, et entraîner une dépression, voire un suicide. Les conséquences, en cas de diffusion de la vidéo peuvent aussi être professionnelles et sociales, car le référencement sur les moteurs de recherche peut amener n'importe qui à tomber sur ces images »[282] .

TITRE TROISIEME : CONSIDERATIONS COMPARATIVES DE LA REPRESSION DE LA CYBERCRIMINALITE EN DROITS CONGOLAS ET FRANÇAIS

Il a été révéler au début de cette œuvre qu'elle tienne compte d'une façon comparatiste en tentant de construire de nouvelles pensées décloissonantes. Elle aborde la compréhension du droit voisin et du sien propre. Dans cette perspective V.MENSBRUGGHE souligne que : « il faut reconnaitre cependant que rien aujourd'hui dans les sciences humaines ne peut avancer sans les passeurs de frontières »[283].

Eu égard à ce qui précède, ce titre aura donc le mérite, comme son intitulé le mentionne clairement, de relever dans ses différents chapitres les ressemblances et les dissemblances en matière de cybercriminalité dans les législations sous examen pour enfin en dégager un rapport unique.

Pour ce faire, nous comparons à tour de rôle le système de répression de la cybercriminalité en RDC (chapitre 1) en droit français (chapitre 2). Enfin, nous formulerons nos perspectives d'avenir pour un système efficient de répression de la cybercriminalité en RDC (chapitre 3).

CHAPITRE PREMIER : LE SYSTEME DE REPRESSION DE LA CYBERCRIMINALITE EN RDC

Dans ce chapitre, la législation congolaise sera présentée par rapport à ses réactions conte la criminalité informatique. Ainsi donc, nous exposerons la qualification des crimes contre les TIC (section 1), la qualification des crimes facilités par les TIC (section 2), et enfin, nous parlerons des autorités judiciaires chargées de la poursuite de la cybercriminalité et l'insuffisance du droit spécifique aux TIC en RDC (section 3).

SECTION 1ère. QUALIFICATION DES CRIMES CONTRE LES TIC

Deux principaux paragraphes vont constituer la pierre angulaire de cette section. Il s'agira de la qualification des cybercrimes en matière informatique (§1) et la qualification des cybercrimes portant atteinte aux télécommunications en RDC (§2).

§1. *Qualification des cybercrimes en matière informatique*

D'après le Professeur AKELE ADAU : « la qualification est une question primordiale du droit spécial à cause du principe de la légalité des délits et des peines. Le juge doit tenir compte des incriminations et des sanctions prévues par la loi »[284].

Pour ce faire, « il doit confronter les faits avec le texte discriminateur pour vérifier et établir que les éléments constitutifs de l'infraction se trouvent bien réunis dans le cas d'espèce »[285].

1.1. Etat de législation spécifique en matière informatique

En RDC, l'activité informatique est régie par l'ordonnance n°87/243 du 22 juillet 1987 portant règlementation de l'activité informatique au zaïre.

Ainsi donc, au terme e l'article 9 de l'ordonnance sus-évoquée : «tout acte accompli à l'occasion d'une application informatique et qui porte atteinte à la sécurité de l'Etat, à l'ordre public ou aux bonnes mœurs, est punissable conformément aux lois pénale en vigueur »[286]. En effet, cette disposition reste l'unique à caractère répressif.

Toutefois, il conviendrait de préconiser que, cette ordonnance quand bien même qu'elle organise l'activité informatique, ne réprime pas particulièrement les infractions ontologiques de l'informatique. Cet article renvoi, la répression aux lois pénales en vigueur, notamment le code pénal, y compris d'autres textes particuliers à caractère répressif. Or, les infractions contenues dans les lois pénales en vigueur sont celles facilités par les TIC et qui feront l'objet de la 2ème section.

§2. Qualification des cybercrimes portant atteinte aux télécommunications en RDC

Les télécommunications font partie intégrante des NTIC, raison pour laquelle, il existe une législation dont il faut ressortir son état (2.1), ainsi que les cybercrimes qui portent atteintes à ces télécommunications (2.2).

2.1. Etat de législation pénale sur les télécommunications

2.1.1. Loi cadre n°013/2002 du 16 octobre 2002 sur les télécommunications en République Démocratique du Congo

A. Dispositions de droit pénal de fond

La loi-cadre sus-évoquée réprime un certain nombre de comportements à l'occasion de l'usage des télécommunications. Cette répression est prévue aux articles 69, 70, 71, 72, 73, 74, 75, 76, 77, 78 et 79.

B. Dispositions relatives au droit procédural

L'article 68 de l'ordonnance sous examen, prévoit une procédure spéciale pour les infractions en matière de communication. Ainsi donc, au terme de l'article sus-mentionné, « les infractions en matière des télécommunications donnent lieu à une procédure de transaction. L'administration peut transiger avec le contrevenant et faire payer une amende transactionnelle dont les taux sont revus périodiquement par le Ministre »[287].

2.2. Qualification des cybercrimes portant atteintes aux télécommunications en droit congolais

La loi-cadre sur les télécommunications catégorise les cybercrimes en deux groupes, d'une part les atteintes aux correspondances (2.2.1) et d'autre part, les atteintes aux règles de cryptologie (2.2.2).

2.2.1. Qualification des cybercrimes portant atteinte aux correspondances

A. Qualification d'altération, soustraction, égarement, détournement, destruction, suspension, retardement, dissimulation et prise de connaissance des correspondances adressées a des tiers

Au terme de l'article 71 de la loi-cadre sur les télécommunication qui dispose que : « quiconque aura altéré, copié sans autorisation, ou détruit toute correspondances émise par voie de télécommunication, l'aura ouvert ou s'en sera emparé pour en prendre indûment connaissance ou aura employé un moyen pour surprendre des communications passées par un service public des télécommunications, sera puni d'une servitude pénale de six mois et d'une amende qui ne dépassera pas cents mille francs congolais constants, ou l'une de ces peines seulement »[288].

B. *Qualification du détournement des correspondances émises, transmises ou reçues par la voie des télécommunications*

Cette qualification est prévue à l'article 72 de la loi-cadre sous examen. Au terme de cette disposition « tout agent au service d'une exploitation de services publics de télécommunications qui aura commis l'un des actes prévus à l'article précédent, ou l'aura facilité ou qui aura intentionnellement omis, dénature ou retardé la transmission d'une correspondances par voie de télécommunication, sera puni d'une servitude pénale d'un an ou plus ou d'une amende ne dépassant pas cents mille francs congolais constats ou de l'une de ces peines seulement »[289].

C. Qualification de l'exploitation du secret de communication

Toute personne désignée à l'article 72, qui hors le cas où la loi les y obligerait, auront révélé ou ordonné de révéler, l'existence ou le contenu d'une correspondance émise par voie de télécommunication, tombe sous le coup de cette cyberinfraction.

En conséquence, « elle est punie d'une servitude pénale de six mois au plus et d'une amende qui ne dépassera pas cents mille francs constants ou de l'une de ces peines seulement »[290].

D. Qualification de l'abatage d'arbres, creusement des fouilles, construction, démolition, dégradation d'une ligne téléphonique

Ce cybercrime consiste à l'élagage ou l'abatage d'arbres, au creusement des fouilles ou des touchées, à des constructions ou démolitions, à tout autre travail susceptible soit de dégrader une ligne téléphonique, soit d'en commettre le fonctionnement.

En effet, « quiconque aura procédé sans avoir averti, au moins huit jours à l'avance l'autorité de la circonscription administrative, laquelle en avise immédiatement l'exploitant des télécommunications sera puni d'une servitude de quinze jours au minimum et d'une amende allant de dix mille à cents mille francs congolais constants ou de l'une de ces peines seulement »[291].

E. Qualification de l'interception illégale des communications privées et radiotéléphoniques ou des correspondances émises, transmises ou reçues par la voie des télécommunications

Selon l'article 75 de la loi-cadre sur les télécommunications, « ceux qui, par défaut de précaution, auront soit gêné ou empêché la correspondance sur la voie de télécommunication d'utilité publique, soit détruit, abattu ou dégradé tout ouvrage ou objet affecté à cet usage, seront puis d'une amende ne dépassant pas cinq mille francs congolais constants »[292].

F. Qualification de destruction, déplacement, renversement ou dégradation des voies ou installations de télécommunications en temps de guerre

« Quiconque aura en temps de guerre détruit, déplacé, renversé ou dégradé par quelque moyen que ce soit, en tout ou en partie, des voies ou installations des télécommunications fixes ou de campagne servant à des buts militaires, soit de son propre gré, soit à l'instigation d'autrui, dans l'intention défavoriser les dessins de l'ennemi, sera puni de la peine capitale »[293].

2.2.2. Qualification des cybercrimes portant atteinte aux règles de la cryptographie

A. Définition de la prestation de cryptographie

On entend par prestation de cryptographie : « toutes prestations visant à transformer à l'aide de convention secrètes des informations ou signaux clairs en informations ou signaux intelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet »[294].

B. Qualification de l'exploitation ou fourniture d'une prestation de cryptographie

« Toute personne qui aura exploité un moyen de cryptographie soit fourni ou fait fournir une prestation de cryptologie sans autorisation ou déclaration préalable est puni d'une servitude pénale d'un mois et d'une amende de dix mille à cinquante mille francs congolais constants ou de l'une de ces peines seulement »[295].

SECTION 2. QUALIFICATION DES CRIMES FACILITES PAR LES NTIC EN DROIT PENAL CONGOLAIS

Nous examinons dans cette section la qualification fondée sur le code pénal congolais, notamment dans ledécret du 30 janvier 1940 tel que modifié et complété à ce jour (§1), et la

qualification des crimes facilités par le NTIC portant atteintes aux autres valeurs en droit congolais (§2).

§1. Qualification du code pénal : décret du 30 janvier 1940 tel que modifié et complété à ce jour

Le code pénal congolais incrimine certains comportements manifestés lors de l'utilisation des nouvelles technologies de l'information et de la communication. Il s'agit en effet, des infractions traditionnelles, des infractions de droit commun, c'est-à-dire « l'ensemble des règles juridiques qui s'appliquent à toutes les situations en dehors des cas particuliers ou spécifiques »[296].

Somme toute, diverses qualifications font l'objet principal de ce point. Il s'agit des atteintes aux personnes (1.1), contre les propriétés (1.2), contre la foi publique (1.3), et la qualification contre la moralité sexuelle (1.4).

1.1. Qualification des atteintes aux personnes

L'internet peut à l'heure actuelle être à la base d'une multitude d'atteintes à l'honneur et à la considération d'une personne soit par des imputations dommageables et des injures, d'une part et d'autre part par l'aversion tribale et raciale.

A. Imputations dommageables et injures

Les imputations dommageables autrement appelées diffamation et les injures sont prévues et réprimées par les articles 74, 75 et 77 du code pénal ordinaire.

En effet, la diffamation suppose « l'imputation d'un fait précis de nature à porter atteinte l'honneur ou à la considération d'une personne ou à l'exposer au mépris »[297].Par contre, « l'injure se consomme par le seul fait d'offenser une personne par des expressions blessantes, outrageantes, par mépris ou invectives »[298].

A.1. Les éléments constitutifs de la diffamation et injure

Les imputations dommageables et l'injure comportent des éléments communs et des éléments propres à chacune d'elles.

A.1.1. Eléments communs

Deux éléments essentiels peuvent être retenus, il s'agit de la publicité et de la catégorie des personnes protégées »[299].

a. La publicité

« Le code pénal congolais ne donne pas la définition de la publicité, il faut comprendre par le terme publiquement en l'employant dans le sens usuels de "en public", c'est-à-dire en présence de plusieurs personnes »[300]. En effet, la publicité est définie, à en croire LIKULIA BOLONGO « d'après les circonstances et les lieux. Ainsi, la publicité peut résulter soit de propos proférés, soit d'écrits ou images distribués, vendus ou exposés dans les lieux ou réunions publics »[301].

Par ailleurs, « par lieux publics, on entend outre les lieux publics par nature, c'est-à-dire affectés à l'usage de tout et accessible à chacun à tout moment (voie publique), les lieux publics par

destination (bureau, salle d'audience, salle de cours et tribunaux, bars) ouvert au public à certain moment déterminé et aussi les lieux publics par accident, privé en principe mais devenant occasionnellement public par le fait de la présence d'un certain nombre des personnes »[302].

Somme toute, dans le cadre de la cybercriminalité, cette publicité ne se traduit pas par les propos mais par les écrits, image et autres moyens. Ainsi donc, s'il s'agit d'un écrit : livre, presse, correspondance ou d'image : dessins, gravures, peintures, emblèmes, l'exposition doit avoir eu lieu dans un lieu public.

Cette publicité se manifeste souvent à l'internet par les écrits adressés à une personne mais adressée également à plusieurs personnes, dont nous citons l'exemple flagrant du réseau social Facebook. Dans le même ordre d'idée, il s'agit aussi de la publication d'une image ou d'un écrit dans un pays, il suffit seulement que la diffusion soit faite au Congo et que, la personne diffamée soit suffisammentdésignée et que cela soit diffusé ou reconnu par plusieurs personnes sur le web. Cette publicité existe aussi dès lors que, les projections de film ont été faites au moyen de la télévision.

b. Les personnes protégées : les particuliers

Il s'agit ici, selon les articles 74 et 75 du code pénal, des personnes. La diffamation ou l'injure doit être dirigée directement ou indirectement contre une personne.

A.1.2. Eléments propres à chacun de ces infractions

a. *Diffamation*

La diffamation existe, chaque fois qu'il existe un fait précis, de nature à causer préjudice à la victime. Ainsi donc, trois éléments sont exigés pour son existence, à savoir :

- Un acte d'imputation ;
- Un fait précis
- Un préjudice.

1. Acte matériel d'imputation

D'après le Professeur AKELE, « imputer un fait à une personne, c'est affirmer que cette personne est l'auteur. En d'autres termes, c'est mettre un fait au compte ou à la charge d'une personne » [303].

2. Un fait précis

Il s'agit ici d'un fait nettement déterminé, c'est-à-dire aussi un fait ui peut faire l'objet d'une preuve. En effet un fait est précis lorsque sa véracité ou sa fausseté peut faire l'objet d'une preuve directe ou indirecte.

3. Le préjudice

La loi exige que le fait précis puisse porter atteinte à l'honneur ou à la considération d'une personne ou susceptible de l'exposer au mépris public. C'est-à-dire tout fait dirigé contre la dignité, la loyauté, l'honnêteté, l'estime ou la morale ; et aussi toute imputation de compromettre

les égards résultant de la position sociale acquise par la victime.

4. L'élément moral

L'élément moral de cette infraction se traduit par le terme employé par la loi : celui qui a méchamment…L'auteur doit être animé par la volonté de nuire ou d'offenser la victime.

5. Régime répressif

La peine applicable est de huit jours à un an et une amende de vingt mille francs ou l'une de ces peines seulement.

b. L'injure

Le législateur de la RDC prévoit deux formes d'injures, simple et publique.

b.1. Eléments commun : élément moral

« L'agent doit avoir agi avec volonté d'offenseur, c'est-à-dire avec l'intention coupable. Il faut *"l'animus injuriandi*" »[304].

b.2. Eléments propres à chacune des injures

a. L'injure publique

Prévue par l'article 75 du code pénal, il suffit que le fait précis soit outrageant ou offensant mais en public.

b. L'injure simple

Prévue par l'article 77, c'est ainsi que tombe sous le coup de cet article, les injures par correspondances, lorsqu'elle n'a pas été répandu ou en public, ou par téléphone. Elle exige un dol spécial. Dans ce cadre, il n'est pas utile que la personne visée soit normalement citée.

b.3. Régime répressif

L'injure publique est punie conformément à l'article 75 du code pénal à une peine de huit jours à 2 mois de servitude pénale et d'une amende n'excédant pas cinq cents francs ou d'une de ces peines seulement. Par contre, l'injure simple, fait puni et prévu par l'article 77 du code sous examen, d'une peine de huit jours et une amende de deux cents francs ou l'une de ces peines seulement.

B. Racisme et tribalisme

1. Définition

Au terme de l'article 1^{èr} de l'ordonnance n°66-342 du juin 1966, qui dispose que : « quiconque, soit par des paroles, gestes, écrits, images ou emblèmes, soit par tout autre moyen, aura manifesté de l'aversion ou de la haine raciale, ethnique, tribale ou régionale, ou aura commis un acte de nature à provoquer cette aversion ou cette haine »[305].

2. Eléments constitutifs du racisme et du tribalisme

Deux éléments doivent être réunis pour l'existence de cette infraction. Il s'agit d'un fait matériel (2.1) et d'un élément moral (2.2).

2.1. Faits matériels

D'après LIKULIA BOLONGO, « matériellement cette infraction se présente sous diverses formes. La première forme est constituée par le fait d'avoir, par paroles, écrits, images, manifesté de l'aversion (mépris, dégout) ou de la haine (animosité, l'hostilité, l'antipathie) raciale, ethnique, tribale ou régionale. Encore peut-il qu'il ait manifestée ou extrémisée. La deuxième forme est tout acte de nature à provoquer cette aversion ou cette haine. La troisième forme se particularise par la participationou maintien d'un cercle, club, association ou un groupement à caractère racial, tribal, … Et la quatrième forme, est constituée par le fait, à titre quelconque, d'assurer ou de continuer d'assurer ou l'administration de l'association tribale à caractère politique »[306].

2.2. Elément moral

C'est la volonté de poser un acte discriminatoire, injurieux ou susceptible de provoquer le désordre ou mieux de troubler l'ordre public.

3. La non dénonciation du racisme

Comme son intitulé l'indique, cette infraction est reprochée à toute personne. Deux éléments sont à retenir pour son existence, à savoir :

3.1. Personne susceptible de commettre cette infraction

A en croire LIKULIA, « la loi punit toute personne qui s'abstient de dénoncer le fait du racisme et du tribalisme. Peu importe, soit un particulier ou un dépositaire de l'autorité publique »[307].

3.2. Un acte matériel d'abstention

Cette infraction se réalise dès le temps où l'agent qui a eu connaissance des faits réprimés s'abstient de les dénoncer à l'autorité judiciaire.

3.3. Elément moral

Lorsque l'agent a agi volontairement et avec connaissance de cause de s'abstenir de dénoncer le racisme ou le tribalisme.

4. Régime répressif

Pour le racisme et le tribalisme, la loi prévoit une servitude pénale d'un mois à deux ans et d'e amende de cinq cents à cent mille francs et d'une de ces peines seulement. En revanche, une servitude pénale de quinze jours à un an et d'une amende de deux cent cinquante à cinquante mille francs ou d'une de ces peines seulement, est prévue pour la non-dénonciation du racisme et du tribalisme.

1.2. Qualification des atteintes contre la propriété

Les NTIC sont aussi à la base de la perpétration de certaines infractions liées à la propriété privée. Il s'agit ici du vol simple (1.2.1), de l'escroquerie (1.2.2), de l'abus de confiance (1.2.3), et enfin, des tromperies sur les choses vendues (1.2.4).

2.1.1. Le vol simple

A. Définition

D'après l'article 79 du code pénal, qui prévoit que : « quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol »[308]. Donc, le vol est la soustraction frauduleuse de la chose appartenant à autrui.

B. Eléments constitutifs

B.1. Eléments matériels

Les éléments matériels du vol sont au nombre de trois : l'acte de soustraction (a), l'objet de soustraction (b), et enfin, l'appartenance à autrui (c).

a. Acte de soustraction

Nous partageons la même opinion avec le Professeur AKELE, lorsqu'il dit à propos de la soustraction que : « sinon pas de vol, car c'est l'élément caractéristique du vol. Il y a soustraction matérielle et juridique. La soustraction matérielle, c'est l'enlèvement ou l'appréhension de la chose, un acte matériel accompli à l'insu ou contre le gré du propriétaire. Par contre, la soustraction juridique intervient quand la chose passe de la possession du légitime détenteur à une simple détention en propriété »[309].

b. L'objet du vol ou la chose susceptible de vol

En principe, seuls les biens mobiliers peuvent faire l'objet du vol. Cependant, une exception se manifeste et veut que, les biens immeubles qui peuvent faire l'objet d'un détachement est susceptible de vol. Il s'agit des immeubles par nature (pierre précieuse, sable, gravier, minerai, etc…), les biens immeubles par incorporation (arbre, fruit, récolte, porte d'une maison, fenêtre, etc…) et les immeubles par destination (animaux, ustensiles).

Cela étant, il s'agit également des immeubles incorporels. Il en est ainsi « des écrits, des disques, des bandes contenant des chansons, un écrit constituant un instrument de preuve »[310].

Il sied de rappeler que, dans le cadre de l'informatique et de la communication, c'est l'acception de l'immeuble incorporels, qui selon nous, est d'application. Il s'agit ici de l'objet du vol des données contenues dans un système informatique, dans un réseau informatique et dans un support de stockage informatique. Fréquemment, c'est le vol des informations sur l'internet, car dans certains sites web, l'appropriation des données doit faire l'objet d'une autorisation préalable, au cas contraire le vol existerait.

c. La chose soustraite doit appartenir a autrui

La soustraction frauduleuse exige que la chose volée puisse appartenir à une personne morale, privée que particulière. Par contre, les choses sans maître et abandonnées ne sont prises en compte.

B.2. Elément moral

L'élément moral est complexe du fait que, il y a là-dedans : « l'intention coupable ou dol général, et un but de s'enrichir au détriment du propriétaire légitime de la chose : dol spécial »[311].

C. REGIME REPRESSIF

Selon l'article 80 du code pénal congolais, qui dispose que : « les vols commis sans violences ni menaces sont puni d'une servitude pénale de cinq ans au maximum et d'une amende de dix mille à deux cents mille francs congolais ou d'une de ces peines seulement »[312].

1.2.2. L'escroquerie[313]

A. Définition

Issue de la compréhension de l'article 98 du code pénal congolais, la définition de cette prévention est : « le fait de se faire remettre volontairement une chose appartenant à autrui, soit en faisant usage d'un faux nom ou d'une fausse qualité soit en employant des manœuvres frauduleuses » [314]. Elle se diffère de l'abus de confiance en ce que la remise de la chose à autrui est obtenue irrégulièrement.

B. Eléments constitutifs

B.1. *Eléments matériels*

Ils sont au nombre de quatre, à savoir :

- L'emploi par l'auteur d'un des moyens indiqués par le législateur (article 98) ;
- L'auteur agit avec mauvaise foi, c'est-à-dire la remise matérielle par la victime de la chose convoitée ;
- La chose, objet de la remise doit être celle qui est déterminée par le législateur ;
- L'emploi des manouvres frauduleuses (publicité mensongère).

Ainsi donc, dans le cadre de cette étude, l'escroquerie est appelée ANARQUE. C'est-à-dire, depuis un certain temps, cette pratique est née pour escroquer les victimes de fonds (argent) tout en usant des fausses qualités (d'une banque, d'une entreprise, d'une conférence, etc…) et aussi en usant des manœuvres frauduleuse sans formes de publicité à des sites faux et inexistants.

B.2. Elément moral

Ici, c'est l'intention frauduleuse, sinon il n'y a pas d'escroquerie.

C. Régime répressif

L'article 98 in fine prévoit que : « …est puni d'une servitude pénale de trois mois à cinq ans et d'une amende dont le montant ne dépasse pas deux mille francs ou d'une de ces peines

seulement »[315].

1.2.3. L'abus de confiance

A. Définition

D'après l'article 95 du code pénal, qui dispose que : « quiconque a frauduleusement détourné, soit dissipé au préjudice d'autrui des effets, deniers, marchandises, billets, quittances de toute nature contenant ou opérant obligation ou décharge et qui lui avait été remis à la condition de les rendre ou d'en faire un usage ou un emploi déterminé est puni d'une servitude pénale de trois mois à cinq ans et d'une amende dont le montant ne dépasse pas mille francs congolais ou d'une de ces peines seulement »[316].

B. Eléments constitutifs

B.1. Conditions préalables

Trois conditions sont à remplir pour l'existence de cette infraction : un contrat, une remise et une chose, objet de remise.

a. Un contrat

On définit le contrat comme étant « un accorde de volonté en vertu duquel la chose a été remise à titre précaire. Autrement dit l'abus de confiance implique la violation d'un contrat translatif de la détention ou de la possession d'une chose »[317].

Par ailleurs, sont générateurs d'abus de confiance[318] :

- Le gage ou le nantissement ;
- Le mandat ;
- Le prêt à usage ;
- Le transport ;
- Le louage de service ;
- Le travail ;
- Le dépôt

Il s'agit dans le cadre de cette étude, de toutes ces catégories des contras susceptibles d'être réalisés au moyen d'internet ou du réseau informatique. Surtout en ce qui concerne le commerce électronique, des offres en lignes et les prestations de service sur l'internet.

b. La remise de la chose

La deuxième condition pour que cette infraction puisse exister, c'est la remise de la chose consistant en une tradition. En effet, le Professeur NYABIRUNGU souligne que : « cette remise doit être volontairement, c'est-à-dire en vertu d'un contrat et à titre précaire. Ceci, pour le détenteur de la rendre et d'en faire un usage ou emploi déterminé par le contrat »[319].

c. La chose objet de remise

Pour qu'il ait l'abus de confiance, il faut réellement une remise de l'un des objets énumérés à l'article 95 du code pénal et qui sont : effets, les deniers, marchandises,billets, quittances, écrits

de toute nature contenant ou opérant obligation ou décharge.

B.2. Les éléments constitutifs

Trois éléments sont à retenir : un acte matériel constitué par le détournement ou la dissipation, un préjudice et l'intention coupable.

B.2.1. Elément matériel

Il s'agit du détournement et de la dissipation. Celle-ci « consiste dans un acte de dissipation mettant l'agent dans l'impossibilité de rendre ou restituer la chose reçue »[320]. Tandis que, « le détournement qui se réalise par l'appropriation de la chose d'autrui »[321].

B.2.2. Le préjudice

Le Professeur LIKULIA aborde que : « l'article 95 du code pénal prévoit que : quiconque a frauduleusement soit détourné, soit dissipé au préjudice d'autres…La loi exige donc que, le détournement ait été commis au préjudice d'autrui. Il peut s'agir des propriétés, des possesseurs ou des détenteurs »[322].

B.2.3. Elément moral

Le détournement et la dissipation doivent avoir été réalisés avec l'intention frauduleuse. En effet, « celle-ci est un élément essentiel de l'infraction d'abus de confiance. Cette intention se traduit de l'impossibilité de restituer la chose ou d'en faire l'usage ou l'emploi déterminé »[323].

C. Régime répressif

L'abus de confiance est puni de trois mois à cinq ans de servitude pénale et d'une amende dont le montant ne dépasse pas cents francs ou d'une de ces peines seulement.

En effet, « le prévenu a le droit de poser certaines fin de non-recevoir. Il s'agit de la novation, de la compensation, de la remise de la dette, de la confusion et de la prescription »[324].

1.2.4. Les tromperies

Deux formes de tromperie sont à retenir :

1.2.4.1. La tromperie sur la qualité de la chose vendue

Elle se définie comme étant « le fait pour le vendeur d'induire l'acheteur en erreur sur la qualité de la chose faisant l'objet de la transaction dans le but de se procurer un bénéfice illicite »[325].

A. Eléments constitutifs[326]

Les éléments constitutifs de la tromperie sur la qualité de la chose vendue sont :

- Un fait de tromperie (duper, abuser,…) ;
- La tromperie doit porter sur une marchandise ;
- La tromperie doit avoir lieu dans une convention ;
- La tromperie doit être réalisée par un des modes prévus par la loi (identité de la chose, nature et origine de la chose) ;
- L'intention coupable.

B. Régime répressif

Cette prévention est puni d'un an au plus de servitude pénale et d'une amende dont le montant ne dépasse pas mille francs, ou d'une de ces peines[327].

1.2.4.2. La tromperie sur la quantité de la chose

A vrai dire, l'internet constitue un milieu virtuel, il est évident que l'acheteur et le vendeur ne soient pas dans un même lieu afin d'évaluer la quantité des marchandises, et cela occasion la tromperie sur la quantité de ces marchandises.

Ainsi donc, trois types d'éléments constitutifs sont à réunir pour l'existence de cette incrimination. Il s'agit notamment :

- De l'emploi des manœuvres frauduleuses ;
- Du but poursuivi qui est la quantité de la chose vendue ;
- De l'existence d'un contrat de vente ;
- Du préjudice subi par la victime ;
- De l'existence de l'intention coupable.

Enfin, cette infraction conserve le même régime répressif[328] que son corollaire, c'est-à-dire la tromperie sur la qualité de la chose vendue.

1.3. Qualification des atteintes à la foi publique

Une seule infraction est retenue quant à la valeur protégée. Il s'agit du faux en écriture.

1.2.1. Faux en écriture

Dans la pratique informatique, cette infraction est fréquente et se commet du jour au jour par les utilisateurs de l'ordinateur. En effet, il s'agit notamment « de l'altération de la vérité dans un écrit de nature à porter préjudice et accompli avec l'intention frauduleuse et à dessein de nuire »[329].

A vrai dire, cette infraction requiert deux éléments constitutifs pour son existence. C'est-à-dire les éléments matériels (A) et moral (B).

A. Elément matériel[330]

Le faux en écriture est constitué par l'altération de la vérité qui consiste en une altération matérielle de l'écrit. La modification de l'écrit peut résulter d'un grattage, d'une surcharge, de la suppression d'une partie du texte, de l'insertion après coup d'une fausse clause, de la fabrication intégrale d'un écrit, de l'opposition d'une fausse signature »[331].

En effet, dans le cadre du présent mémoire, il est loisible de s'attarder sur le faux porté sur un écrit, manuscrit, dactylographie, imprimé ou photographie. L'altération de la vérité doit causer préjudice à la victime.

B. Elément moral

L'intention frauduleuse est requise dans le dessein de nuire au chef de la victime.

C. Régime répressif

Cette infraction facilitée par les TIC est punie par l'article 124 du code pénal d'une servitude pénale de six mois à cinq ans et d'une amende de vingt-cinq à deux mille francs ou d'une de ces peines seulement.

1.4. Qualification des atteintes contre la moralité sexuelle

Pendant nos investigations, quatre types d'infractions ont été retenus quant à la moralité sexuelle facilitée par TIC. On y trouve le harcèlement sexuel (1.4.1), la pornographie mettant en scène des enfants (1.4.2), des attentats à la pudeur (1.4.3) et des outrages publics aux bonnes mœurs (1.4.4).

1.4.1. Le harcèlement sexuel (cyber-harcèlement)

A. Définition

Selon l'article 174 d du code pénal congolais, qui dispose que : « quiconque aura adopté un comportement persistant envers autrui, se traduisant par des paroles, des gestes soit en lui donnant des ordres ou en proférant des menaces ou en imposant des contraintes, soit en exerçant des pressions graves, soit en abusant de l'autorité que lui confère ses fonctions en vue d'obtenir de lui des faveurs sexuelles »[332].

De cette évidence, il convient de noter que le harcèlement commis au moyen de l'internet est appelé cyber-harcèlement. Il s'agit d'un acte d'incitation sexuelle purement psychologique se traduisant par des paroles, des gestes, les ordres, voire même des contraintes.

B. Eléments constitutifs[333]

Deux éléments constitutifs sont à retenir :

- Le fait matériel de harceler qui consiste à tout agissement, tout comportement ou toute attitude qu'une personne aura affichée de manière persistante envers la victime ;
- L'élément morale implique l'agent doit avoir accompli son acte avec une intention coupable.

C. Régime répressif

La loi pénale congolaise prévoit à son article 174 d in fine, une peine de servitude pénale de un à deux ans et d'une amende de cinquante mille à cent mille francs congolais ou d'une de ces peines seulement. En outre, « le harcèlement sur enfant est puni de trois à douze ans de servitude pénale et d'une amende de vingt mille quatre cents mille francs »[334].

1.4.2. Le pornographie mettant en scène des enfants

A. Définition

On entend par pornographie mettant en scène des enfants, « toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes d'un enfant, à des fins principalement sexuelles »[335].

B. Eléments constitutifs

B.1. Eléments matériels

Les éléments matériels de cette infraction facilité par les TIC consiste par le fait « de produire, de distribuer, de diffuser, de vendre, de se procurer…tout matériel mettant en scène un enfant »[336].

B.2. Elément moral

C'est l'intention qu'a l'agent sur l'enfant à des fins sexuelles.

B.3. Régime répressif

Une servitude pénale est prévue à l'article sus-évoqué, d'une peine de cinq à quinze ans principales et d'une amende de deux cents mille à un million des Francs congolais.

1.4.3. L'attentat à la pudeur

A. Définition

L'attentat à la pudeur est défini comme, « tout acte contraire aux mœurs exercé intentionnellement et directement sur une personne sans le consentement valable de celle-ci » [337].

B. Eléments constitutifs

L'élément matériel retenu est l'acte matériel portant atteinte à la pudeur. Il s'agit en fait, de toute action physique ou immédiate contraire aux mœurs exercée sur une personne. En outre, l'agent doit avoir agi consciemment, avec la volonté d'enfreindre la loi, c'est-à-dire l'intention coupable.

C. Régime répressif

Les articles 167 et 168 du code pénal congolais, punis cette infraction de diverses façons, à savoir :

- Une servitude pénale de six mois à cinq ans pour tout attentat à la pudeur sans violences, ruses ou menaces ;
- Une servitude pénale de six mois à cinq ans pour tout attentat avec violences, ruses ou menaces pour les majeurs ;
- Une peine de cinq à quinze ans est prévue pour tout attentat commis avec violences, ruses ou menaces sur la personne ou à l'aide de la personne de moins de dix-huit.

1.4.4. L'outrage aux bonnes mœurs

Toute reproduction de l'immoralité, de l'impudicité et d'obscénité au moyen de l'internet est punie conformément à la loi.

§2. Qualification des crimes facilites par les TIC portant atteintes aux autres valeurs en droit congolais

Il s'agit des délits de presse (2.1) et des atteintes aux droits intellectuels et aux droits voisins (2.2).

2.1. Qualification des délits de presse

D’entrée de jeu, il convient de rappeler que, le délit de presse, est toute infraction quel que soit sa nature, qui se commet par voie de presse. Il s’agit, selon l’article 74 de la loi n°96-002 du 22 juin 1996 fixant les modalités de l’exercice de la liberté de presse, de « toute infraction par voie de presse écrite ou audiovisuel »[338].

Cela étant, les infractions de presse regroupent à la fois, les infractions de droit commun (A) commises par la voie de presse, celles de droit militaire (B) et les infractions relevées dans la loi du 22 juin 1996 (C).

A. Délits de presse et infractions de droit commun[339]

Les infractions de droit commun commises au moyen de presse sont :

- La provocation directe à la désobéissance aux lois ;
- Les outrages envers les membres du parlement, gouvernement et de la cour constitutionnelle ;
- La propagation des faux bruits ;
- Offense envers le chef de l’Etat ;
- Les outrages envers l’emblème ;
- Imputation dommageables ;
- Racisme et tribalisme ;
- Dénonciation et imputations calomnieuse ;
- Etc…

B. Délits de presse et infractions militaires

Les infractions du code pénal militaire du 18 novembre 2002 susceptible de participer au délit de presse sont :

- La provocation à la désertion ;
- L’incitation à commettre l’une des infractions contre le secret de la défense nationale ;
- La participation à une entreprise de démoralisation de l’armée en vue de nuire à la défense nationale;
- La trahison notamment par le fait de livrer ou de rendre accessible à une puissance étrangère des renseignements, procédés, objets, documents…. ;
- Etc…

C. Délits de presse dans la loi du 22 juin 1996[340]

Cette loi prévoit les infractions suivantes :

- De l’incitation au vol, au meurtre, au pillage, à l’incendie ;
- De l’incitation à la discrimination, à la haine ou à la violence à l’égard d’une personne ou d’un groupe des personnes, en raison de leur origine ou de leur appartenance à une ethnie, nation, race, religion ;
- De la provocation des infractions par discours, écrits, imprimés, dessins, gravures, images, emblème ou tout autre support de l’écrit, la parole ou de l’images vendues ou distribuées, diffusées ou exposées dans les lieux ou des réunions publiques ;
- L’incitation des membres des forces armées et des services de l’ordre de se détourner de leur devoir ;
- La publication des actes d’accusation et de tous les autres actes de procédure judiciaire avant qu’ils n’aient été lus en audience ;

- La divulgation des délibérations des cours et tribunaux ;
- L'enregistrement, la fixation ou la transmission sans autorisation de la parole ou de l'image aux audiences des cours et tribunaux ;
- La participation comme auteur à une diffusion ou une émission contraire à la loi, à l'ordre public et aux bonnes mœurs ;
- L'irrégularité de diffusion par non habilitation ou non-respect des formalités administratives….

En effet, pour que ces infractions soient retenues, il faut de la publicité et un élément intentionnel.

2.2. Qualification des atteintes aux propriétés intellectuelles,aux droits d'auteurs et droits voisins

A. Atteintes aux propriétés intellectuelles

La propriété intellectuelle est régie par la loi n°82/001 du 07 janvier 1982. En effet, l'article 88 dispose que : « toute atteinte portée sciemment aux droits du breveté, constitue un délit de contrefaçon qui engage la responsabilité, tant pénale que civile de l'auteur »[341].

Somme toute, selon l'article 93 de la loi sus-mentionnée, « le délit de contrefaçon est passible d'une peine de servitude pénale d'un à six mois et d'une amende dont le montant est fixé par les mesures d'exécution ou d'une de ces peines seulement »[342].

B. Atteintes aux droits d'auteurs et droits voisins

D'après l'article 96 de la loi 86-033 du 05 avril 1986 portant protection des droits d'auteurs et droits voisins, qui dispose que : « toute atteinte méchante ou frauduleuse portée en connaissance de cause aux droits d'auteurs constitue l'infraction de contrefaçon »[343].

Enfin, « la contrefaçon est punie d'une servitude pénale d'un mois à un ans et d'une amende de cinq mille à dix mille francs ou d'une de ces peines seulement »[344].

Toutefois,l'application méchante ou frauduleuse sur un objet d'art, un ouvrage de littérature ou de musique, du nom d'un auteur ou de tout singe distinctif adopté par lui pour désigner son œuvre, sera puni d'une servitude de un à cinq ans et d'une amende de dix mille à cinquante mille ou d'une de ces peines seulement.

SECTION 3. LES AUTORITES DE POURSUITES ET LES JURIDICTIONS COMPETENTES

La présente section aborde d'une part les juridictions congolaises compétentes pour la répression de la cybercriminalité (§2) et d'autre part les autorités chargées de poursuites (§1).

§1. Les autorités de poursuites

En RDC, l'autorité de poursuite est le Ministère public. Ainsi, en matière répressive, « le Ministère public recherche les infractions aux actes législatifs et règlementaires qui sont commises sur le territoire de la République. Il reçoit les plaintes et les dénonciations, accomplit tous les actes d'instructions et saisit les cours et tribunaux »[345].

§2. Les juridictions compétentes

La justice est rendue en RDC, par les cours et tribunaux. Il s'agit des juridictions de droit commun d'une part et d'autre par les juridictions spéciales.

A. Juridictions de droit commun

On peut citer :

- Le tribunal de paix ;
- Le tribunal de grande instance ;
- La cour d'appel ;
- La cour de cassation.

B. Juridictions spéciales

Sont classées dans cette catégorie, les juridictions suivantes :

- Le tribunal pour enfant ;
- Les tribunaux militaires ;
- La cour militaire ;
- La haute cour militaire.

CHAPITRE DEUXIME : LE DROIT FRANÇAIS FACE A LA CYBERCRIMINALITE

Ce chapitre aura le mérite d'analyser sous deux sections, la qualification de la cybercriminalité en droit français (section 1) et les organes français de lutte contre cette criminalité ainsi que les juridictions chargées de la répression (section 2).

SECTION 1ère : QUALIFICATION DE LA CYBERCRIMINALITE EN DROIT FRANÇAIS

La qualification de la cybercriminalité en droit français, nous renvoie directement à réfléchir sur l'état de la législation en matière informatique et de communication (§1), sur la qualification des crimes contre les TIC (§2) et sur la qualification des crimes facilités par les TIC (§3).

§1. Etat de la législation en matière informatique et de communication[346]

Le législateur français commencé à percevoir l'informatique comme un instrument criminogène à partir des années 78. Dans ce contexte, de nombreux textes furent adoptés ces dernières années avec la volonté de créer un arsenal juridique sur la cybercriminalité. Sans se vouloir exhaustif, on peut citer :

1.1. La convention Européenne sur la cybercriminalité et le protocole additionnel, relatif a l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques

La convention sur la cybercriminalité « a été adoptée par le Conseil de l'Europe à Budapest (Hongrie) le 08 novembre 2001 et ouvert à la signature le 23/11/2001. Cette convention est le premier instrument de droit international conventionnel contraignant spécifiquement élaboré pour lutter contre la criminalité affectant les systèmes, réseaux et données informatiques »[347].Elle est entrée en vigueur le 1èr juillet 2004 et elle est le premier traité international sur les infractions pénales commises via l'internet et d'autres réseaux informatiques.

Par ailleurs, en France, la convention ainsi que son protocole additionnel a été ratifie par la loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la convention du Conseil de l'Europe, qui est entrée en vigueur en France le 23 mai 2005. Elle a comme objectif :

- L'harmonisation des législations des Etats signataires ;
- La modernisation en matière de la procédure ;
- L'amélioration de la coopération internationale en matière d'entraide répressive et l'extradition.

Il sied de noter que, la présente convention européenne dont fait partir la France, incrimine quatre types d'infractions, à savoir :

- Les infractions informatiques : falsification et fraude informatique ;
- Les infractions de contenu : la pornographie enfantine (Le Protocol additionnel inclut la propagation via internet d'idées racistes et xénophobes) ;
- Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le partage non autorisé via internet des œuvres protégées ;
- Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données ou des systèmes.

1.2. Loi relative à l'informatique, aux fichiers et aux libertés

Il s'agit de la loi n°78-17 du 06 janvier 1978. En effet, « le législateur de 1978 a entendu protéger le citoyen contre la collecte et l'utilisation abusive de renseignement sur lui »[348]. Ainsi donc, cette loi crée les incriminations suivantes :

- Création d'un fichier clandestin ;
- L'enregistrement ou de la conservation illicite d'information illicite ;
- La divulgation volontaire ou par imprudence, à des tiers d'informations nominatives ;
- Le détournement d'informations nominatives de leur finalité.

Il faut donc rappeler que, les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du nouveau code pénal[349].

1.3. La loi Godfrain du 05 février 1988 relative a la fraude informatique

La loi n°88-19 du 05 janvier 1988 relative à la fraude informatique a introduit les articles 323-1 à 323-7 dans le code pénal français.

1.4. La loi du 15 novembre 2001 relative à la sécurité quotidienne

Cette loi « a posé le principe de la conservation pour une durée d'un an des données de connexion des abonnés par les opérateurs de téléphonie fixe et mobile et aux fournisseurs d'accès à l'internet pour les besoins d'une procédure pénale. La loi permet aux autorités judiciaire de disposer des moyens aux fins de procéder à un cryptage des données »[350].

1.5. La loi du 21 juin 2004 pour la confiance dans l'économie numérique

Elle a modifié les articles 323-2 et suivants du code pénal. Cette loi a en outre modifié l'article 94 du code de procédure pénale relatif à l'inclusion des données informatiques dans la liste des pièces susceptibles d'être saisies lors de la perquisition réalisées en flagrant délit ou au cours d'une instruction »[351].

1.6. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme

« C'est la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers »[352]. En effet, « avec cette loi, l'obligation de conservation et de communication à la justice des données techniques a été élargie aux cybercafés et aux bornes wifi »[353].

1.7. La loi du 1ère aout 2006 relative au droit d'auteur et aux droits voisins

La présente loi vise à préserver les droits des créateurs. L'offre de moyens illicites de mise à disposition du public d'œuvres ou objets protégés est réprimée. Les éditeurs et les distributeurs de logiciels dédiés ou utilisés dans ce but sont désormais passibles du délit de contrefaçon.

§2. Qualification des crimes contre les TIC

En droit français, la cybercriminalité est réprimée par le code pénal qui organise d'une part les atteintes à la personnalité ; et d'autre part des atteintes aux systèmes de traitement automatisé des données ainsi que les atteintes aux intérêts fondamentaux de la nation.

2.1. Qualification des atteintes à la personnalité

2.1.1. Qualification de l'atteinte au secret des correspondances (interception)

Constitue l'infraction de l'atteinte au secret des correspondances, « le fait commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à la destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance »[354].

En outre, il s'agit « du fait commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »[355].

Ces deux infractions sont punies d'un an d'emprisonnement et d'une amende de quarante-cinq mille euros.

2.1.2. Qualification des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

Selon l'article 226-16 du code pénal français, qui dispose que : « le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de trois cents mille euros d'amende »[356].

L'article 226-7-1 prévoit que : « le fait pour un fournisseur de service de communication de ou pas procéder à la notification d'une violation de données à caractère personnel à la commission

nationale de l'informatique et des libertés ou l'intéressé est puni de cinq ans d'emprisonnement et de trois cents euros d'amende »[357].

En outre, constitue l'atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques[358] :

- Le fait, de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ;
- Le fait, de procéder à un traitement de données à caractère personne concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commercial, ou lorsque cette opposition est fondée sur des motifs légitimes ;
- Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui directement ou indirectement, fait apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celle-ci ;
- Le fait, de conserver les données à caractère personnel au-delà de la durée prévue par la loi ou le règlement ;
- Le fait, pour toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité ;
- Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'identité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ;
- Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personne faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la communauté européenne.

En somme, toutes ces atteintes sont punies de « cinq ans d'emprisonnement et de trois cents mille euros d'amende »[359].

2.2. Qualification des atteintes aux intérêts fondamentaux de la nation

Seul le sabotage a été retenu à titre d'infraction informatique.

2.2.1. Le sabotage

A. Définition

L'article 411-9 alinéa 1 du code pénal français définit le sabotage comme étant : « le fait de détruire, détériorer ou détourner tout document, matériel, construction, équipement, installation, appareil, dispositif technique ou système de traitement automatisé d'information ou d'y apporter des malfaçons »[360].

B. Régime répressif

Une peine de quinze ans de détention criminelle et une amende de deux cent vingt-cinq mille euros sont prévus. La même infraction est punie de deux ans d'emprisonnement et d'une amende de trois cents mille euros, lorsqu'il est commis dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger.

2.3. Qualification des atteintes aux systèmes de traitement automatise des données

2.3.1. Qualification d'atteinte à l'intégrité des donnes

Cette infraction est punie d'après l'article 323-3 du code pénal sous examen, qui prévoit que : « le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de sept mille cinq cents euros d'amende »[361].

2.3.2. Qualification d'atteinte à l'intégrité des systèmes

L'alinéa 2ème de l'article sus-évoqué dispose que : « lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et de cents mille euros d'amende » [362].

En outre, « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de septante-cinq mille euros d'amende »[363].

2.3.3. Qualification d'abus de dispositif

L'article 323-3-1 prévoit que : « le fait, sans motif d'importer ou détenir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adoptés pour commettre une ou plusieurs infractions prévus par les articles 323-1 à 323-3 est puni des peines respectivement par l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée »[364].

2.3.4. Qualification d'accès illégal

Par l'accès illégal, il faut entendre « le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données »[365]. De ce fait, cette infraction est punie de deux ans d'emprisonnement et de trente mille euros d'amende.

2.3.5. Qualification des infractions informatiques (falsification et fraude informatique)

La loi pénale française intervient ici, lorsqu' l'on accède ou maintien, frauduleusement dans tout ou partie du système et cela résulte « soit la suppression ou la modification des données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de quarante-cinq mille euros d'amende »[366].

2.3.6. Qualification des infractions se rapportant a la pornographie enfantine

Cette qualification est prévue par le code pénal, spécialement dans son article 227-23. En effet, elle consiste par le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de septante-cinq mille euros d'amende.

Par contre, le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à cents mille euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentationdu mineur à destination d'un public non déterminé, un réseau de communication électronique.

Ainsi, le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et de trente mille euros d'amende.

2.4. Qualification des infractions issues du code de la propriété intellectuelle

Le code de la propriété intellectuelle français prévoit en soi plusieurs infractions. Mais la matière étant vaste, nous allons se baser que dans quelques-unes.

- ***Article L335-1 CPI***

Toute édition d'écrits, de composition médicale, de dessin, de peinture ou de toute autre production, imprimé ou gravé en entier ou partie, au mépris des lois et règlement relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon, est un délit puni de trois ans d'emprisonnement et de trois cents mille euros d'amende.

- ***Article L335-1 CPI***

Est puni de trois ans d'emprisonnement et de trois cents mille euros d'amende le fait :

1. d'édicter, de mettre à la disposition du public ou de communiquer au public, sciemment ou sous quelque forme que ce soit, un logiciel manifestement destiné à la disposition du public non autorisée d'œuvres ou d'objets protégés ;
2. d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au premier point.

§3. Qualification des infractions facilitées par les NTIC

Plusieurs infractions réprimées par le code pénal français sont commises par le biais des nouvelles technologies de l'information et de la communication. De ce fait, les infractions ci-dessous ont été sélectionnées dans cette catégorie, à savoir :

- Actes racismes et xénophobes
- harcèlement sexuel ;
- Vol ;
- Escroquerie ;
- Abus de confiance ;
- Blanchiment des capitaux ;
- Dénonciation calomnieuse ;
- Terrorisme
- Diffusion des messages à caractère violent ;
- Chantage ;
- Faux en écriture,

- Etc…

SECTION 2. LES ORGANES FRANÇAIS DE LUTTE CONTRE LA CYBERCRIMINALITE ET LES JURIDICTIONS COMPETENTES

La présente section aborde d'une part les organes français de lutte contre la cybercriminalité (§1), et d'autre part, les juridictions compétences pour sa répression (§2).

§1.les organes français de lutte contre la cybercriminalité

A. Au niveau national[367]

La cybercriminalité est reconnue par beaucoup d'experts comme étant la nouvelle forme de criminalité du 21ème siècle. Dès lors, pour la contrôler, la France a mis en place de nouveaux organes de lutte. En voici quelques exemples :

1. Service Technique de Recherches Judiciaires et de la Documentation, crée en 1998 au sein de la gendarmerie (STRJD) ;
2. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLTIC) crée le 15 mai 2000 au sein de la direction centrale de la police judiciaire du Ministère de l'intérieur ;
3. Office Central de Répression des Violences aux Personnes (OCRVP) crée en 2006 pour lutter contre la pédopornographie sur internet ;
4. Service de l'Informatique et des Traces Technologiques (SITT) ;
5. Investigateurs en Cybercriminalité, qui sont les directions inter-régionales et régionales de police judiciaire (ICC) ;
6. Brigade d'Enquête sur les Fraudes aux Technologiques de l'Information (BEFTI).

B. La coopération internationale

Les Etats européens ont rapidement compris que pour être efficace, la lutte contre la cybercriminalité devrait être européenne. Ainsi donc, plusieurs organes ont été créés, entre autre :

1. International police (INTERPOL) : crée le 7 septembre 1923 dans le but de promouvoir la coopération policière internationale. C'est une organisation internationale de police criminelle (OIPC) ayant pour siège dans la ville de Lyon en France ;
2. Eurojust, organe de l'Union Européenne ayant pour compétence l'amélioration de l'efficacité des autorités compétentes des Etats membres dans la lutte contre la criminalité organisée transfrontière, donc la cybercriminalitétransnationale ;
3. Enisa, Agence Européenne chargée de la sécurité des réseaux et de l'information ;
4. Safer Internet Plus, programme européen qui lutte contre les contenus illicites, le traitement des auteurs non désirés et préjudiciables, et qui fait lapromotion d'un environnement plus sûr.

§2. Les juridictions compétences pour la répression de la cybercriminalité

Il a été constaté que, en droit français, les infractions cybernétiques sont punissables soit d'un an, cinq ans, sept ans ou de quinze ans d'emprisonnement et d'une amende. Par conséquent, les juridictions suivantes restent compétentes. A savoir :

2.1. Le tribunal correctionnel

Ce tribunal « juge les auteurs des délits, c'est-à-dire lorsqu'il risque une peine d'emprisonnement (10 ans au maximum) ou une amende »[368].

2.2. La cour d'assise

Elle est compétente pour ce qui est du crime, celui-ci est puni d'une peine afflictive ou infamante. Il s'agit de la réclusion criminelle[369] à perpétuité ou à temps et la détention criminelle à perpétuité ou à temps, qui est une peine politique de privation de liberté.

2.3. La cour de cassation[370]

La Cour de cassation intervient lorsqu'un plaideur a fait l'objet d'un jugement qui ne lui a pas donné satisfaction et qui n'est pas, ou plus, susceptible d'appel. Le recours en cassation, qui s'exerce au moyen d'un pourvoi, n'est donc possible que contre une décision rendue par une juridiction du premier degré statuant en premier et dernier ressort, ou contre une décision rendue en deuxième instance par une cour d'appel. Dans le premier cas, le plaideur forme un pourvoi en cassation contre le jugement du tribunal ; dans le second cas, son pourvoi est formé contre l'arrêt de la cour d'appel.

La Cour de cassation n'est pas un troisième degré de juridiction. En effet son rôle n'est pas de réexaminer les faits d'une affaire, qui sont établis définitivement. Elle a pour mission de déterminer si le tribunal ou la cour d'appel dont la décision est attaquée ont interprété et appliqué aux faits les règles de droit (lois, règlements, etc.) de manière correcte. La Cour de cassation est le juge du droit, et non du fait.

CHAPITRE TROISIEME : LES PERSPECTIVES POUR UN SYSTEME EFFICIENT DE REPRESSION DE LA CYBERCRIMINALITE EN REPUBLIQUE DEMOCRATIQUE DU CONGO

A en croire le Professeur R-B MANASI N'KUSU, lorsqu'il précise que : « face à un tableau aussi sombre, le droit pénal congolais doit chercher la parade, aussi bien sur le plan interne que sur le

plan international, en agissant tour à tour sur les textes légaux que sur les structures des organes chargés de la prévention et de la répression des crimes »[371].

En conséquence, quelques pistes de solution sont annoncées tant sur le plan international (section 1) que sur le plan national (Section 2).

SECTION 1. AU NIVEAU INTERNATONAL

Pour mener, en priorité une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace sur base des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques ; et pour la nécessité d'une coopération entre la RDC et d'autres Etats, il est de besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information.

A cela, nous proposons au gouvernement congolais, comme le cas de son homologue sud-africain, de ratifier la convention européenne sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest en Hongrie. Laquelle convention prévoit les mesures pénales de fond et procédurales ; y compris, le protocole additionnel à la convention sus-évoquée relatif à l'incrimination d'actes de nature raciste et xénophobe, adopté à Strasbourg (France) le 28 janvier 2003.

SECTION 2. AU NIVEAU NATONAL

Pour adapter la législation congolaise à la nouvelle forme de criminalité qui ronge toute l'humanité, le législateur doit bien se focaliser tant sur le droit pénal de fond (§1) qu'au niveau du droit pénal de forme (§2).

§1. Au niveau du droit pénal de fond

Le droit pénal congolais mérite d'être révisé (1.1). Toutefois, certaines nouvelles règles spécifiquement liées aux NTIC doivent être adoptées (1.2), et ainsi abrogée la loi sur l'informatique de 1987 (1.3).

1.1. Révision du code pénal et ajustement des certaines infractions

Le code pénal congolais, notamment le décret du 30 janvier 1940 doit être actualisé et mis à jour afin d'ajuster certaines infractions qu'il édicte et ayant des liens avec la cybercriminalité. Il s'agit de :

- L'élargissement de la définition du vol au vol d'information ;
- L'élargissement de la définition de la trahison et espionnage aux valeurs informatiques ;
- L'élargissement de la notion du faux en écriture au faux en informatique ; et falsification informatique ;
- L'élargissement de la définition de recel d'objet au recel d'information ;
- L'élargissement de la définition de l'escroquerie à l'escroquerie d'information ;
- L'élargissement des fraudes à la fraude informatique ;
- L'élargissement de harcèlement au cyber-harcèlement.

1.2. Adoption des infractions spécifiques aux NTIC

Sur ce point, le législateur congolais doit :

- Adopter une loi reprenant toutes les infractions qui portent atteintes aux NTIC, c'est-à-dire une loi relative à la cybercriminalité ;
- Adopter des lois, comme son homologue français, relatives à l'informatique, aux fichiers et aux libertés et à l'économie numérique.

1.3. Abrogation de l'ordonnance de 1987

Plusieurs innovations sont observées à ce jour, par conséquent, nous proposons au législateur congolais de supprimer son droit positif, c'est-à-dire d'éliminer sur l'arsenal juridique congolais, l'ordonnance n°87/243 du 22 juillet 1987 portant règlementation de l'activité informatique en République du Zaïre, car elle ne s'adapte plus aux réalités technologiques actuelles et qui selon nous, sa présence reste en désuétude.

§2.Au niveau du droit pénal de forme

Au niveau de la procédure, nous suggérons au gouvernement congolais ce qui suit :

- D'insérer dans le code de procédure pénale, des règles relatives à la preuve électronique ;
- De créer une institution administrative chargée de gérer les libertés des personnes vis-à-vis de l'informatique ;
- De créer d'autres structures d'enquête policière en matière de cybercriminalité, c'est-à-dire la police informatique ;
- De renforcer la capacité des structuresexistences, notamment les services de la police judiciaire,
- De recycler le personnel judiciaire, notamment les avocats, les défenseurs judiciaires, les magistrats, greffiers, etc… ;
- D'insérer dans l'enseignement supérieur et universitaire, notamment dans la faculté de droit, un département du droit pénal et la cybercriminalité ; ainsi que les cours relatifs au droit de l'informatique et de la communication (NTIC).

CONCLUSION GENERALE

Nous voici au terme de notre mémoire qui aporté sur ***l'étude comparative de la répression de la cybercriminalité en droits congolais et français.***

Il était question dans cette étude d'identifier les divergences et les convergences entre les deux systèmes juridiques. En effet, notre inquiétude résidait dans la question de savoir s'il existe un système de répression de la criminalité informatique dans les deux législations, c'est-à-dire procéder à l'étude minutieux des mécanismes juridiques prévus en droits congolais et français pour la lutte et l'éradication du fléau à caractère nouveau, que l'on nomme *"la cybercriminalité".*

Ainsi pour y parvenir, nous avons utilisé les méthodes exégétique, comparative, sociologique et la technique documentaire pour la collecte de données.En effet, l'essentiel de ce travail a été exposé en deux parties. La première à essayer de confronter la valeur du principe de la légalité criminelle face à la cybercriminalité et ensuite, la deuxième s'est focalisée sur les technologies de l'information et de la communication ainsi que leur usage, l'issue de la cybercriminalité.

De ce fait, dans la première partie, il a été retenu que le principe de la légalité criminelle est pris en otage car, 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 dansl'arsenal juridique pénal. Logiquement, ces crimes échapperaient à toute poursuite judiciaire parce qu'elles ne sont pas encore érigées en infractions. Cet 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

Pour dire que dans notre droit moderne, il n'y a pas d'infraction ni des peines sans un texte légal. C'est qui ressort du principe de la légalité des délits et des peines, qui a été développé par César BECCARIA au 18ème siècle. Il s'agit donc, d'un principe plus important du droit pénal car seuls peuvent faire l'objet d'une condamnation pénale, que les faits déjà définis et sanctionnés par le législateur au moment où l'accusé a commis son acte et seuls peuvent leur être appliquées les peines édictées à ce moment déjà par le législateur, *nullumcrimennullapoena sine lege*. Ainsi donc, dans le cadre de la cybercriminalité, l'étude de ce principe se justifie dans la mesure où, il y a une nécessité de la politique criminelle qui consiste à la loi d'avertir avant de frapper, il permet également de limiter le droit de punir et il reste un rempart contre l'arbitraire du pouvoir.

Amorçant la seconde partie, à laquelle, les technologies de l'information et de la communication ont été au centre de notre étude, nous avons compris que l'expression TIC nageait dans un contour assez flou. En dépit d'une définition unanime, les TIC sont un ensemble des technologies parmi lesquelles figurent souvent l'ordinateur et qui, lorsqu'elles sont combinées ou interconnectées, permettent de numériser, de rendre accessible et de transmettre, en principe à n'importe quel endroit, une quantité quasi illimité et très diversifiée de données. Les TIC sont constituées de trois secteurs, à savoir : l'électronique, l'informatique et la télécommunication. En effet, cette étude n'intéresse que les deux derniers secteurs.

Par ailleurs, les TIC apportent bel et bien des changements dans les sociétés partout dans le monde, elles améliorent la productivité des industries, révolutionnent les méthodes de travail et remodèlent les flux de transfert des capitaux, en les accélérant. Or, cette croissance rapide a également rendu possible des nouvelles formes de criminalité liées à l'utilisation des réseaux informatiques, appelées *cybercriminalité, cyberbanditisme, cyberdéliquance, criminalité de hautes technologies ou criminalité des NTIC*.

Somme toute, la cybercriminalité constitue les infractions des NTIC. Elle ne définit pas à elle seule une infraction, mais un ensemble d'atteintes aux biens ou aux personnes commises via l'utilisation des nouvelles technologies. Autrement définit, la cybercriminalité regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement

connecté sur le réseau. C'est une criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale.

Par conséquent, à l'heure actuelle la cybercriminalité regroupe deux types d'infractions, d'un part les infractions pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit et d'autre part les infractions dont la commission est facilitée par les NTIC. Il s'agit ici des infractions de droit commun, de nature traditionnelle. Ce sont les infractions prévues par le code pénal et elles prévues dans des textes pénaux spécifiques.Ces différentes infractions sont perpétrées de diverses manières, soit par les infections informatiques, regroupant les infections simples et les infractions auto-reproductrices ; soit également par les attaques cybernétiques, qui sont l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système, et généralement préjudiciable ; et enfin, par les arnaques, caractérisées par l'ingénierie sociale, le scam, le hameçonnage et la loterie internationale.

Au regard des considérations comparatives de la répression de la cybercriminalité en droits congolais et français, il faut simplement retenir qu'en droit français, le législateur a pu trouver des solutions pour l'éradication de ce fléau depuis les années 78, notamment en adoptant la loi relative à l'informatique, aux fichiers et aux libertés, insérant ainsi quelques articles dans le code pénal français. Ensuite, la loi Godfrain du 05 février 1988 relative à la fraude informatique, insérant en son tour, quelques articles dans le même code pénal. Par ailleurs, la France fait partir de la convention européenne sur la cybercriminalité du 23 novembre 2001 ainsi que des diverses lois en la matière.

Ainsi donc, le droit français réprime, les infractions ontologiques de la cybercriminalité, notamment les infractions contre la confidentialité, l'intégrité et la disponibilité des données, et systèmes informatiques ; les infractions informatiques, les infractions liées aux atteintes à la propriété intellectuelle et aux droits voisins. Hormis ces infractions, le code pénal français réprime également, quelques infractions facilitées par les NTIC, c'est-à-dire les infractions de droit commun ou de nature traditionnelle.

En outre, sur le plan organisationnel, nous avons compris que la France est dotée des plusieurs organes chargés de lutter contre la cybercriminalité tant au niveau national qu'au niveau international.

Quant au droit congolais, la législation pénale congolaise relative aux NTIC est composée d'une loi, en l'occurrence de la loi cadre n°13/2002 du 06 octobre 2002 sur les télécommunications et d'une ordonnance n°87/243 du 22 juillet 1987 portant règlementation de l'activité informatique au Zaïre. Par ailleurs, cette législationréprime six infractions ontologiques de la cybercriminalité, qui apparait inappropriée, inadaptée et trop rudimentaire à la réalité évolutive des NTIC. En effet, face à cette déficience juridique, certaines dispositions du code pénal et d'autres lois particulières ont été retenues à titre des infractions facilitées par les NTIC.

De ce qui précède, il a été constaté l'inexistence en droit congolais de toutes les règles de coopérations internationales contre la cybercriminalité, la non adoption des nouvelles lois capables de régir les NTIC et leurs criminalités ; la non adhésion à la convention européenne sur la cybercriminalité comme son homologue sud-africain ; l'inefficacité des sanctions en vigueur en droit pénal congolais, l'insuffisance des organes chargés de lutter contre ce fléau.

Comparativement, et par rapport au droitfrançais, le droit pénal congolais accuse son inefficacité à réprimer la cybercriminalité, ce qui affirme notre hypothèse et fait appel à un système efficient. Raison pour laquelle, nous suggérons au législateur congolais de s'adhérer à la convention européenne sur la cybercriminalité ainsi que sur son protocole additionnel pour ainsi assoir sa coopération internationale avec d'autres pays ; procéder à la révision du code pénal tout en

ajustant certaine infractions, c’est-à-dire adopter des lois nouvelles et spécifiques au TIC, notamment sur la cybercriminalité, abroger l’ordonnance de 1987 qui ne s’adapte plus à la réalité congolaise actuelle, et enfin, au niveau de la procédure, créer d’abord quelques institutions spécifiques chargées de lutter contre ce fléau tout en renforçant aussi l’efficacité des structuresexistantes, recycler le personnel judiciaire dans la lutte contre la cybercriminalité et aussi, créer au sein de la faculté de droit, un département de la cybercriminalité et quelques cours liés au droit de l’informatique.

Au demeurant, vue que toute œuvre humaine a toujours été imprégnée d’imperfection et en reconnaissant que nous n’avons pas épuisé toutes les notions et matières relatives à notre sujet d’étude sur la cybercriminalité par rapport à sa diversité, nous invitons tous chercheurs ayant un gout envers ce sujet à nous compléter.