REPUBLIQUE DU SENEGAL

Un Peuple Un But –Une Foi

MINISTERE DE L'ENSEIGENEMENT SUPERIEURE ET DE LA RECHERCHE

****

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR

****

FACULTE DES SCIENCES JURIDIQUES ET POLITIQUES

MEMOIRE

En vue de l'obtention du diplôme de Master Recherche Droit Privé

SUJET :

LA POLITIQUE PENALE SENEGALAISE A L'AUNE DE LA CYBERCRIMINALITE

Présenté par :
Mr. Mouhamed Tall

Sous la direction de :
Dr. Thierno Amadou Ndiogou
Maitre-Assistant à la FSJP-UCAD

Année Universitaire: 2017/2018

Avertissement

La faculté des Sciences Juridiques et Politiques n'entend donner aucune approbation ou improbation aux opinions émises dans ce présent mémoire. Celles-ci doivent être considérées comme propres à leurs auteurs.

Remerciements

« Aucun de nous, en agissant seul ne peut atteindre le succès »

Nelson Mandela, discours d'investiture le 10 mai 1994.

Par cette citation, je voudrai remercier tout le corps professoral et administratif de la faculté des Sciences Juridiques et Politiques (FSJP/UCAD). Particulièrement aux enseignants qui depuis la 1ère année, n'ont cessé de nous accompagner en nous dispensant un enseignement de qualité, malgré les obstacles liés aux manques de moyens logistiques, documentaires, etc.

Je remercie profondément mon encadreur, Monsieur Thierno Amadou Ndiogou, enseignant chercheur, pour l'attention portée à mon travail. Je salue votre sens de l'écoute, du respect et de la disponibilité à mon égard, que Dieu vous accompagne

Ma profonde gratitude va à l'endroit de mon père et de ma mère qui m'ont été d'un soutien moral et matériel permanent et indéfectible à la réalisation de ce mémoire.

Mes remerciements s'adressent à :

A mon grand frère Papa Diagne Tall, qui s'est investi financièrement et moralement tout au long de mes études. Que soit ici exprimée ma profonde gratitude

A tous mes frères et sœurs plus particulièrement à Ndiaga TALL, Fatim Tall, Bassirou Mbengue, Serigne Khadim Gueye et Mame Mor Seck pour leurs aides et soutien

Mes amis du master II Recherche sans qui cette aventure n'aurait pas été possible : Mor Talla Diouf, Mor Mbacké Gaye, Amadou Seck Ndiaye, Pape Mamadou Diagne, Mouhamed Ndoye, Ibrahima Niang, Etienne Alphonse Sarr, Pape Massaer Mboup, Thierno Fall, Ousmane Lo, Ndeye Thioro Yade et Youssou Faye mes compagnons de toujours

Je suis très reconnaissant à mon cousin Massamba Thiam pour son soution et collaboration tout au long de mes études et à mon maitre coranique, père, ami et frère El hadji Souleymane Kamara pour sa collaboration, ses prières et conseils très précieux. Que soit ici exprimée ma profonde gratitude.

Dédicace

Je dédie ce modeste travail

A ma famille ;

A mes amis ;

Aux enseignants de la faculté des Sciences Juridiques et Politiques.

Principaux sigles et abréviations

ADIE…Agence de l'informatique de l'Etat

ALD…Actualité législative Dalloz

ARTP…Agence de Régulation des Télécommunication et des Postes

Act. Jur. pén…Actualité juridique-pénal

Arch. pol. Crim…Archives de politique criminelle

ARPA…Advanced Research Projects Agency

Arpanet…Advanced Research Projects Agency Network

Batik…Bulletin d'analyse sur les technologies de l'information et de la communication

Bull. crim…Bulletin des arrêts de la chambre criminelle de la Cour de cassation

CCE…Cour des Communautés Européennes

CEDEAO…Communauté Economique des Etats de l'Afrique de l'Ouest

CEDH…Cour européenne des droits de l'homme

CREDILA... Centre de recherche, d'étude et de documentation sur les institutions et les législations africaines

CS…Cour Suprême

Chr…Chronique

Cons. Const…Conseil constitutionnel

Cah. Dr. Auteur…Cahier du Droit d'auteur

Cass. Crim…Chambre criminelle de la cour de cassation

C P…Code pénal

CPI…Code de la propriété intellectuelle

Comm. com. Elec…Revue Communication-Commerce Electronique

D…Recueil Dalloz

D. affaires…Revue de droit des affaires

Dr. pén…Revue Droit Pénal

Dir…Sous la direction

EDJA…Editions juridiques africaines

Éd…Edition

Gaz. Pal…Gazette du Palais

GAFI…Groupe d'action financière sur le blanchiment des capitaux

IC3…Internet Crime Complaint Centre

IR…Informations rapides (Dalloz)

NSFN…National Science Fondation Network

Id…Idem

J.O…Journal Officiel

J.O.C.E…Journal officiel de la Communauté Européenne

J.C.P…Juris-Classeur, La semaine juridique

J.C.P.I…Juris-Classeur, Propriété Intellectuelle

J.C.P. Entrep. Et Aff…Juris-Classeur Entreprise et Affaires

J.D.I…Journal du Droit International

LGDJ…Librairie générale de droit et de jurisprudence

Le Monde…Journal le Monde

N.D.A…Les Nouveaux Dossiers de l'Audiovisuel

N.D.P…Revue du Droit Public et de Science politique

OAPI…Organisation africaine de la propriété intellectuelle

OHADA…Organisation pour l'harmonisation du droit des affaires en Afrique

OSIRIS…Observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal

Propr. Intell…Propriétés intellectuelles

RSC…Revue de sciences criminelles et de droit pénal comparé

Rev. Sc. crim…Revue de Science Criminelle et de Droit Pénal Comparé

R.I.D.A…Revue Internationale de Droit d'auteur

R.L.D.A…Revue Lamy Droit des Affaires

R.L.D.I…Revue Lamy Droit de l'Immatériel

R.T.D. com…Revue Trimestrielle de Droit Commercial

RTD civ…Revue trimestrielle de droit civil

RTDH…Revue trimestrielle de droits de l'homme

RDTI…Revue du droit des technologies de l'information

Somm…Sommaires commentés (Dalloz)

STAD…Système de traitement automatisé de données

TGI…Tribunal de grande instance

TR…Tribunal régional

TRHC…Tribunal régional hors classe

TTHC…Tribunal du travail hors classe

Trib. Corr…Tribunal correctionnel

UEMOA…Union économique et monétaire ouest-africaine

SOMMAIRE

INTRODUCTION

« Depuis les premiers temps de l'histoire, la criminalité n'a jamais cessé de se manifester dans toutes les civilisations et dans tous les lieux de la Terre »[1].

Le XXI[ème] siècle voit la consécration des technologies numériques comme la fin du moyen âge a vu celle de l'imprimerie. Cette révolution contemporaine est notamment liée à la structure même d'Internet et de l'espace virtuel qu'il génère : le cyberespace[2].

L'ère numérique permet l'accès à la culture et à la croissance, elle rend possible la constitution d'une économie en ligne et rapproche le citoyen de son administration. Les technologies numériques sont porteuses d'innovation et de croissance, en même temps qu'elles peuvent aider ou accélérer le développement des pays émergents. Mais il faut reconnaitre que tous les progrès génèrent aussi de nouvelles fragilités et vulnérabilités propices aux menaces ou risques, car ils aiguisent l'imagination des criminels[3]. Elle est d'autant plus dangereuse qu'elle pénètre au sein des familles, là où la délinquance ordinaire n'avait pas accès jusqu'à présent. Avec l'apparition d'un secteur quaternaire de l'économie, celui où l'information est devenue source de richesse, la cybercriminalité est devenue une réalité. Elle se joue des frontières entre les Etats, rapproche la victime de son agresseur mais éloigne le délinquant de son juge.

En 1972, le doyen Jean CARBONNIER[4] affirmait déjà que « l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance ». Aujourd'hui, cette observation résonne toujours avec autant de force et de gravité. Indéniablement, les nouvelles technologies d'Internet ont changé radicalement nos civilisations. Elles sont porteuses d'innombrables avantages et opportunités sans précédent. Mais les enjeux qui leurs sont attachés sont autant de menaces qui ont donné naissance à « de nouvelles types de délinquance et suscité la commission de délits classiques (…). Qui plus est, la délinquance peut avoir des conséquences de plus lourde portée que par le passé dans la mesure où elle ne se cantonne plus à un espace géographique donné et ne se soucie guère des frontières

[1] R. MERLE et A. VITU, Traité de droit criminel, Tome I, 3[e] éd., Paris ? Cujas, 1978, p. 25.
[2] Le cyberespace est communément défini comme un ensemble de données constituant un univers d'information et de communication, lié à l'interconnexion mondiale des ordinateurs.
[3] A. LEPAGE, « Internet : un nouvel espace de délinquance », Act. Jur. Pén., n°6, juin 2005, Dossier, p. 217
[4] J. CARBONNIER, Sociologie juridique, 2[ème] éd., PUF, Paris 2004, p. 401.

nationales »[5]. En effet, Internet n'a pas seulement favorisé la perpétration d'actes de criminalité classique, il a modernisé cette criminalité et à donner naissance à de nouvelles infractions. L'exigence d'une démarche globale de modernisation des instruments de répression devant l'autorité judiciaire était devenue un enjeu de politique criminelle. Il s'agit pour la répression pénale de s'adapter aux évolutions de la criminalité. C'est dans ce cadre que s'inscrit notre étude sur la politique pénale sénégalaise à l'aune de la cybercriminalité.

Pour appréhender la notion de « *politique pénale* », celle-ci doit être inscrite par rapport à un cadre, la politique criminelle ; puis, elle doit être considérée comme un instrument d'expression de la politique criminelle. C'est dire alors que la politique pénale ne doit nullement être confondue avec la politique criminelle. Cette dernière, nourrie d'apports pertinents[6], est considérée comme « *science et art, explicative, préventive et répressive* »[7] du phénomène criminel. Elle est une stratégie juridique et sociale, fondée sur des choix de politiques publics pour répondre avec pragmatisme aux problèmes posés par la prévention et la répression de la criminalité[8]. Elle s'élabore en fonction d'option théorique[9] ou simplement d'écoles de pensée[10]. D'abord, de la politique, on peut dire qu'elle est compréhensible et conduite des affaires de la cité. La politique criminelle correspondrait alors à l'analyse et à la compréhension d'une affaire particulière de la cité d'une part et d'autre part à la mise en œuvre d'une stratégie pour répondre aux situations de délinquance ou de déviance[11]. La fonction de la politique était ainsi élargie en une réponse punitive et répressive au crime, pour s'affirmer ensuite dans sa richesse avec Marc Ancel et le mouvement de la Défense Sociale Nouvelle[12]. Marc ANCEL dans sa définition de la politique criminelle a ajouté « à la fois les problèmes de prévention et le système de répression »[13]. D'une manière beaucoup plus large, on peut

---

[5] Le Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité, op. cit., pp. 1et 2.

[6] Voir M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, Paris, PUF, 1992 ; du même auteur, *Modèles et mouvements de politique criminelle*, Paris, Economica, 1983 ; M. ANCEL, *La Défense Sociale nouvelle*, Paris, Cujas, 3ème éd., 1981.

[7] C. LAZERGES, *La politique criminelle*, PUF, 1987, p. 6.

[8] D. NZOUABETH, « La tolérance en matière pénale au Sénégal », Annales africaines, Nouvelle série, vol. 2, Décembre 2017, n° 7, CREDILLA, p. 161.

[9] Sur l'évolution des options théoriques, Voir M. KALUSZYNSKI, « Quand est née la criminologie ? Ou la criminologie avant les Archives... », Disponible sur le site : https://criminocorpus.revues.org/126 (consulté le 5 janvier 2017).

[10] Mais en droit Sénégalais, l'on constate une bifurcation des écoles de pensées de la politique criminelle.

[11] Ch. LAZERGES, Introduction à la politique criminelle, harmattan, 2000 p.7.

[12] M. ANCEL, La défense sociale nouvelle (Un mouvement de politique criminelle humaniste), Paris, Cujas, 1954, 2ème éd. 1966, 2ème éd. 1981.

[13] G. LEVASSEUR.., « La politique criminelle », arch. de philosophie, T.XVI, 197, p.131 et suivants ; Voir également « Réflexions sur la prévention générale », APC, n°3 ; 1977, p.13 et suivants. J.BERNAT DE CELIS, « La politique criminelle à la recherche d'elle-même ».APC n°2, 1977, p.3 et suivants.

retenir la politique criminelle comme l'ensemble des procédés par lesquels le corps social organise les réponses au phénomène criminel.

Par cette définition, on peut donc dire que la politique criminelle ne se réduit pas au droit pénal et à la procédure pénale ou à la criminologie, mais s'inscrit dans une stratégie globale qui n'est rien d'autre que la politique sociale d'un Etat donné, plus précisément la politique dite de la ville de cet Etat[14] ou d'une communauté d'Etats. Il devient clair que ni le droit pénal ni les sciences criminelles ne doivent s'approprier la politique criminelle, qui dépassent leur champ d'action respectif mais elle peut les servir tous. Telle est la vision de Mireille Delmas MARTY, qui, selon, elle, toute politique criminelle est science et art, explicative, préventive et répressive. Toute politique criminelle s'inscrit dans un système de politique criminelle[15]. La politique criminelle peut donc être qualifiée comme étant une réflexion épistémologique sur le phénomène criminel, un décryptage du phénomène criminel et des moyens mis en œuvre pour lutter contre les comportements de déviance ou de délinquance mais elle est également une stratégie juridique et sociale, fondée sur des choix politiques pour répondre avec pragmatisme aux problèmes posés par la prévention et la répression du phénomène criminel entendu largement. Une politique criminelle s'élabore en fonction d'options théoriques ou plus simplement d'écoles de pensée, elle peut aussi être analysée en termes de modèles de politique criminelle. Elle est diversement conçue et reçue par les instances étatiques législatives, judiciaires ou policières et par la société civile elle-même. Les conflits de politique criminelle sont un frein à sa réception et à sa mise en œuvre effective.

Ainsi, si le décryptage du phénomène criminel et des moyens mis en œuvre pour lutter contre les comportements de déviance ou de délinquance se fait grâce à la politique criminelle[16], la politique pénale apparaît comme un réseau de décisions et d'actions concrètes qui dynamisent la réponse pénale au phénomène criminel[17], ici le terrorisme[18]. La politique pénale est donc une modalité d'expression de la politique criminelle au même titre que d'autres stratégies lesquelles participent toutes à la canalisation des comportements contraires à l'ordre public social. Il s'agit donc de l'un des types d'action de la politique criminelle qui vise à élaborer les incriminations et les sanctions qui s'ensuivent et s'individualisent dans les décisions

[14] Ch. LAZERGES, Introduction à la politique criminelle, harmattan, 2000 p.7.
[15] Les grands systèmes de politique criminelle, coll. Thémis, PUF, 1992, p .8
[16] Ch. LAZERGES, « La défense sociale nouvelle a 50 ans. L'actualité de la pensée de Marc ANCEL », *RSC 2005*, pp. 165 et s.
[17] S. ENGUELIGUELE, *op. cit.*, pp. 22 et s.
[18] M. MASSE, «La criminalité terroriste», *RSC 2012*, p. 89.

prononcées par la justice répressive. Dans le cadre de notre étude, on considère la politique pénale comme le réseau de décisions et d'actions concrètes qui dynamisent la réponse pénale au phénomène criminel. C'est une modalité d'expression de la politique criminelle au même titre que d'autres stratégies lesquelles participent toutes à la canalisation des comportements contraires à l'ordre social.

On entend parler du numérique partout, sans savoir exactement ce qui se cache derrière ce terme. Serait-ce le mot à la mode pour dire informatique ? Ne pensez-vous pas que c'est un peu réducteur ? Pour bien comprendre ce à quoi on a affaire, voici quelques bases à connaitre avant de prendre le tournant. Le numérique englobe l'informatique, mais son périmètre est plus large car il recouvre aussi les télécommunications (téléphone, radio, télévision, ordinateur) et Internet. Au quotidien, on ne peut plus imaginer nos activités sans Smartphone ou sans les réseaux sociaux par exemple. Ces nouveaux usages génèrent des masses énormes de données (informations) qu'il faut être capable de traiter. Si le numérique modifie nos activités, il change en même temps notre façon de comprendre et de penser. Notre univers entier est transformé par cet ensemble de technologies. On entend d'ailleurs souvent parler de culture numérique ou encore de révolution numérique.

Internet comme lieu de naissance de nouvelles infractions est un thème de recherche qui soulève la question de l'efficacité du droit pénal pour faire face à cette criminalité toujours à la pointe du progrès et de plus en plus « professionnalisé ».

Ainsi, la question au centre de notre réflexion est celle de savoir **quels sont les défis de la politique pénale sénégalaise face aux évolutions de la criminalité du numérique ?**

L'intérêt porté à cette nouvelle réalité réside donc autant dans la nature des attaques qui sont commises que dans leur objet. Le numérique comme moyen de développement d'infractions préexistantes pose également la question de l'adaptation du droit pénal face à ces infractions classiques qui existaient déjà avant l'arrivée d'internet, mais qui ont trouvé en lui un redoutable moyen de développer, de franchir les frontières et de se pérenniser.

Au Sénégal, l'espace dématérialisé qu'offrent les TIC, notamment l'Internet, est de plus en plus le lieu virtuel de commission de divers agissements répréhensibles[19]. A titre illustratif, au

[19] Sur l'ensemble de la question, « Internet : un nouvel espace de délinquance », dossier, Act. Jur. pén, 2005, n° 6, juin, p. 217 ; W. CAPELLER, « Un net pas très net », in « L'immatériel et le droit », Arch. Phil. Dr, n° 143, p. 167 ; M. QUEMENER et J. FERRY, Cybercriminalité. Défi mondial, 2e édition, Paris, Economica, 2009, p. 1.

début du mois de mai 2001, le site officiel du gouvernement du Sénégal[20] a été victime d'une attaque de la part d'un pirate informatique se disant membre de la « Hack Army ». Le hacker, après avoir réussi à s'introduire dans le système informatique de la primature, a laissé le message suivant : « Vous avez des problèmes de sécurité ! »[21]. En janvier 2008, les actes de sabotage informatique, réalisés au moyen d'un cheval de Troie envoyé depuis le forum de discussion du site d'information « nettali.com », ont rendu indisponible son serveur pendant des semaines[22]. Le cyberespace est devenu criminogène. Une nouvelle forme de criminalité charriée par les premières lueurs de la société sénégalaise de l'information, appelée « cybercriminalité », venait d'apparaître. L'analyse des infractions qui y sont commises met en évidence deux phénomènes à la fois paradoxaux et complémentaires : la perversion du moyen de communication n'a pas seulement favorisé la commission d'actes de criminalité classique, mais il a modernisé cette criminalité et donné naissance à d'autres infractions inédites. En réalité, si le premier phénomène montre une véritable montée en puissance des groupes criminels, le deuxième phénomène démontre l'accentuation de la vulnérabilité des victimes. Sans aucun doute, l'étude de ce sujet nous permet de comprendre que le numérique par ces différentes caractéristiques, a rendu à la fois les criminels mieux armés et les victimes plus vulnérables. Cette évolution criminelle se perçoit d'une part, au caractère nouveau des actes, et, d'autre part, au nombre et à la fréquence des actes commis. L'ampleur du phénomène, de même que l'impact et l'importance des dangers qui en résultent, frappent l'opinion et démontrent visiblement la vulnérabilité d'une société de plus en plus dépendante des systèmes informatiques. Dans la même lancée, les actes terroristes se sont adaptés à cette nouvelle situation en usant d'Internet pour assurer la propagande et la diffusion large de leurs messages au-delà des limites continentales. Internet est devenu le lieu le plus prisé pour la revendication d'actes terroristes[23]. Les cybers terroristes usent du piratage informatique pour élargir leurs emprises sur les infrastructures critiques des pays. Aujourd'hui, le sabotage informatique constitue une action d'éclat comparable à un attentat parce qu'il peut paralyser toutes activités. Ces sabotages peuvent avoir des effets néfastes sur le fonctionnement des

[20] http://www.gouv.sn

[21] V. « Le site web du gouvernement attaqué par un hacker », in Batik, Osiris, n° 22, mai 2001, p. 4.

[22] Ch. Mb. GUISSE, « Sabotage et destruction du site Nettali.com : le parquet aux trousses d'un cheval de Troie » : http://www.osiris.sn/article3464.html; V. également, TRHC Dakar, du 17 avril 2012, affaire du système WARI, inédit. Dans cette affaire, le tribunal régional hors classe de Dakar a condamné, pour accès frauduleux à un système, un ancien salarié de la société gérant le système « Wari » qui s'est introduit dans ce système avant de procéder à des transferts frauduleux d'argent au profit d'un de ses amis.

[23] Le cyber terrorisme : une mutation du crime organisée, source : http://tresorkalonji.over-blog.com/pages/cyber-terrorisme-une-mutation-du-crime-organise-4595390.html, consulté le 01/03/2019 à 20 heures 20.

services de sécurité et de défense. Tout est aujourd'hui informatisé dans les armées. On parle de cybernétisation. Le cyberterrorisme existe bel et bien aujourd'hui et il est important de l'intégrer dans les stratégies actuelles de lutte contre la cybercriminalité. A côté de l'utilisation de l'Internet comme moyen de propagande, les virus informatiques constituent un problème à ne pas négliger. Les pirates informatiques ont tendance à s'organiser et se spécialiser en groupes éparpillés partout dans des territoires différents. Ce sont ces réseaux qu'on observe aujourd'hui en Afrique de l'Ouest, les informations peuvent être collectées dans un pays, transmises à des groupes établies dans un autre pays chargé d'appâter les victimes et l'argent est souvent envoyés et réceptionnés dans un autre pays. En tout état de cause, la criminalité du numérique a connu des évolutions.

Notre étude, au service de la recherche politico-criminelle d'un dispositif répressif adapté à la lutte contre la criminalité des réseaux, permet de répondre à un double enjeu dans l'encadrement juridique du phénomène cybercriminel. D'une part, elle s'inscrit dans le cadre de l'appel émis par le sommet mondial sur la société de l'information tenu en deux phases, à Genève en décembre 2003 et à Tunis en novembre 2005. Cet appel avait pour objectif l'édification d'un environnement juridique propice au développement des TIC. Cet objectif majeur constitue pour les pays en développement un des piliers fondamentaux de leur croissance économique. D'autre part, dans un contexte de mutation de l'ordre pénal, l'élaboration d'une stratégie innovante de politique criminelle contre la criminalité numérique devant le juge sénégalais constitue une occasion pour le génie africain d'inventer des réponses pénales adaptées à la cybercriminalité en dépassant l'approche mimétiste classique. Elle contribue à l'édification d'une société africaine de l'information et des connaissances suffisamment sécurisée et ancrée dans les valeurs positives de l'Afrique. La civilisation n'est en réalité qu'une architecture de réponses, pour parler comme Cheikh Hamidou Kane. Sous l'impulsion de cette perspective africaine du droit, l'organisation d'un dispositif pénal adapté à la cybercriminalité devant la justice pénale, présente le mérite de conjurer le développement de paradis numériques au Sénégal.

Dans un tel contexte, l'organisation d'une réponse répressive méthodique contre la criminalité du numérique devant le législateur sénégalais est largement tributaire de l'articulation d'un mouvement de politique criminelle fondé sur une stratégie d'expansion de son champ. Cette option stratégique est destinée à protéger la société contre cette nouvelle forme de délinquance devant la justice pénale. A cet égard, face à la recrudescence des agissements cybercriminels, il s'agira, par une démarche de modernisation de la politique criminelle,

d'attirer ces nouveaux comportements d'écart aux normes suscités par les TIC dans le champ pénal[24].

Ainsi, pour mieux cerner les contours de notre sujet, nous verrons d'abord, l'élaboration d'une stratégie d'adaptation des règles pénale de fond à l'ère du numérique **(chapitre I),** avant d'examiner ensuite, l'articulation d'une stratégie d'adaptation des règles pénales de forme à l'ère du numérique **(chapitre II)**.

[24] Sur l'exposé du mouvement d'expansion du champ de la politique criminelle, M. DELMAS-MARTY, Les grands systèmes de politique criminelle, Paris, PUF, 1992, p. 305-306 : « Qu'il s'agisse de l'informatique ou de la communication audiovisuelle, le progrès technique a suscité l'apparition de nouvelles normes juridiques, donc de nouveaux comportements d'écart à ces normes » ; du même auteur, Modèles et mouvements de politique criminelle. Paris Economica, 1983, p. 159 et s.

CHAPITRE I: L'ADAPTATION DES REGLES PENALES DE FOND A L'ERE DU NUMERIQUE

Chaque société, au courant du processus d'écriture de son histoire et de son évolution économique, conçoit, génère et organise des valeurs intrinsèques à sa vision, parfois sa culture, mieux même sa situation géographique, ou juste financière l'oriente. La conversion alors de groupes sociaux analogiquement distinctes l'une de l'autre, vers une forme unifiée de configuration sociétale, globalisée axée sur une technologie de l'information ouverte et fluide s'est accompagnée d'une diversification des agissements répréhensibles ayant pour cible les technologies numériques de l'information et de la communication, retenons aussi par ailleurs, que ses agissements concernent leurs composantes immatérielles.

Pour des raisons de politique criminelle compréhensible, il a paru nécessaire d'adapter les règles pénales de fond au numérique qui est à la fois une criminalité de la communication (section 1) et une criminalité par la communication (section 2).

SECTION 1 : LE NUMERIQUE, CRIMINALITE DE LA COMMUNICATION

C'est celle dont l'objet même est de menacer le réseau. Il en est ainsi de ce que l'on appelle le « hacking » dont les modalités et le domaine alimentent les controverses. Il ne s'agit pas d'une catégorie clairement définies, mais d'un ensemble plus ou moins flou d'actes illicites liés au réseau et qui, pour reprendre la terminologie de la Convention du Conseil de l'Europe sur la cybercriminalité, mettent en cause le « trafic ».

Au courant de nos travaux, nous verrons d'abord, l'adoption de nouvelles infractions face à la criminalité à l'être du numérique (paragraphe 1) avant de nous interroger ensuite sur l'adaptation de certaines infractions aux TIC (paragraphe 2).

Paragraphe 1 : L'adoption de nouvelles infractions face à la criminalité à l'être du numérique

Cette phase de nos travaux est fondamentale. Car, il ouvrira d'abord, notre compréhension sur les atteintes à l'intégrité des données et des systèmes informatiques (A) enfin, sur une autre échelle d'étude de mieux appréhender la notion de l'intrusion informatique (B).

A. Les atteintes à l'intégrité des données et des systèmes informatiques

Nous porterons notre analyse en premier lieu, sur les actes de sabotage visant les systèmes informatiques, notamment les attaques par saturation (1), en dernier lieu, il nous faudra profondément penser les attaques de sabotage visant les données informatiques (2).

1. Les actes de sabotage visant les systèmes informatiques

On distingue un ensemble de comportements et de pratiques techniques médités et accomplis sur et par le réseau Internet dans l'intention de nuire à la sécurité du réseau, des systèmes et des données informatiques qui le composent. Dans cet ensemble, l'un des dangers le plus présent à cause de sa fréquence et, d'ailleurs, le plus facile à exécuter, est le sabotage des systèmes informatiques. Il s'agit d'une attaque très à la mode pouvant viser les systèmes par deux façons : matérielle ou immatérielle. La première façon concerne les différentes pratiques matérielles susceptibles d'engendrer un dommage matériel, comme les incendies, la destruction matérielle des équipements informatiques. La seconde façon concerne les attaques organisées et exécutées par des moyens informatiques pour causer un dommage logique, tel que par exemple les envois des virus *DoS.* Seule l'analyse des attaques de sabotage informatique engendrent des dommages logiques sera traitée dans cette partie. Donc nous étudierons l'essor des attaques du sabotage informatique, avant de passer en revue les mécanismes et les manifestations des attaques par *DoS.*

-*l'essor des attaques du sabotage* informatique : Dans ce nouvel environnement numérique, où les unités de temps et la longueur de distance volent en éclat, la commission des actes de sabotage contre les systèmes informatiques semble devenir un « art » facile. Il n'est plus nécessaire d'être sur place pour saboter un système informatique puisqu'on peut le faire à distance grâce au réseau Internet. Chaque jour les médias font l'écho d'une atteinte de sabotage informatique commise sur Internet. Les pertes sont colossales et le nombre des victimes ne cesse d'augmenter. La sécurisation du réseau et des systèmes informatiques caractérise aujourd'hui un problème dont la résolution semble impossible, car le danger vient du réseau même. Indispensable pour la communication entre ordinateurs, Internet sert aujourd'hui d'un instrument fragilisant la sécurité des systèmes informatiques. Il représente une nécessité à la fois pour les victimes qui cherche à se moderniser, se cultiver, et pour les pirates qui l'exploitent de différentes manières en quête de déstabiliser la sécurité des systèmes qui y sont connectés. Passerelle d'action, Internet porte aussi de nombreux éléments structurels susceptibles d'affaiblir la résistance des systèmes informatiques. Une fois connectés au réseau mondial, les ordinateurs deviennent accessibles. Et de ce fait, ils deviennent vulnérables aux attaques informatiques. C'est cette fusion des technologies de l'information et de la communication qui met les systèmes informatiques et les saboteurs face-à-face. Evidemment, si on devait qualifier l'ère du Net, on parlerait de l'ère

d'accessibilité et du partage des données. Or, ces dernières sont actuellement source d'inquiétudes et de problèmes.

Outre les vulnérabilités fragilisant la sécurité des systèmes informatiques, la structure d'Internet comprend aussi de nombreux éléments susceptibles de favoriser la commission des actes de sabotage. Accessibilité, universalité, fragilité et facilité de mise en œuvre, etc. Et autant d'autres éléments propres à Internet encourageant aujourd'hui la croissance des actes de sabotage, le constat est redoutable. Tous les systèmes peuvent être attaqués. Grace à l'Internet, les actes de sabotage visant à déstabiliser les systèmes informatiques sont à portée de main. La contribution du réseau Internet est considérable. A l'heure actuelle, le sabotage apparait sous un jour nouveau. Au-delà de la qualification légale, le sabotage en ligne n'a rien en commun avec le sabotage hors ligne. La différence ne tient pas uniquement au nombre d'années qui les sépare. Elle tient également aux nouvelles technologies nées de la particularité d'Internet. Cette nouveauté réside tout particulièrement dans les mécanismes et les manifestations.

- *Les* mécanismes *et les manifestations des attaques par DoS : sabotage à distance.* The Denial of Service attack est le synonyme de l'attaque informatique par saturation qui consiste à envoyer des milliers de courriers électroniques depuis une machine ou des dizaines voire des milliers d'ordinateurs fonctionnant en réseau[25], dans le but de submerger les serveurs récepteurs, de les paralyser pendant plusieurs jours ou heures et d'en bloquer ainsi l'accès aux internautes. D'une manière générale, on parle de déni de service quand un internaute ou un groupe est privé d'un service utilisant des ressources qu'il est en droit d'avoir en temps normal. En d'autres termes, le DoS entrave la disponibilité des ressources pour les utilisateurs autorisés. En ce sens, le déni de service pourrait toucher par exemple l'accès au réseau ou à un spécifique, tels que le service messagerie électronique, le service de ressources partagées telles que les sites Internet, ou tout autre service virtuel nécessitant une connexion électronique via le réseau. En revanche, dans le cas d'un réseau interne, cette attaque ne peut que viser les systèmes locaux. Ainsi défini, le DoS est l'une des attaques informatiques la plus connue et la plus simple à comprendre. Aujourd'hui, ce type d'attaque est devenu un jeu d'enfant grâce aux logiciels du piratage informatique permettant la constitution des réseaux

[25] En octobre 2005, la force de police néerlandaise annonce l'arrestation des trois internautes qui s'était introduits dans 100 000 machines à l'aide d'un robot malveillant dénommé « *Toxbot* ». Les trois jeunes (19, 22, 27 ans) avaient utilisés ce réseau de *Botnet* pour mener des attaques regroupés type *DDos* ou des attaques de pillage sur les comptes *PayPa*l ou *Ebay*. Cf. *Cops Smash* 100 000 Node *Botnet*, *Botnet Army Disarmed*, www.governementsecurity.org, p. 1.

zombies. Agissant sur l'ordre du pirate, ces réseaux d'ordinateurs souvent piratés forment un véritable « peloton d'exécution » informatique. Cependant, ce danger menaçant les systèmes informatiques individuels ou en réseau, coute très cher. En termes de sécurité et d'économie, les pertes et les enjeux sont énormes. Chaque année, des milliers d'ordinateurs sont victimes de perturbation, de ralentissement et de saturation électroniques occasionnées par la perpétration des attaques de DoS. Hormis les pertes dues au blocage total ou partiel des sites et systèmes victimes, qui pourrait durer des heures voire des jours, le déni de service nuit gravement à la notoriété des cibles puisqu'il interrompt le cours normal des cyber-transactions. L'image et la réputation de la société victimes se voient détériorer après chaque attaque réussie, sans évoquer la répercussion de ces attaques informatiques sur le commerce électronique en général. Souvent utilisées dans son objectif hacking[26], les attaques de déni de service sont aussi un moyen de pression politique. Depuis quelques années, on observe une forte utilisation de ce procédé dans les conflits politiques et militaires. De nombreux groupes politiques ainsi que des guérillas et des indépendantistes s'en servent. Mais il arrive parfois que ce texte d'attaque soit utilisé comme un procédé de pression économique et de chantage. En réalité, la combinaison sabotage informatique chantage est aujourd'hui à son apogée. Pour s'en convaincre, il suffit de rendre compte de l'impuissance des entreprises de plus en plus dépendantes de l'informatique. Sans doute, cette vulnérabilité est le prix du progrès extraordinaire d'internet. Au niveau économique, la situation est cruciale et suscite des craintes légitimes. On peut imaginer l'embarras des sociétés et des entreprises qui se trouvent confrontées à une attaque. Pourtant, si le caractère révélateur ne se trouve pas dans les faits mêmes, le recours à la justice semble nouveau. On sait, rares sont les victimes de cybercriminalité qui font appel à la justice. Par craintes de représailles ou de mauvaises publicités, ces dernières préfèrent faire appel aux moyens silencieux de protection technique. C'est pourquoi on pourrait conclure qu'il est difficile de recenser avec précision le volume des actes de la cybercriminalité. Mais fort heureux est de constater que le droit ne se préoccupe pas des infractions suivant leur quantité ou leur fréquence mais plutôt le droit intervient pour un besoin de sécurité juridique.

[26] Le 8 février 2000, le site Internet de l'agence du voyage français, les nouvelles frontières, a été victime d'une attaque de DoS menée par des Hackers américains basés en Pennsylvanie. Le serveur a été saturé par une vague de messages électroniques, 2 000 courriers par minute. Cf. sur cette affaire, D. MARTIN et F. P. MARTIN, *op*. cit., p. 45.

2. Les actes de sabotage visant l'intégrité des données informatiques

A considérer les dangers qui guettent sans relâche le réseau Internet, les promesses de la philosophie de partage et du « turbo » économique semblent encore loin de se concrétiser. Hormis les lourds dégâts dus aux attaques de sabotage visant les systèmes informatiques, les entreprises ainsi que les particuliers sont en outre victimes des pertes de données. A l'instar des systèmes informatiques, les données qui y sont stockées peuvent à leur tour être l'objet d'attaques spécifiques de sabotage. Mais à la différence des systèmes informatiques qui ne peuvent être que l'objet d'attaques de déstabilisation ou de destruction, les données sont au contraire sujettes à plusieurs formes d'attaques, telles que la suppression, la détérioration, la modification ou l'adjonction. Il est particulièrement important de souligner que la destruction des systèmes informatiques entraine souvent une perte de données qui y existent. De même, l'effacement, la destruction ou la modification de certaines données peuvent entrainer une panne dans le système informatique concerné. C'est dans ce sens que nous distinguons entre les données informatiques servant au bon fonctionnement des systèmes informatiques et les autres données informatisées (personnelles, économiques, etc.) créées, stockées et échangées par les biais de ces systèmes. Quoi qu'il en soit, cette pratique est particulièrement dévastatrice à la fois pour les entreprises, les particuliers et la sécurité du réseau. Etudes, budgets, rapports, programmes, plans ou images, etc. autant de documents et de données informatiques et informatisées qui « valent de l'or ». Leur destruction peut entrainer une paralysie, voire une mort économique pour l'entreprise victime. Effectivement, s'il est aujourd'hui des thèmes qui transcendent toutes les priorités, la protection des données informatiques en est assurément une. Cette consécration ne relève pas seulement de l'organisation du travail, mais aussi de leur valeur particulièrement importante dans le domaine économique. Avec le développement accéléré du commerce électronique, la protection des données informatiques et informatisées concrétise aujourd'hui un enjeu économique vital.

Effectivement, qui n'a pas entendu parler du sabotage ? Véritable danger, le sabotage des données informatiques pourrait être en effet l'œuvre d'un employé mécontent ou d'un concurrent déloyal. Aussi, il pourrait être l'œuvre d'un cybercriminel qui cherche à tirer profit de cette pratique redoutable. Actuellement, la grande dangerosité des virus réside dans leur capacité et rapidité d'assurer un développement et une prolifération dans les délais très courts et atteignant un volume critique en quelques minutes. Il faut donc dire avec l'arrivée d'Internet et des nouvelles technologies de communication, les virus informatiques sont

devenus une arme de « destruction massive ». Aujourd'hui, l'utilisation des virus informatiques change et prend les formes qui peuvent les rendre plus dangereux et plus difficile à combattre. Malgré l'utilisation des moyens techniques de protection, qui a limité l'effet des virus et à réduit le nombre des systèmes atteints, le nombre de virus n'a pas cessé d'augmenter. En outre, force est de constater que les virus sont devenus plus agressif et beaucoup plus sophistiqué. Cette évolution technique a aussi entrainé une évolution des pratiques de groupes criminels. La facilitation de la commission de ces délits par les technologies de l'information et de la communication impose au législateur sénégalais de prendre en compte cette mutation dans sa politique pénale à travers l'édiction de ses règles modernes pour sécuriser la société avec l'avènement des TIC. Toujours l'attaque, les délinquants utilisent la méthode de l'intrusion informatique.

B. L'intrusion informatique

L'interrogation focale que l'on serait amené à se poser pourrait être celle-ci : quelles sont les modus operandi des pirates pour saboter des systèmes informatiques ? Pour l'apport de réponses précises et notables à ces interrogations, nous examinerons, à tour de rôle, les modalités de l'attaque d'intrusion (1), et les motivations des pirates informatiques (2).

1. Les modalités de l'attaque d'intrusion

Hier inconnues du grand public, les attaques par intrusion informatique représentent aujourd'hui une entité pathologique à part entière et en plein développement. On désigne ainsi un ensemble de comportements et de pratiques techniques prémédités et accomplis sur le réseau Internet dans l'intention de s'introduire de manière non autorisée et frauduleuse dans un ou plusieurs systèmes informatiques appartenant à autrui. Dans cet ensemble, l'une des pratiques d'intrusion la plus fréquente et, par ailleurs, la plus facile à organiser est l'utilisation d'un cheval de Troie type Backdoors[27], key-loggers[28], ou d'autres, qui constitue fidèle « traceur » permettant la prise des contrôles des ordinateurs infectés. Outre ce stratagème du cheval de Troie, il existe bien évidemment d'autres méthodes peu classique permettant de réaliser le même objectif, à savoir s'emparer de façon clandestine d'ordinateur d'autrui. A ce stade, on pense tout naturellement à la technique de casser les codes d'accès, appelé

[27] Les Backdors ce sont des programmes cheval de Troie qui permet au pirate de créer des portes dérobées dans la cible.
[28] Est un renifleur de clavier ou de mot de passe.

autrement « cracking »[29]. Dans ce cas, le pirate utilise des programmes de déchiffrage fonctionnant avec des dictionnaires qui proposent de nombreux mots de passe à des fréquences très élevées[30]. Il y a aussi les méthodes qui reposent sur la technique d'exploitation des failles existantes dans le système informatique. Celle-ci est à l'inverse de la technique du cheval de Troie, elle ne crée pas la faille. Ainsi, face à la montée excessive du nombre des vulnérabilités, chaque ordinateur devient accessible via trois, voire quatre techniques différentes. Ce qui laisse aux pirates la liberté du choix. A vrai dire, dans la saga de la cybercriminalité, les pirates ne sont jamais à cours de mauvaises idées. On constate que les méthodes les plus courante et fréquentes d'intrusion informatique sont le cheval de Troie et l'usurpation d'identité.

En principe, les mécanismes de l'attaque d'intrusion varient en fonction de la cible et de l'objectif recherché. L'une de ces mécanismes est l'utilisation du spyware[31] type cheval de Troie. Utilisé depuis des siècles par les guerriers grecs, ce stratagème continue à exercer une étonnante fascination. Actuellement, force est de constater l'apparition des programmes informatiques malicieux en tout genre qui retracent inlassablement la saga Troyenne au cours de laquelle « les Troyens reçurent en cadeau, pendant la guerre de Troie, un cheval de bois géant, auquel ils ouvrirent les portes de la cité. Au milieu de la nuit, des soldats grecs, qui s'étaient cachés dans le cheval, en sortirent pour ouvrir les portes et permettre à l'armée grecque de prendre la cité ». En termes simples et actuels, la méthode du virus type « Trojan » en anglais, ou « cheval de Troie » en français, permet à l'intrus d'ouvrir une brèche, via un fichier infecté, dans un ordinateur en vue d'en prendre le contrôle. Il s'agit de l'une des techniques les plus courantes pour passer à travers le système de protection. Elle consiste à utiliser le courrier électronique pour piéger la cible. Une fois le courrier électronique est ouvert, l'intrus pourrait, sans que le maitre légal en prenne conscience, piloter à distance la machine piratée, dite aussi Zombie, pour la réalisation de son projet criminel qui va d'un simple « coup d'œil » aux détériorations de données, en passant par son utilisation pour le brouillage des pistes.

Concernant l'usurpation d'identité, comme l'on sait, dans le domaine de la cybercriminalité, des formes fort divers. Ainsi, on distingue l'usurpation d'identité permettant l'intrusion dans

[29] Le cracking est l'intrusion de manière forcée dans un système informatique afin de saboter, d'altérer ou de détruire les données de traitement ou les données traitées à l'intérieur du système.
[30] Certains logiciels tentent milliers de mots de passe par seconde.
[31] Les spywares sont des programmes espions qui se nichent discrètement dans les systèmes informatiques pour surveiller leurs activités. Ils peuvent entrainer des défaillances logiques, submerger les victimes sous des flots publicitaires, éventer des mots de passe et d'autres données confidentielles.

les systèmes informatiques de l'identité attaquée, de l'usurpation d'identité permettant l'envoi de faux courriers électroniques. Contrairement aux techniques de cheval de Troie reposant sur le social engineering, les attaques par usurpation d'identité se forgent sur l'utilisation des techniques permettant au pirate de se faire passer pour un utilisateur autorisé. L'expert en informatique Merike Keao définit ce type d'attaque comme « la fourniture des fausses informations sur l'identité d'un client en vue d'accéder sans y être autorisé à des systèmes et à leurs services ». Cela dit, elle implique l'envoi des données qui ne sont pas ce qu'elles prétendent être. L'exemple classique de telle attaque reste l'usurpation d'adresse IP. Au-delà d'usurpation d'adresse IP, il faut noter que cette attaque peut s'appliquer à toutes les couches de la communication entreprise entre deux machines, client-serveur. Une fois réalisée, l'intrus pourrait, sans que le maitre légal en prenne conscience, utiliser la machine piratée pour réaliser son projet délictueux. Ce dernier peut aller d'une simple curiosité à un véritable acte d'espionnage. Ainsi, nous étudierons les éléments qui peuvent motiver le piratage informatique.

2. Les motivations des pirates informatiques

Au-delà du caractère mécanique, le piratage informatique est souvent perpétré afin d'accomplir une ou plusieurs missions allant d'un acte crapuleux entre particuliers à une politique de dissuasion sinon de destruction économique massive pratiquée par des Etats. Le piratage informatique pourrait être motivé par le but lucratif, l'espionnage, le défi technologique ou la déception amoureuse. Pour commencer notre analyse sur une note anecdotique mais révélatrice, nous reprenons l'affaire de l'informaticienne britannique qui s'est vue condamner par le Tribunal de Leicester, centre de Grande-Bretagne, pour avoir harcelé via Internet un ancien amant. Dans les faits, l'amoureuse éconduite qui prétend être l'objet d'un cyber-harcèlement, a payé des pirates informatiques canadiens pour bombarder son amant de courriers électroniques à caractère injurieux. De plus, pour constituer des fausses preuves de ses allégations, elle a piraté elle-même l'ordinateur de son ancien amant. In fine, pour frapper plus dur, elle a inscrit son ancien amant sur un certain nombre de sites Internet, dont un site de prisonniers homosexuels, qui a valu à sa victime de recevoir des lettres à contenu pornographique. Mais le piratage informatique n'a pas toujours pour cause une histoire d'amour. Dans un environnement internationalisé et fortement concurrentiel, la maitrise de l'information devient un élément déterminant dans les prises de décision destinées non seulement à conquérir de nouveaux marchés mais aussi à protéger les intérêts

économiques acquis[32]. En réalité, avec le développement accéléré de l'économie mondiale et l'essor exceptionnel des nouvelles technologies, l'espionnage informatique joue un rôle primordial. Aujourd'hui, une nouvelle géopolitique se dessine : elle place en position de force les pays maitrisant cette arme et contraint les autres à s'en doter afin de protéger les intérêts nationaux. Certainement, l'apparition d'instruments d'espionnage extrêmement performants a rendu ce concept viable, le réseau Echelon fournit un excellent exemple[33], même si nous considérons que l'espionnage est aussi vieux que l'histoire de l'humanité. Il a été pratiqué avant l'irruption d'Internet. Outre cet aspect économique, la recherche et la maitrise de l'information peuvent s'appliquer à tous les domaines de l'activité humaine. Le domaine militaire-sécurité est à la base du concept de l'espionnage. Il est important de comprendre que cet aspect d'espionnage n'est pas forcément un moyen d'attaque. Habituellement, il s'agit d'un moyen de prévention contre toutes les menaces réelles ou potentielles.

Parallèlement à l'espionnage, il est possible de citer le but crapuleux qui motive certaines bandes de pirates informatiques. Pour ces derniers, Internet est sans doute le lieu tout trouvé pour réaliser des fortunes. La fraude aux cartes de crédit, le vol et la commercialisation des données confidentielles le concernant menacent sérieusement l'avenir du commerce électronique. Avec en arrière-fond le but lucratif, l'intrusion informatique est devenue une pratique en plein « boom » sur Internet. Elle consiste à extorquer de l'argent aux entreprises ainsi qu'aux individus. Sans doute, l'exemple classique est l'utilisation des virus espions promettant l'extorsion de données concernant les cartes et les comptes bancaires traditionnels ou Internet. Traduisant cette réalité, le commerce illicite le plus lucratif est évidemment celui des numéros de cartes bancaires[34]. Sur Internet, celui-ci est réalisé à grande échelle par une

[32] C'est la doctrine du « Shaping the World », telle que l'a exposée le Président Clinton dans un discours de 2000 sur l'état de l'Union. Selon le Président américain, pour saisir toutes les occasions offertes à notre économie, « nous devons dépasser nos frontières et mettre en forme la révolution qui abat les obstacles et installe de nouveaux réseaux parmi les nations et les individus, les économies et les cultures : la globalisation » ; discours disponible sur l'adresse Internet suivante www.wihtehouse.gouv.

[33] Créé en 1948, Echelon est le système d'espionnage le plus vaste dans le monde. Il regroupe les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande. Selon le rapport du comité du Parlement européen, chargé d'enquêter sur Echelon, il s'agit d'un réseau de surveillance de taille mondiale capable d'intercepter les appels téléphoniques, les télécopies et les courriers électroniques ; cependant, il est très peu probable qu'il sert à l'espionnage industriel. Ce rapport rédigé par Duncan Campbell a d'ailleurs fait l'objet d'une audience publique du Parlement européen. Rapport disponible sur l'adresse Internet suivante : www.europarl.eu.int.

[34] En mars 2006, les experts chez l'éditeur américain de logiciels de sécurité Sunblet Software et la société américaine de sécurité informatique Secure Science ont annoncé la découverte sur le réseau Internet des fichiers contenant des données personnelles de 17 millions d'abonnés à des sites pornographiques qui étaient proposés à vendre pour 300 dollars. Cf. SAIZ (j.), « Petite escroquerie entre escrocs », www.lesnouvelles.net, 10 mars 2006, p. 1.

chaine des criminels. A la tête de cette chaine, on trouve des hackers[35] dont la mission consiste à voler les numéros de cartes bancaires ou de crédit, etc. Les victimes classiques de ce type de pratique sont sans aucun doute les sites marchands en ligne, les sites bancaires et pratiquement tous les sites contenant de données financières. Au-delà de l'impact économique, cette criminalité a ses propres modes opératoires, qui font fi des systèmes du dispositif de protection technique et juridique. Elle utilise ensuite, selon le besoin, les tendances et les pratiques qui caractérisent l'économie légale. Elle s'est internationalisée, décentralisée et délocalisée. Comme nous avons vu, le réseau est la forme de son mode opératoire et organisationnel avec un profond professionnalisme criminel qui apparait à plusieurs occasions.

Les nouvelles technologies de l'information et de la communication, combinées à la phase de la mondialisation dans tous les domaines sont, en effet, à l'origine de profonds bouleversements économiques, sociaux, philosophiques et juridiques tels que l'apparition dans nos Codes pénaux contemporains, de nouveaux chapitres consacrés à la lutte contre cette nouvelle criminalité de la communication.

<u>Paragraphe 2 :</u> L'adaptation de certaines infractions aux TIC

La cybercriminalité présente un caractère protéiforme aux dimensions changeantes. Les comportements répréhensibles liés aux TIC ayant pour objet les valeurs immatérielles du cyberespace ne sont pas toujours réalisés au moyen de procédés nouveaux inconnus des instruments de la politique criminelle. Ils sont souvent commis à l'aide d'actes frauduleux bien connus des mécanismes du droit pénal, puisque se découlant de sources dans les catégories classiques du droit pénal spécial. Sur le plan de l'analyse pénal, ces mutations macro-criminologiques de la délinquance au Sénégal ont quasiment fait sorti de ses gongs le législateur dans son activité rédactionnelle, qui avait besoin d'être approfondi face à une situation d'inadaptation juridique, face à laquelle il fallait quand bien même trouver une solution appropriée.

Il s'agit en réalité d'une technique de formulation normative des infractions informatiques consistant à étendre des notions communes du droit pénal. Cette méthode d'incrimination complémentaire sera articulée, d'une part, autour de la protection pénale spécifique des

[35] Aujourd'hui, ce terme sert à désigner les internautes mal intentionnés qui pratiquent la délinquance informatique dans tous ses facteurs.

créations informatiques (A) et, d'autre part, autour de la protection générale de l'information (B).

A. La protection pénale spécifique des créations informatiques

Avec l'avènement de la micro-informatique et du réseau internet, les utilisations irrégulières des créations informatiques prennent des formes d'une grande variété[36]. Ces pratiques sont de plus en plus banalisées dans la société de l'information. Dans un tel contexte, malgré l'existence de protections techniques, la protection des créations informatiques par le droit pénal s'est révélée très vite comme une nécessité impérieuse. En tout état de cause, la répression pénale effective des atteintes aux droits des auteurs des créations numériques passe nécessairement par une protection des créations informatiques par le droit d'auteur (1) et de la répression pénale des atteintes aux créations informatiques (2).

1. La protection des créations informatiques par le droit d'auteur

Les créations informatiques, expression communément employée par la doctrine juridique de la propriété intellectuelle, regroupent l'ensemble des créations en rapport avec le processus de traitement automatique des informations[37]. Elles renvoient essentiellement aux logiciels, aux bases de données et aux œuvres multimédias. En droit sénégalais, le principe de la protection pénale des créations informatiques par le droit d'auteur est largement tributaire de l'intégration des logiciels et des bases de données dans les catégories des œuvres de l'esprit. Dans une approche classique, les spécialistes de la propriété intellectuelle n'étaient pas favorables à une protection des logiciels par le droit d'auteur, en raison du fait que la loi française de 1975 ne protégeait que les œuvres procédant d'une démarche artistique, c'est-à-dire les productions « *de l'esprit ou du génie appartenant aux beaux-arts »*[38]. Or, les programmes d'ordinateur, constituant des instruments pour faire fonctionner les machines, sont par essence de nature technique et utilitaire. On voit mal comment un programme pourrait exprimer sa personnalité à travers les instructions dont le caractère technique est très marqué[39]. Devant les controverses jurisprudentielles et les hésitations doctrinales, le

[36] Copies, plagiat, de programmes informatiques, reproductions illicites de bases de données ou de sites web

[37] Sur cette définition, F. MACREZ, Créations informatiques : bouleversement des droits de propriété intellectuelle. Essai sur la cohérence des droits, Paris, Litec, 2011 ? p. 20, n° 7

[38] R. PLAISANT, « La protection du logiciel par le droit d'auteur », Gaz. Pal. 2., Doctr., p. 348.

[39] Sur ces difficultés, Ch. D. DJOMGA, La contrefaçon des logiciels dans l'espace OAPI. Etude comparée de l'accord révisé et des législations du Sénégal, du Gabon, de la Cote d'Ivoire et du Cameroun, Editions ISIS, Yaoundé, octobre 2011, p. 18 et s. ; D. WAFO, « La protection par le droit d'auteur du logiciel en Afrique noire : le pénible éveil », Penant, n°818, mai à septembre 1995, p. 156 et s.

législateur français devait adopter la loi n° 85-660 du 3 juillet 1985[40]. Ce texte a consacré la solution fondamentale que les logiciels sont des œuvres de l'esprit protégées par le droit d'auteur[41]. La chambre plénière de la Cour de cassation, dans trois arrêts rendus le 7 mars 1986 et notamment dans la célèbre affaire Pachot, a relevé toute ambiguïté en déclarant qu'un « *logiciel, dès lors qu'il est original, est une œuvre de l'esprit protégée par la loi sur le droit d'auteur* »[42]. En Afrique, l'Annexe VII de l'Accord portant révision de l'accord de Bangui du 02 mars 1977 instituant une Organisation africaine de la propriété intellectuelle relatif à la propriété littéraire et artistique prévoit dans son article 5 que « *la présente Annexe s'applique aux œuvres, qui sont des créations intellectuelles originales dans le domaine littéraire et artistique, scientifique, telles que : i) les œuvres exprimées par écrit, y compris les programmes d'ordinateur (...)*». Au Sénégal, sous l'empire de la législation antérieure, le droit d'auteur était notamment régi par la loi n° 73-52 du 04 décembre 1973 relative à la protection du droit d'auteur[43], texte fortement inspiré par la loi française du 11 mars 1957. L'article 1er de cette loi disposait que sont notamment considérées comme œuvres de l'esprit les œuvres classiques de l'espace physique que sont notamment les livres, les brochures, les conférences, les allocutions, les sculptures, les œuvres cinématographiques, les œuvres d'architecture, les œuvres photographiques le folklore, etc. Mais ce texte ne visait pas expressément les logiciels dans son énumération indicative[44]. A notre connaissance, la jurisprudence sénégalaise n'a pas encore eu l'occasion de se prononcer sur la délicate question de la protection des programmes informatiques par le droit d'auteur, ce qui pouvait être source de confusion, quant à l'effectivité de cette protection[45]. Le Sénégal a récemment adopté la loi n° 2008-09 du 25 janvier 2008 sur les droits d'auteur et les voisins, en vue notamment, précise l'exposé des motifs de cette loi, de « *respecter ses obligations internationales et de mettre sa législation en conformité avec certaines conventions* ». Aux termes des dispositions de l'article 6 de cette loi intitulé « *liste énonciative des œuvres de l'esprit protégeables* » « *sont considérées comme œuvres de l'esprit au sens de la présente loi*

[40] JO du 4 juillet 1985, p. 7495.
[41] A. LUCAS, « Les programmes d'ordinateurs comme objets de droits intellectuels », JCP, éd. G. I, n° 3081 ; J. HUET, « Les logiciels sont protégés par le droit d'auteur », D. 1985, p. 261 ; J.-R. BONNEAU, « La protection des logiciels », Gaz. Pal., 19 septembre 1985, p. 503 ; M. VIVANT, « Le logiciel aux pays des merveilles », JCP, I n° 3208.
[42] Cass. Ass. Plén. 7 mars 1986, affaire Pachot, D. 1986, Jurisp. P. 405, note B. Edelman ; JCP G. 1986, II, 20631, note J.M. MOUSSERON, B. Teyssié et M. Vivant ; RTD. Com. 1986, p. 399, obs. A. Francon.
[43] JORS, n° 4333 du 29 décembre 1973, p. 399.
[44] I.CAMARA, Le statut juridique de la contrefaçon des phonogrammes et œuvres littéraires et artistiques du Sénégal, Dakar, EDJA, mars, p. 10.
[45] A.J. COLY, « Protection internationale des logiciels informatiques : la législation sénégalaise à la traine » http://www.osiris.sn/article905.html.

les créations intellectuelles de forme dans le domaine littéraire et artistique, notamment : 1° Les œuvres du langage, qu'elles soient littéraires, scientifiques ou techniques y compris les programmes d'ordinateurs, et qu'elles soient écrites ou orales ».

Ainsi, en droit d'auteur sénégalais, les programmes d'ordinateurs sont assimilés à des œuvres de langage de nature technique écrites et exprimées en langage informatique perceptibles aux informaticiens et destinées à une machine. Il s'agit au fond d'une « *protection de replie choisie par défaut »*[46] Conformément au droit commun du droit d'auteur, la protection des logiciels par le droit de la propriété intellectuelle est subordonnée à la condition classique de l'originalité du programme et elle porte sur un objet spécifique. Mais il faut noter également que la loi a posé une condition pour que l'œuvre de l'esprit puisse bénéficier de cette protection légale : il s'agit de l'originalité du logiciel. Cette exigence de l'originalité est expressément posée par l'article 7 de la loi n° 2008-09 du 25 janvier 2008 sur les droits d'auteur et les droits voisins. Ce texte dispose que « *les œuvres de l'esprit ne peuvent bénéficier de la protection que si elles sont originales ».* La notion standard d'originalité ne fait l'objet d'aucune conceptualisation légale en droit français[47]. Aussi a-t-elle suscité à propos des logiciels des controverses au point que l'on a pu parler d'une crise contemporaine de l'originalité[48]. En droit sénégalais, le législateur a pris le soin de définir l'originalité. L'alinéa 2 de l'article 7 de la loi du 25 janvier 2008 énonce en effet que « *l'originalité s'entend de la marque de la personnalité de l'auteur ».* Ainsi, le législateur sénégalais semble avoir consacré la conception subjective classique de l'originalité dont la paternité est souvent attribuée à Desbois[49], selon laquelle l'originalité serait l'expression de la personnalité de l'auteur. Cette conception tournée vers les beaux-arts établit un net départ entre l'originalité et la nouveauté. Une œuvre est originale lorsqu'elle exprime le caractère unique d'un individu. Il en résulte ainsi que l'originalité, notion subjective identitaire du droit d'auteur, n'est pas la nouveauté, concept objectif du droit de propriété industrielle. Dans cette optique, une œuvre originale peut bien être nouvelle, mais elle peut bénéficier de la protection tout en étant dénuée de toute nouveauté. Cependant, cette approche personnaliste de l'originalité s'accommode mal de la logique des œuvres d'entreprise comme les logiciels dominés par des

[46] F. MACREZ, « Logiciels : le cumulard de la propriété intellectuelle » in J.-M. BRUGUIERE (dir), L'articulation des droits de propriété intellectuelle, Paris, Dalloz, 2011, p. 45.
[47] X. DESJEUX, « Logiciel, originalité et activité créative dans la loi du 3 juillet 1985 », Expertises, p. 32.
[48] Ch. CARON, Droit d'auteur et droits voisins, Litec, 2006, p. 67.
[49] H. DESBOIS, Le droit d'auteur, Dalloz, 1ère édition, 1950, n° 50 et s.

impératifs industriels impliquant « *une élision de l'auteur* »[50]. Comment à travers l'association d'un ensemble d'instructions exprimées en langage informatique évolué, le programmeur peut-il exprimer sa personnalité ?

Il a été admis en doctrine que, si l'originalité marque la personnalité de l'auteur, elle implique nécessairement la nouveauté, puisqu'elle « *appréhende les caractéristiques d'une personne qui sont forcément distinctes de celles des autres individus* »[51], la personnalité humaine étant unique. La jurisprudence française n'a pas manqué de suivre cette évolution conceptuelle associant originalité et nouveauté, surtout à propos des programmes d'ordinateurs[52]. Déjà, dans la célèbre affaire Pachot, jugée le 7 mars 1986 par l'Assemblée plénière de la cour de cassation française, les hauts magistrats ont décidé qu'était original le logiciel que l'auteur avait marqué de son « *apport intellectuel* » et que l'originalité s'entendait d'un « *effort allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante et que la matérialisation de cet effort résidait dans une structure individualisée* »[53]. Le critère tiré de l'apport intellectuel semble évoquer « un *basculement vers la nouveauté* »[54]. Un apport est forcément nouveau par rapport à ce qui impose la recherche de l'absence d'antériorité. Force est ainsi de prendre acte de la tendance à l'objectivation de l'originalité du logiciel[55]. Le droit d'auteur sénégalais, reprenant l'annexe VII de l'Accord portant révision de l'accord de Bangui du 02 mars 1977, ne protège que « *les œuvres du langage, qu'elles soient littéraires, scientifiques ou techniques, y compris les programmes d'ordinateurs, et qu'elles soient écrites ou orales* ». Mais le droit français vise « *les logiciels y compris le matériel de conception préparatoire* »[56]. Le matériel de conception préparatoire couvre, selon la Directive européenne du 14 mai 1991 sur la protection des programmes d'ordinateur, « *l'ensemble des travaux de conception aboutissant au développement d'un programme, à condition qu'il soit de nature à permettre la réalisation d'un programme d'ordinateur à un stade ultérieur* ». Il

[50] Ch. CARON, ibid. ; C. CASTET-RENARD, Droit de l'internet : droit français et européen, Montchretien, 2e édition, 2012, p. 207, n° 563.
[51] Ch. CARON, op. cit., p. 68 ;
[52] Ch. D. DJOMGA, La contrefaçon des logiciels dans l'espace OAPI. Etude comparée de l'accord révisé et des législations du Sénégal, du Gabon, de la Cote d'Ivoire et du Cameroun, éditions ISIS, Yaoundé, octobre 2011, p. 20.
[53] Cass. Ass. Plén. 7 mars 1986, D. 1986, Jurisp. P. 405, note B. Edelman ; JCP G. 1986, II, 20631, note J.M. Mousseron, B. Teyssié et M. Vivant ; RTD Com 1986, p. 399, Obs. A. Francon.
[54] M. VIVANT et J.-M. BRUGUIERE, Droit d'auteur, 1ère éd., Dalloz, 2009, p. 178.
[55] En ce sens, A. LATREILLE, « Logiciel, objets de propriétés », RLDI, n° 49, mai 2009, p. 38.
[56] V. art. 112-2 13° du Code de propriété intellectuelle français.

s'agit des ébauches et maquettes, des analyses et du manuel d'utilisation du logiciel considéré par la jurisprudence française comme une œuvre littéraire[57].

Dans l'Accord de Bangui révisée le 24 février 1999 et en droit international du droit d'auteur, seule une protection par le droit d'auteur des bases de données est prévue.[58] En adoptant la loi du 25 janvier 2008 sur les droits d'auteur et les droits voisins, le Sénégal a entendu se conformer à ses engagements internationaux, en comblant les lacunes de la législation antérieure. Aux termes de l'article 8 alinéa 3 de cette loi, *« sont également protégés à ce titre les anthologies et recueils d'œuvres ou de données diverses, tels que les bases de données, qu'elles soient reproduites sur support exploitable par machine ou sous toute autre forme, qui, par le choix ou la disposition des matières, constituent des œuvres originales »*. Il résulte de ce texte qu'en droit positif sénégalais, la base de données est élevée au rang d'œuvres dérivée encore appelée œuvre composite. Il s'agit d'une « œuvre nouvelle à laquelle est incorporée une œuvre préexistante sans la collaboration de l'auteur de cette dernière »[59]. Conformément aux principes généraux du droit d'auteur, pour prétendre à la protection, les bases de données doivent présenter un caractère d'originalité. Il s'agit, comme en matière de logiciel, de la marque de la personnalité du producteur de la banque de données. Cette exigence s'articule essentiellement autour du critère tiré des choix arbitraires faits par l'auteur. L'article 8 de la loi de 2008 évoque à ce sujet *« le choix ou la disposition des matières »*, comme critère de l'originalité de la base des données. La jurisprudence ne cesse de répéter que la protection est accordée aussi bien aux bases de données électroniques qu'à celles qui existent sur un format papier[60]. D'ailleurs, l'article 8 de la loi du 25 janvier 2008 sur le droit d'auteur et les droits voisins vise les bases de données *« qu'elles soient reproduites sur support exploitable par machine ou sous toute autre forme »*. Mais, la protection des bases de données électroniques, compte tenu de la multiplication des atteintes dont elles sont exposées, du fait de l'utilisation des technologies numériques, pose les problèmes de politique criminelle les plus délicats. La protection légale porte sur l'ensemble de l'œuvre composite que constitue la base de données et non sur les éléments et données qu'elle constitue. Il est

[57] CA Paris, 1er juin 1994, D. 1995, Somm. p. 286, obs. C. Colombert.
[58] Selon l'article 6 de l'Accord de Bangui précité, « les recueils d'œuvres (…) ou de simples faits ou données, telles que (…) les bases de données, qu'elles soient reproduites sur support exploitable par machine ou sous toute autre forme, qui, par le choix, la coordination ou la disposition des matières, constituent des créations intellectuelles ».
[59] Cette définition de l'œuvre composite est donnée par l'article 113-2 alinéa 2 du Code de propriété intellectuelle français.
[60] TGI Lille, 19 novembre 2009 :www.legalis.net.

évident que les éléments constitutifs de la b ase peuvent, s'ils sont originaux, donner prise au droit d'auteur dans les conditions du droit commun.

En tout état de cause, l'intégration des créations informatiques dans le champ du droit d'auteur présente le mérite de garantir la répression pénale des atteintes dirigées contre ces œuvres.

2. La répression pénale des atteintes aux créations informatiques

Au Sénégal, sous l'empire de la législation pénale antérieure, la protection des attributs des auteurs d'œuvres de l'esprit en général était assurée par le délit de contrefaçon. Pour reprendre l'expression du professeur Caron, cette infraction « est au droit d'auteur ce que le vol est aux biens corporels »[61]. La contrefaçon était prévue par les articles 397 à 401 du Code pénal. Il ressort de ces textes que l'infraction de contrefaçon réprimait essentiellement la violation des droits patrimoniaux, à savoir le droit de reproduction et le droit de représentation. La question était très discutée de savoir si la violation du droit moral du titulaire pouvait engager la responsabilité pénale de son auteur sous la qualification de contrefaçon[62]. La loi n° 2008-09 du 25 janvier 2008 sur les droits d'auteur et les droits voisins, ayant expressément abrogé les dispositions des articles 397 à 401 du Code pénal[63], a procédé à une refonte du droit pénal sénégalais de la propriété littéraire et artistique. Désormais, la répression des atteintes aux droits des auteurs d'œuvres de l'esprit relève des articles 142 à 144 de la loi n° 2008-09 du 25 janvier 2008. Ces textes dissipent toute ambiguïté en érigeant en infraction la violation des droits patrimoniaux et moraux de l'auteur. Sur le plan de l'élément matériel, le délit de contrefaçon portant sur les créations informatiques peut recouper trois actes matériels. Il s'agit de la violation des droits patrimoniaux (article 142), de la violation du droit moral des auteurs (article 144) et de la diffusion, de l'importation et de l'exportation d'exemplaires illicites (articles 143). Par un souci de clarté, il importe d'isoler, d'une part, la violation des droits patrimoniaux et, d'autre part, l'atteinte aux droits moraux des auteurs de créations numériques. Les atteintes aux droits patrimoniaux des auteurs prévues par l'article 142 de la loi de 2008 sur le droit d'auteur et les

[61] Ch. CARON, op. cit., p. 385, n° 486 ; C. COLOMBER, « Propriété littéraire et artistique, Droit d'auteur. Règles générales, contrefaçon et infractions aux droits voisins : éléments constitutifs », J-Cl. Pénal, fasc. 336-1, 11, 1991, n° 3. Selon l'auteur, la contrefaçon est « une atteinte à la propriété qu'à l'auteur sur l'œuvre qu'il a lui-même conçue et réalisée ; c'est une violation du droit, pour cet auteur, de conserver l'exclusivité sur ses œuvres, de n'en concéder à autrui la jouissance, la production ou l'imitation que s'il a consenti lui-même expressément »

[62] G. GAVIN, « Vers une sanction pénale du doit morale », RIDA avril 1961, p. 3 ; G. LESSOURD, « Violation du droit moral de l'auteur », JCP, I, 2067 ; A. FRANCON, « Les sanctions pénales de la violation du droit moral », in mélanges Brust, Litec, 1997, p. 171.

[63] V. art.162 de la loi n° 2008-09 du 25 janvier 2008, sur les droits d'auteur et les droits voisins.

droits voisins concernent aussi bien les prérogatives classiques (droit de reproduction, droit de communication au public) que les droits dits modernes (droit de distribution, droit de location). S'agissant des créations informatiques. L'atteinte au droit de reproduction est érigée en infraction par l'article 142 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité. En vertu de l'article 35 de la loi n° 2008-09 du 25 janvier 2008 sur le droit d'auteur et les droits voisins, cette prérogative réside dans le droit exclusif pour l'auteur *« d'autoriser la fixation de son œuvre, par un procédé quelconque, sous une forme matérielle permettant de communiquer au public »*. C'est à ce droit de reproduction, auquel se référait implicitement l'ancien article 397 du Code pénal, qui réprimait *« toute édition d'écrits, de composition musicale, de film, de dessin, de peinture ou de toute autre production imprimée, enregistrée ou gravée en entier ou en partie »*. En effet, l'édition implique un acte de reproduction[64]. Selon l'article 35 alinéa 2 de la loi n° 2008-09 du 25 janvier 2008, le droit de reproduction *« s'applique, que la reproduction de l'œuvre soit totale ou partielle, qu'elle porte sur l'œuvre elle-même ou sur une œuvre qui en dérive, par voie de traduction et d'adaptation »*. Sur le plan pénal, l'article 142 de la loi du 25 janvier 2008 sur le droit d'auteur et les droits voisins incrimine aussi bien les reproductions à l'identique que les imitations de créations informatiques.

Le développement des techniques et l'avènement de l'Internet favorisent les actes de pillage de programmes. Ainsi, constituent des actes de contrefaçon, les reproductions à l'identique fréquemment dirigées contre les œuvres numériques. En droit pénal sénégalais du droit d'auteur, le champ de la reproduction de la violation du droit de reproduction est très large. Il est classique de relever que les reproductions destinées à l'usage privé constituent une exception au droit de reproduction. Mais, compte tenu du particularisme des créations informatiques, le législateur a organisé un régime dérogatoire qui exclut expressément en la matière l'exception de copie privée. C'est du moins ce qui résulte des dispositions de l'article 40 alinéa 2 de la loi n°2008-09 du 25 janvier 2008[65].

Cette solution constitue une transposition en droit interne sénégalais du droit communautaire qui répugne à autoriser la copie privée des œuvres informatiques, si aisée à réaliser. Par conséquent, le cybercriminel qui réalise une copie d'un logiciel ou d'une base de données pour un usage privé encourt les sanctions pénales de l'article 142 de la loi n°2008-09 du 25

[64] Ch. CARON, Droit d'auteur et droits voisins, Paris, Litec, 2006, p. 393, n°495.
[65] Qui dispose que l'exception de copie privée *« ne s'applique pas : (...)c) à la reproduction d'une base de données électroniques ; d) à la reproduction d'un programme d'ordinateur »*.

janvier 2008 sur le droit d'auteur et les droits voisins. Cependant, l'article 41 de la loi du 25 janvier 2008 réduit la portée de cette limite. Ce texte pose, le principe de l'admission de la copie de sauvegarde d'un logiciel, qui dispense le copieur de toute sanction pénale. Selon ce texte, *« le programme d'ordinateur peut donner lieu, de la part de l'utilisateur légitime, à une copie de sauvegarde destinée à remplacer l'original ».* Ainsi, en France, les auteurs admettent que plus d'une simple faculté, le titulaire d'une licence d'utilisation d'un logiciel dispose d'un véritable droit à la copie de sauvegarde destinée exclusivement au remplacement du programme[66]. Ce droit à la copie de sauvegarde, nécessaire à la préservation du logiciel, a pour but de protéger l'acquéreur légitime[67] d'un programme contre la destruction de son exemplaire[68]. Quoi qu'il en soit, les atteintes aux droits patrimoniaux des auteurs de créations informatiques concernent également le droit de communication au public.

L'article 142 de la loi n°2008-09 du 25 janvier 2008 érige également en infraction la violation du droit de communication au public de l'auteur d'une œuvre de l'esprit. Aux termes des dispositions de l'article 34 De cette loi, *« l'auteur a le droit exclusif d'autoriser la communication de son œuvre au public par tout procédé, notamment par voie de radiodiffusion, de distribution par câble ou par satellite, de mise à disposition sur demande de manière que chacun puisse avoir accès à l'œuvre de l'endroit et au moment qu'il choisit individuellement ».* Ce droit, traditionnellement qualifié de « *droit de représentation* », consiste à la communication de l'œuvre au public par un procédé quelconque. Il s'applique aux communications directes de l'œuvre au public, c'est-à-dire celles par lesquelles le public est directement en contact avec l'œuvre.

En France, le législateur a prévu un monopole spécial pour les concepteurs de logiciels s'écartant du droit commun, qui a pour siège les dispositions de l'article L.122-6 du Code de propriété intellectuelle. En effet, le droit de représentation a été amputé des droits patrimoniaux[69]. Cependant, en droit sénégalais du droit d'auteur, les droits patrimoniaux du concepteur du logiciel relèvent du droit commun du droit d'auteur. Concernant la violation des droits moraux des auteurs de créations informatiques, le législateur sénégalais a entendu dissiper toute ambiguïté sur la question de la protection pénale du droit moral des auteurs. Aux termes de l'article 144 de la loi du 25 janvier 2008 portant sur la cybercriminalité,

[66] A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 334, n° 550.
[67] Sur 'exigence jurisprudentielle d'une acquisition légitime du logiciel pour bénéficier de la copie de sauvegarde, CA Paris, 20 septembre 2005, Comm.com. électr., 2005, comm., 23, Obs. Ch. Caron.
[68] En ce sens, Ch. CARON, op. cit., p. 302, n°386
[69] Sur ce monopole spécial, Ch. CARON, *Droit d'auteur et droits voisins*, Paris, Litec, 2006, p. 262, n° 329.

intitulé *«Violation du droit moral », « est punie des mêmes peines la violation du droit moral de l'auteur et de l'artiste interprète »*. Ce texte, qui s'applique en principe aux créations informatiques, concerne toutes les prérogatives du droit moral.

Au-delà de la protection pénale des informations spécifiques que sont les nouvelles créations informatiques, dans une société marquée par la valeur patrimoniale acquise par l'information, la stratégie d'élargissement des incriminations contre les biens devrait s'orienter vers une protection pénale générale de l'information.

B. La protection pénale générale de l'information

Dans la société contemporaine de l'information, les formidables capacités de stockage, de traitement et de diffusion de l'information qu'offrent les TIC ont hissé l'information au rang de valeur marchande[70]. La législation a toujours consacré une protection pénale spécifique de certaines informations dites secrètes[71]. Devant la recrudescence des atteintes dirigées contre les informations de toutes sortes, il a été très vite envisagé en doctrine une protection de « l'information seule »[72] ou, pour reprendre une autre expression, une protection de « l'information en elle-même »[73]. Il s'agit en réalité d'une protection pénale générale de l'information envisagée indépendamment de son support physique. Au Sénégal, en vue d'adapter la répression aux évolutions du patrimoine, le législateur a élargi l'objet des infractions contre les biens par une stratégie d'intégration de l'information dans les principales infractions contre les biens. Par voie de conséquence, impérativement d'ailleurs il nous faudra réfléchir sur deux axes focaux, de prime abord, sur la réception de l'information dans le droit pénal du vol (1), avant de poser un regard analytique sur son intégration dans les autres atteintes juridiques aux biens (2).

1. La réception de l'information dans le droit pénal du vol

Dans la société moderne, l'information est devenue un actif stratégique dans les rapports humains. Lorsqu'elle est numérisée et circule à travers les câbles des ordinateurs et serveurs (fichiers de clientèle, données d'entreprise, etc.), elle est souvent l'objet d'atteintes de toutes

[70] A. AUMONIER et D. BRUTE DE REMUR, La protection de l'information comme enjeu de sécurité, IHESI, 2003, Paris.
[71] G. BEAUSSONIE, « La protection pénale de la propriété sur l'information », Dr. pén., n° 9, septembre 2008, études, p. 32 : *« De nombreuses informations sont déjà protégées par le droit pénal à titre spécial et selon différentes modalités »*.
[72] M.P. LUCAS DE LEYSSAC, « Une information seule est-elle seule susceptible de vol ou d'une autre atteinte juridiques aux biens », D. 1985, p. 43.
[73] J. DEVEZE, « Le vol des biens informatiques », JCP. 1985, p. 43.

sortes. Très vite, au Sénégal, bien avant l'entrée en vigueur de la loi sur la cybercriminalité, la question de la protection de l'information numérisée (fichiers, données d'entreprise, etc.) par le droit pénal des atteintes juridiques aux biens s'est posée en jurisprudence. L'analyse de certaines décisions rendues par les juridictions du fond révèle que, sous l'empire de la législation antérieure, les juges ont admis la possibilité d'une soustraction portant sur une information indépendamment de son support. Le 23 décembre 2005, le tribunal régional de Thiès a jugé un cas de « vol » portant sur le support numérique d'une pièce théâtrale dans l'affaire dite « Mor Todjangué »[74], du nom du titre de la célèbre pièce de théâtre tournée en 2005 par la troupe « Soleil Levant » de Thiès. En l'espèce, après le montage de ladite pièce théâtrale destinée à être dupliquée en France et au Sénégal, l'œuvre de l'esprit a été copiée par D. K. de l'ordinateur de service de la société El Bachir Production, avant d'être diffusée et mise en vente, alors qu'elle n'était pas encore officiellement sortie. Le tribunal a déclaré le prévenu coupable de vol du support de données contenant l'œuvre de l'esprit. Selon les juges: « le sieur D. K. en copiant lesdites données dans un CD aux fins d'usage ultérieur sans le consentement de son légitime propriétaire a commis un vol tel que prévu par les dispositions de l'article 364 du code pénal ». Il résulte de la motivation du juge que l'acte de copiage de l'œuvre de l'esprit numérisée sur CD (information originale) a été considéré comme une soustraction au sens de la loi[75]. On retrouve cette même admission implicite de la soustraction informationnelle dans un jugement du 9 mai 2006 rendu par le tribunal régional hors classe de Dakar, à propos de l'affaire dite de « la Clinique du Cap ». Dans cette espèce, M. D., technicienne supérieure de laboratoire à ladite clinique, s'était introduite dans le laboratoire de biologie en compagnie d'un informaticien. Elle avait mis en marche l'ordinateur de service stockant les données relatives aux prélèvements et aux résultats d'analyse des patients de la clinique avant d'être interpellée. Les mis en cause furent cités directement devant le tribunal sous la prévention de tentative de vol en réunion. La prévenue fut relaxée, mais seulement pour défaut de preuve du commencement d'exécution. Dans sa démarche intellectuelle, le juge correctionnel a cristallisé toute la problématique du «vol d'information » à la chose objet du vol. On peut lire dans un attendu du jugement que «l'un des éléments constitutifs de ce délit suppose l'existence d'une chose objet de la soustraction, que cette chose non définie par la loi peut être matérielle ou immatérielle, que les données informatiques qui sont stockées sur

[74] TR Thiès n° 1603, 23 décembre 2005, affaire « Mor Todjangué », inédit.

[75] La confusion de qualification qui s'est glissée dans cette décision est manifeste. En effet, dès lors que l'information objet de la reproduction illicite constitue une information originale (œuvre de l'esprit), il n'est pas douteux que la qualification de droit commun de vol est inappropriée. En réalité, la reproduction sans autorisation d'une œuvre de l'esprit constitue une contrefaçon et non un vol.

certains supports qui en gardent la mémoire grâce à leur propriété notamment magnétique constituent comme l'énergie une chose immatérielle, donc susceptible de vol »[76]. Cette décision a été confirmée par un arrêt de la cour d'appel de Dakar du 16 avril 2007[77]. Selon la juridiction d'appel : « au sens de l'article 364 du code pénal, l'un des éléments constitutifs du délit de vol, suppose l'existence d'une chose, objet de la soustraction ; que cette chose non définie par la loi, peut être matérielle ou immatérielle ; qu'ainsi les données informatiques sont susceptibles de vol ».

En jurisprudence, la dématérialisation du délit de vol est une véritable tendance, puisque le juge pénal sénégalais a déjà admis un vol portant sur des programmes télévisés, c'est-à-dire un vol de services. En effet, dans un jugement du tribunal régional de Diourbel rendu le 3 juin 2010[78], des jeunes informaticiens utilisaient des décodeurs pirates et autres amplificateurs d'images pour capter des programmes de la chaine Canal Horizon et Walfajiri TV. Ils consentaient, par la suite, des abonnements à des tiers, moyennant le versement de sommes d'argent. Le tribunal a disqualifié les faits d'exploitation frauduleuse d'un réseau privé de télécommunication reprochés aux prévenus[79] en vol de services. Selon les juges, « le fait pour les prévenus d'utiliser des moyens frauduleux tels que des décodeurs pirates pour capter des programmes de Canal Horizon et de Walfajiri qui sont des chaînes réservées à un public d'abonnés au préjudice des exploitants traduit avec éloquence qu'ils ont soustrait frauduleusement des services qui sont des choses appartenant à ces derniers à leur insu et contre leur gré »[80]. Le tribunal correctionnel de Diourbel a assimilé la captation de programmes télévisuels à l'insu des exploitants à une soustraction frauduleuse au sens de l'article 364 du code pénal sénégalais. Mais, si le tribunal ne s'en explique pas vraiment, c'est certainement en raison des difficultés à caractériser en l'espèce l'acte matériel de soustraction. En réalité, la nature immatérielle et reproductible des ondes hertziennes n'est pas sans perturber la théorie générale du vol, en particulier le mécanisme de la soustraction.

En France, dans l'arrêt « Canal Plus » rendu par la cour d'appel de Paris, le 24 juin 1987, les magistrats ont été saisis d'un cas similaire de captation frauduleuse d'une émission télévisée codée à l'aide d'un «décodeur pirate ». Mais le raisonnement retenu a été très différent : « le

[76] TRHC Dakar n° 1981 du 9 mai 2006, affaire de la Clinique du Cap, inédit
[77] CA Dakar, n° 680 du 16 avril 2007, inédit.
[78] TR Diourbel, n° 551 du 3 juin 2010, inédit.
[79] V. ancien article 58 du code des télécommunications du Sénégal.
[80] Cette décision a été d'ailleurs infirmée par un arrêt de la CA de Dakar, n° 378 du 18 mars 2013, inédit. La juridiction d'appel a fondé l'infirmation sur le fait que le juge d'instance a disqualifié les faits en vol de service sans avoir au préalable mis les parties en position de discuter cette dernière prévention.

branchement frauduleux n'a pas pour effet de déposséder le propriétaire du programme qui continue à diffuser, ni le téléspectateur abonné qui ne subit aucun trouble dans sa réception(…) la notion de soustraction ne se conçoit pas puisque aucune atteinte directe n'est portée au corpus de la possession de la société productrice tant sur l'émission en clair que sur l'émission cryptée »[81]. Le législateur français a été d'ailleurs obligé d'intervenir pour combler ce vide juridique, en adoptant une incrimination spécifique de captation frauduleuse de programmes télévisés réservés à un public déterminé[82].

À la faveur de la loi du 25 janvier 2008 portant sur la cybercriminalité, le législateur a envisagé de consacrer la théorie du vol l'information. Aux termes des dispositions de l'article 431-53 du code pénal issues de la loi du 25 janvier 2008 sur la cybercriminalité : « la soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol ». Au Sénégal, l'accueil du vol d'information a été largement tributaire du recours au système de l'assimilation de la soustraction frauduleuse d'information au vol. En effet, l'article 431-53 du code pénal n'a pas identifié la soustraction frauduleuse d'information au préjudice d'autrui au vol, mais l'a simplement assimilé à ce délit[83]. Mais, la réception de l'information dans le droit pénal du vol ne semble pas avoir dissipé les difficultés juridiques du vol portant sur une information. En effet, dans tous les cas, le juge pénal devra caractériser un acte matériel de soustraction pour entrer en voie de condamnation pour vol d'information. Ce qui n'est pas chose aisée. Le juge pénal sénégalais a déjà fait application de l'article 431-53 du code pénal sur le vol d'information, pour la première fois, à notre connaissance, dans un jugement rendu par le tribunal régional de Thiès le 18 septembre 2012, à propos de l'affaire de l'Agence New-Look Business[84]. Dans cette espèce, P.Y, ingénieur informaticien, chargé du service de la clientèle de l'Agence New-Look Business, avait pendant son service, copié dans sa clé USB des données de l'agence relatives aux clients et aux actes de cession. Après avoir cessé ses fonctions à ladite agence, dans le courant du mois d'octobre 2011, il proposait à ses responsables, la remise de la clé USB moyennant le versement de la somme de 1 500 000 francs CFA. Le parquet de Thiès avait poursuivi le prévenu pour vol d'information au préjudice de l'employeur en visant les dispositions de l'article 431-53 du code pénal. Le

[81] CA Paris, 24 juin 1987, affaire dite Canal Plus, Gaz. Pal. 1987. 2. 512, note De Marchi ; RSC 1987, p. 211, obs. Bouzat.

[82] Sur le piratage audiovisuel, J. SAINATI, « La lutte contre la piraterie audiovisuelle en France », Rev. inter. pol. crim., mars-avril 1992, p. 21 ; M. VERON, Droit pénal spécial, 11e édition, Paris, Dalloz, 2006, p. 254, n° 380.

[83] V. P.A. TOURÉ, « Le vol d'information : virage ou mirage du droit pénal sénégalais ? », à paraitre ; P.A. TOURÉ, Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal, Thèse Doctorat, Saint-Louis, 2010, n° 178 et s.

[84] TR Thiès, n° 505/2012 du 18 septembre 2012, affaire de l'Agence New-Look Business, inédit.

tribunal a déclaré le prévenu coupable des faits à lui reprochés au motif qu'il « a copié des données relatives à l'activité de l'Agence New-Look Business, à sa clientèle, à son patrimoine et ce, à l'insu de son employeur lequel a soutenu, sans être contredit par le prévenu, qu'il avait interdit aux employés de faire des copies des informations allant jusqu'à installer un système de sécurité désactivé à chaque fois par celui-ci ». En jugeant dans les décisions précitées que les données informatiques peuvent faire l'objet de vol, les juges du fond ont admis, sans motivation, qu'elles peuvent être soustraites. Cependant, dans l'analyse pénale classique, la soustraction ne peut se concevoir sans une dépossession, c'est-à-dire un dépouillement du propriétaire de la chose, au moins un instant[85]. Or, la nature infiniment reproductible de l'information conduit à une dilatation de la notion de soustraction. En réalité, l'ubiquité et le caractère « répétitible » de l'information qui, surtout lorsqu'elle est numérisée[86], a la faculté incontestable de se retrouver en même temps dans plusieurs patrimoines, constituent « un ultime rempart contre la reconnaissance du vol d'information »[87]. Les informations stockées dans les systèmes d'information qui sont la cible des pirates sont, pour la plupart du temps, simplement dupliquées ou téléchargées et non ravies, parfois à l'insu même de leurs titulaires. C'est tout le sens de l'aphorisme de Barlow : « si je vous vends une information, nous sommes deux à la posséder »[88]. La doctrine majoritaire repousse ainsi l'idée de toute soustraction d'information au motif que « les données ne sont pas soustraites de l'ordinateur où elles demeurent intactes»[89].

Mais, devant l'inadaptation des conceptions matérielle et juridique de la soustraction à l'information, une partie de la doctrine a proposé une reformulation du concept de soustraction plus adaptée au cyberespace, par la consécration d'une conception économique. Selon cette approche économique de la soustraction, il y aurait alors soustraction par le simple

[85] OLLARD, La protection pénale du patrimoine, Paris, Dalloz, coll. Nouv. Bibl. de thèses, 2010, p. 299, n° 515. Selon cet auteur, la notion de soustraction évoque irrésistiblement « l'idée d'un enlèvement, d'une frustration, d'un dépouillement du propriétaire, qu'il s'agisse du dépouillement de la chose elle-même – soustraction matérielle – ou du dépouillement de la possession – soustraction juridique »

[86] Sur la question du vol de données informatiques, G. VANDENBERGHE, « Vol de données informatiques : une révolution dans le droit pénal ! », DIT, 1986, n° 2, p. 95.

[87] D. CIOLINO-BERG, « Vol d'information sur Internet », Comm. com. électro. novembre 2003, p. 22.

[88] J.P BARLOW, cité par J. -F. CASILE, Le code pénal à l'épreuve de la délinquance informatique, Thèse, Aix-Marseille, 2002, p. 380, n° 1058.

[89] J. PRADEL et C. FEUILLARD, « Les infractions commises au moyen de l'ordinateur », Rev. dr. pén et crim, 1985, p. 317 ; dans le même sens, J. DEVEZE, « Le vol des biens informatiques », JCP, 1985, I, 3210, n° 18 ; V. M. CHAWKRI, « Le vol d'informations : quel cadre juridique aujourd'hui ? », disponible à l'adresse suivante http://www.droit-tic.com/pdf/vol_information.pdf : « On pourrait parler de partition, de partage de connaissance, mais pas d'une dépossession pouvant tomber sous le coup de la loi pénale. Le détenteur de l'information perdra son monopole et son exclusivité, mais pas la possession de cette information » ; J. HUET et H. MAISL, Droit de l'informatique et des télécommunications, Paris, Litec, 1989, p. 869 et 870 ; S. DETRAZ, « Vol du contenu informationnel de fichiers informatiques », note sous cass. crim., 4 mars 2008, D. 2008, jur, p. 2213.

fait de priver autrui de l'exclusivité de la possession de l'information. La soustraction informationnelle résiderait dans la perte de l'exclusivité de l'information[90] qui, après avoir été dupliquée par un tiers, peut être complètement vidée de sa valeur patrimoniale[91]. Cependant, du point de vue de la politique criminelle, cette nouvelle approche de la soustraction est susceptible d'étendre sensiblement le domaine de la répression du vol. Dès lors que la soustraction est entendue comme une usurpation de l'exclusivité de l'information, le délit de vol logiquement serait consommé dès la prise de connaissance de l'information. Dès cet instant, le propriétaire est privé de son usage exclusif. La seule captation intellectuelle de l'information, sa seule prise de connaissance semble dès lors caractériser la soustraction constitutive du vol. On peut légitimement se demander si, à la lumière de l'approche économique de la soustraction, le fait de lire un document, de surprendre une conversation, ne constituerait pas une soustraction[92]. Par ailleurs, l'avènement de cette nouvelle conception de la soustraction contribuerait à défigurer exagérément la philosophie originelle du délit de vol. L'article 364 du code pénal sénégalais évoque la soustraction d'une « chose » appartenant à autrui et non celle de sa valeur (l'exclusivité de l'information). Dès lors, considérer la dépréciation de la valeur de l'information comme un acte de soustraction reviendrait à ériger le préjudice économique en une composante du vol en dehors de toute prévision législative[93]

En définitive, dans la théorie générale du vol, la caractérisation de la soustraction d'information se heurte à de sérieux obstacles juridiques. Il y a une dimension concrète irréductible dans l'appréhension frauduleuse constitutive du vol[94].

2. L'intégration de l'information dans les autres atteintes juridiques aux biens

En droit pénal spécial, les autres infractions contre les biens désignent les appropriations frauduleuses autres que le vol. Il s'agit notamment de l'abus de confiance, de l'escroquerie, du recel, l'extorsion de fond et du chantage. Les trois infractions fondamentales que sont

---

[90] S. DETRAZ, R. OLLARD, J.-C. SAINT-PAUL, « Contre le vol d'information », in V. MALABAT, B. DE LAMY et M. GIACOPELLI (dir.), « La réforme du code pénal et du code de procédure pénale. Opinio doctorum», Paris, Dalloz, 2009, p. 109.

[91] P. LUCAS DE LEYSSAC, « Vol », Rép. Pén. et Proc. Pén. Paris, Dalloz, mai 2005, n° 37.

[92] D. CHILSTEIN, « Le salarié et les documents de l'entreprise », Dr. pat., n° 149, juin 2006, p. 61 : « Or, dans la logique de la dématérialisation de l'infraction, la prise de connaissance non autorisée s'apparente nécessairement à une soustraction frauduleuse (…) En effet, l'élément matériel de l'infraction se modèle forcément à son objet immatériel » ; R. OLLARD, La protection pénale du patrimoine, Thèse Bordeaux IV, 2008, Dalloz, 2010, p. 306, n° 527 ; plus récemment, R. OLLARD et F. ROUSSEAU, Droit pénal spécial, Paris, Bréal, 2011, p. 255.

[93] S. DETRAZ, R. OLLARD, J.-C. SAINT-PAUL, op. cit., p. 110.

[94] D. CHILSTEIN, « Le salarié et les documents de l'entreprise », Dr. pat., n° 149, juin 2006, p. 61 ; R. OLLARD, op. cit., p. 309, n° 535.

l'escroquerie qui sera étudiée dans la section suivante, l'abus de confiance et le recel constituent la véritable matrice criminologique de la délinquance informatique et ont souvent pour cible l'information. Ainsi, dans le cadre de la stratégie de modernisation du droit pénal des atteintes aux biens, il s'agira au préalable de montrer les difficultés de la réception de la ressource informationnelle dans ces infractions avant d'étudier les modalités de son intégration dans l'objet de ces délits. Dans la loi portant sur la cybercriminalité, la dématérialisation des infractions contre les biens n'a curieusement pas concerné le délit d'abus de confiance. En tout état de cause, le juge sénégalais a déjà eu l'occasion de répudier la thèse de l'abus de confiance d'information dans l'affaire « Résidence James.com » jugée par le tribunal régional hors classe de Dakar, le 19 juillet 2007[95]. Dans cette espèce, la promotrice d'une société, dans le cadre de ses activités commerciales, avait créé un site web dénommé « résidence James.com » hébergé par la société PEXE Sarl, avant de le faire enregistrer auprès d'un registrar. À l'expiration du contrat d'hébergement, elle avait donné mandat à la société PEXE d'opérer ledit transfert. Cependant, cette société n'a exécuté que le transfert technique auprès d'un nouveau registrar, en s'appropriant ainsi le nom de domaine qu'il a enregistré pour son compte personnel. La partie civile a cité directement le directeur de la société PEXE devant le tribunal correctionnel sous la prévention d'abus de confiance. Elle a fait valoir que ce dernier a détourné à son profit son nom de domaine. Le tribunal a jugé que: « le délit d'abus de confiance suppose, en droit sénégalais, outre l'existence d'un des contrats limitativement prévus par l'article 383 du code pénal, la remise d'une chose corporelle ayant une valeur juridique (…) ; que l'article 383 du code pénal sénégalais ne vise dans son contenu que les choses corporelles ». Sur ce fondement le prévenu fut relaxé. Cette décision a jugé, sous l'empire de la législation antérieure, que le nom de domaine, bien immatériel par essence, est insusceptible d'abus de confiance. Cette solution est tout à fait fondée en droit puisque dans la théorie générale de l'abus de confiance, l'exigence de la matérialité de la chose objet de l'infraction d'abus de confiance, ne souffre pas de doute[96]. Pourtant, l'essor contemporain des TIC s'est accompagné du développement des techniques de fraudes portant sur des valeurs et ressources patrimoniales, comme les informations. Il n'est pas rare de relever des cas de détournement d'informations stratégiques, à l'image du

[95] TRHC Dakar, n° 19 juillet 2007, affaire « Résidence Saint James », inédit.

[96] S. JACOPIN, « Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse », Dr. pén, avril 2001, p. 4 ; M. VERON, Droit pénal spécial, Paris, Sirey, 11e éd. juin 2006, p. 293, n° 440 ; P. CONTE, Droit pénal Spécial, Paris, Litec, 3e édition, 2007, p. 323, n° 555 : « l'article 408 énumérait la liste des objets qui pouvaient être détournés. Des biens corporels étant seuls visée, l'infraction n'existait pas en cas de détournement d'un bien incorporel » ; cependant contra, M. P LUCAS DE LEYSSAC, « Une information seule est-elle seule susceptible de vol ou d'une autre atteinte juridique aux biens », D. 1985. Chron. p. 51, n° 48 et 49.

numéro de carte de crédit ou de fichiers de clientèle, de nature à porter atteinte au patrimoine d'autrui. La dématérialisation du délit d'abus de confiance aurait le mérite sans nul doute de faciliter une répression judiciaire de ces comportements frauduleux inquiétant de la société de l'information. Cette lacune devrait être corrigée par le législateur pour mieux lutter contre la cybercriminalité au Sénégal. La réforme du Code pénal et du Code de procédure pénale envisage de dématérialiser l'infraction d'abus de confiance. Le nouveau texte d'incrimination de ce délit prévoit qu'il pourra désormais porter sur un « bien quelconque ». Mais il ne semble pas en être de même de l'infraction de recel.

Sous l'empire de la législation classique, la jurisprudence de la première chambre correctionnelle du tribunal régional hors classe de Dakar sur le recel d'information était caractérisée par une certaine ambiguïté. En effet, sur cette même question, la première chambre pénale du tribunal régional hors classe de Dakar a rendu deux décisions difficilement conciliables. Dans le jugement rendu le 21 novembre 2006, à propos de l'affaire « Madiambal DIAGNE »[97], le prévenu, en sa qualité de directeur de publication du journal « le Quotidien », avait été poursuivi de recel, pour avoir publié dans ledit journal un article qui reproduisait un procès-verbal d'interrogatoire au fond de l'ancien Premier ministre Idrissa SECK dans l'affaire des «Chantiers de Thiès ». Le tribunal avait disqualifié les faits en publication interdite d'actes de procédure faite avant sa lecture en audience publique conformément à l'article 267 du code pénal. Mais, au préalable les juges correctionnels avaient été amenés à rejeter la possibilité d'un recel d'information provenant du délit de violation du secret de l'instruction : « attendu que toutefois, quelle que soit l'infraction d'origine, la chose recelée doit avoir une existence matérielle ; qu'elle ne saurait dès lors porter sur une telle information, mais seulement sur son support matériel ; qu'au regard de ce principe, le recel ne peut être retenu en l'espèce, qu'en effet, il n'a pas été dit que le procès-verbal support matériel des informations publiées a été dérobé ou subtilisé ». Ce jugement s'inscrit dans le cadre de la thèse matérialiste du recel, en ce qu'il n'envisage que le recel portant sur les supports matériels des informations (en l'espèce, le procès-verbal d'interrogatoire au fond de M. Idrissa SECK) à l'exclusion de celui ayant pour assiette les informations indépendamment de leur support. Cependant, dans l'affaire « Robert TABET », jugée le 1er avril 2008[98], la première chambre correctionnelle du tribunal régional hors classe de Dakar a admis la possibilité d'un recel d'une information provenant d'un délit d'initié. Dans cette espèce, pour

[97] TRHC Dakar, n° 5310 du 21 novembre 2006, affaire Madiambal DIAGNE, inédit.

[98] TRHC Dakar 1er avril 2008, affaire Robert TABET, inédit.

les besoins de l'obtention d'un prêt auprès du Crédit Lyonnais, R. T avait accepté de consentir une hypothèque sur son immeuble. Mais, malgré les divers remboursements effectués entre les mains du Crédit Lyonnais, le responsable du service contentieux a initié une procédure de vente forcée de son immeuble qui finalement a été adjugé à la banque. Par la suite, informé de l'intention de la banque de céder l'immeuble litigieux, B. T, qui se trouve être l'époux du responsable du service contentieux, chargé de la gestion du dossier de recouvrement du prêt accordé à R. T, l'a acquis à la somme de 80 000 000 de francs CFA. À l'issue de l'instruction du dossier, B. T a été ainsi renvoyé devant le tribunal pour complicité de délit d'initié. Le tribunal correctionnel a disqualifié les faits reprochés au prévenu en recel de délit d'initié au motif que la responsable du service contentieux a commis un délit d'initié au sens de l'article19, alinéa 2, de l'ancienne loi n° 90-06, du 26 juin 1990, portant réglementation bancaire[99]. Selon le tribunal, cette dernière a, dans le cadre de ses fonctions, mis à la disposition de son époux de manière illicite une information confidentielle dont elle a eu connaissance, à savoir l'intention de la banque de céder l'immeuble aux conditions fixées. Les magistrats ont précisé que le délit de recel de délit d'initié résulte de ce que : « le prévenu, ayant connaissance du caractère privilégié et de l'origine frauduleuse de l'information fournie par son épouse, l'a utilisé pour son compte en initiant une procédure de rachat de l'immeuble avec la banque » et « qu'il en a également profité dans la mesure où la transaction a abouti et que ledit immeuble est devenu sa propriété ». Cette décision rappelle l'arrêt « Pechiney Triangle » rendu par la Cour de cassation française, le 26 octobre 1995, ayant déclaré receleur un individu qui a réalisé, en connaissance de cause, des opérations sur le marché boursier grâce à une information privilégiée[100]. Le jugement de première instance a été confirmé dans toutes ses dispositions par un arrêt de la cour d'appel de Dakar, du 24 juillet 2009[101]. Récemment, la Cour suprême du Sénégal, dans un arrêt rendu le 1er avril 2010, a rejeté le pourvoi formé contre la décision de la cour d'appel de Dakar, en précisant qu'en l'espèce, le

[99] Aux termes l'article 19 alinéa 2 de la loi n° 90-06 du 26 juin 1990, « Il est interdit aux mêmes personnes (personnes qui concourent à la direction, à l'administration, à la gérance, au contrôle ou au fonctionnement des banques et des établissements financiers) d'utiliser les informations confidentielles dont elles ont connaissance dans le cadre de leur activité, pour réaliser directement ou indirectement des opérations pour leur propre compte ou en faire bénéficier d'autres personnes ».

[100] Cass. crim., 26 octobre 1995, Bull. crim, n° 328 ; RSC 1996, p. 660, obs. Ottenhof.

[101] CA Dakar, n° 555 du 24 juillet 2009, inédit : « qu'il s'avère ainsi qu'en utilisant des informations encore secrètes et donc confidentielles vu les circonstances présentant les critères d'une origine frauduleuse, illégale à l'égard de sa défunte épouse de qui, il a obtenues en toute connaissance de cause de l'irrégularité du procédé, le prévenu a racheté l'immeuble ; que ledit prévenu a alors utilisé, pour son compte, les informations avec une conscience du caractère frauduleux de ce qu'il faisait, que dès lors ses agissements sont caractéristiques d'un recel de délit d'initié ».

délit de recel découle de « l'appropriation d'une information illégalement communiquée »[102] Depuis que le recel tirer profit a été admis par la jurisprudence française, cette infraction, qui peut avoir pour assiette tous biens de provenance délictueuse, a toujours pu s'appliquer à un bien incorporel du moment que celui-ci pouvait entrer dans le cadre de l'infraction d'origine[103]. En droit pénal, le profit est entendu au sens courant du terme comme « tout ce qui est issu de l'infraction d'origine, sans qu'il y ait lieu de considérer selon la nature corporelle ou incorporelle »[104]. Ainsi, la dématérialisation de l'élément matériel du recel devrait emporter celle de son objet. Le recel est une infraction de conséquence se greffant à une infraction principale fondée sur la seule idée de profit et d'enrichissement procuré par la jouissance d'une chose de provenance délictueuse[105]. Il n'y a aucun obstacle théorique à admettre un profit tiré d'une chose immatérielle comme une information ayant une origine frauduleuse[106]. C'est certainement la raison pour laquelle le rejet de la « recelabilité » d'une information est présenté dans les travaux les plus récents de la doctrine comme une «erreur»[107]. En tout état de cause, la loi du 25 janvier 2008 portant sur la cybercriminalité a eu le mérite de dissiper l'ambigüité qui caractérisait la jurisprudence, en consacrant de façon explicite le recel portant sur une information[108]. L'article 431-57 du code pénal sanctionne «ceux qui auront recelé des informations enlevées, détenues ou obtenues à l'aide d'un crime ou d'un délit ». In fine, ne perdons guère de vue que, la criminalité du numérique, est avant

[102] CS du Sénégal, n° 78 du 1er avril 2010, inédit.

[103] M.L. RASSAT, Droit pénal spécial, Précis Dalloz, 2e édition 1999, p. 180, n° 182 ; du même auteur, Droit pénal spécial, infractions du code pénal, 6e édition, Parios, Dalloz, 2011, p. 209, n° 172

[104] R. OLLARD, La protection pénale du patrimoine, Paris, Dalloz, coll. Nouv. Bibl. de thèses, 2010, p. 187, note n° 848 ; D. CHEVROTIN, « Bévue sur le caractère non "recelable" d'une information », Dr. pén. mars 2001, p. 12 ; C. DE JACOBET DE NOMBEL, « Recel de choses », J.-Cl, pén, Code, 2008, n° 20 ; V. MALABAT, Droit pénal spécial, Paris, Dalloz, 2007, 3e édition, n° 826.

[105] J. DEVEZE, « Les qualifications pénales applicables aux fraudes informatiques », in VIIIe Congrès AFDP, « Le droit criminel face aux technologies modernes de la communication », Paris, Economica et ADI, 1986, p. 197.

[106] En ce sens, V. en droit pénal camerounais, J.-C. NCHIMI MEBA, « La recherche de l'intention dans le recel », Penant, n° 806, juin-octobre 1991, p. 238 : « Il s'agit d'une tendance à la dématérialisation, puisque la chambre criminelle semble admettre l'opinion selon laquelle le recel peut porter sur une information seule (…) Dans la généralité de leurs termes, les articles 460 du code pénal français et 324 du code pénal camerounais s'appliquent aussi à toutes les autres infractions comme la violation du secret professionnel, de secret de fabrique, de détournement d'informations ».

[107] J. DEVEZE, « À propos de l'évolution des délits contre les biens », in « Libre droit », Mélanges en l'honneur de Philippe LE TOURNEAU, Paris, Dalloz, 2006, p. 362 : « C'est donc par erreur que la chambre criminelle a affirmé qu'une information quelle qu'en soit la nature ou l'origine échappe aux prévisions des textes qui incriminent le recel » ; M.L. RASSAT, op. cit., p. 180, n° 182 ; D. CHEVROTIN, « Bévue sur le caractère non "recelable" d'une information », Dr. pén. mars 2001, p. 4. L'auteur propose une véritable « démonstration du caractère recelable d'une information », qui aurait pour conséquence une meilleure protection pénale des secrets.

[108] C. DE JACOBET DE NOMBEL, « Le recel d'information », Dr. pén., décembre 2008, p. 41 ; D. CHEVROTIN, « Bévue sur le caractère non recelable d'une information », Dr. pén. mars 2001, p. 4.

tout subsidiaire à la communication. En réalité, c'est une criminalité qui passe le plus souvent par la communication

SECTION 2 : LE NUMERIQUE, CRIMINALITE PAR LA COMMUNICATION

C'est celle commise au moyen du réseau. Ce modernisant, les criminels « classiques » se sont mis à l'heure du Net. Ils ont bientôt découvert le côté « bénéfique » d'Internet, porteur de nouvelles possibilités et d'opportunités, et ont perverti le progrès technologique. Dans cette catégorie, les criminels cherchent à en tirer profit et moins à perturber le réseau Internet qu'à se l'approprier. De facto, la convivialité d'Internet et la fluidité nouvelle des frontières du virtuel et du réel ouvrent d'inquiétantes possibilités pour la commission d'infractions de droit commun (paragraphe 1). Le réseau numérique est devenu aujourd'hui un moyen de commission d'infractions anciennes (paragraphe 2).

Paragraphe 1 : L'internet, un moyen de réalisation d'infractions de droit commun

Il s'agira de porter notre regard sur des comportements strictement interdit par la loi pénale qui portent atteinte juridiquement aux biens, les infractions contre les personnes, les infractions contre les mœurs et les infractions contre la famille. Dans cette phase, nous nous étendrons sur deux axes. Le premier est porté sur les infractions contre les personnes (A) et le second, celles contre les biens (B).

A. Les infractions portant atteinte aux particuliers

Notre champ analytique, portera dans un premier temps sur les infractions contre les personnes avec l'exemple de la cyberpornographie (1), avant de voir dans un second temps le risque d'exposition des mineurs à contenus illicites (2).

1. Les infractions contre les personnes : l'exemple de la cyberpornographie

La « pornographie infantile » vise : « toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ». Le législateur sénégalais, prenant en charge cette nouvelle forme de délinquance, s'est inspiré de la convention européenne sur la cybercriminalité. On peut même dire qu'il a repris les termes de ladite convention[109]. Définir la pornographie infantile est une tâche particulièrement complexe. Les normes appliquées au sein de chaque société et de chaque

[109] V. article 431-7, 431-34, 431-53 du CP

pays sont extrêmement subjectives et subordonnées à différentes convictions morales, culturelles, sexuelles, sociales et religieuses qui ne se traduisent pas aisément dans les lois. Même en se limitant à une définition légale de la pornographie infantile, ce concept est difficile à cerner. La définition légale de l'enfant et celle de la pornographie infantile diffèrent fortement d'un pays à l'autre. La Convention des Nations Unies relative aux droits de l'enfant ratifiée par 191 Etats membres, donne une définition large et internationale de l'enfant. Dans son article premier, elle stipule : " Au sens de la présente Convention, un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable"[110]. Ainsi, le Conseil de l'Europe qualifie la pornographie infantile en termes généraux comme " tout matériel audiovisuel qui utilise des enfants dans un contexte sexuel ", ce qui recouvre les films, les disques, les bandes dessinées, etc. En outre, au-delà de la définition, il n'y a que peu d'Etats qui interdisent à la fois, la production, la distribution et la détention de ce type de matériel. C'est pourquoi, il est important d'adopter une définition large, interdisant toutes les formes de production, de diffusion et de possession de tout type de documents incitant à l'exploitation sexuelle des enfants (âgés de moins de dix-huit ans)[111]. Après ces éclaircissements, nous allons démontrer

[110] Convention relative aux droits de l'enfant, CRC/C/SR.752 du 28 février 2002.

[111] Au Sénégal, le code pénal en son article 431-34 CP incrimine la production, l'enregistrement, l'offre, la mise à disposition, la diffusion, la transmission d'une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique. Ce texte a pour objet de lutter contre les producteurs de pornographie infantile, à savoir les réseaux pédopornographies et éditeurs de sites de pornographie infantile. L'article 431-35 du CP sanctionne la consommation de la pédopornographie c'est-à-dire l'action de se procurer à soi-même ou à autrui, l'importation ou l'exportation d'une image ou d'une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique. De même la simple possession d'une image ou d'une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées (article 431-36 alinéa 1e CP). La loi en termes clairs, a érigé comme infractions liées à la pornographie infantile les comportements suivants :

- la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

-l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

- la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

- le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

- la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. La loi vise également le délit de facilitation de l'accès à des données à caractère pédopornographique. Il peut s'agir d'images, de documents ou de représentation à caractère de pornographie infantile à un mineur (article 431-36 al 2 CP).

Le législateur protège les mineurs contre le risque d'exposition à des contenus pédopornographiques. Il s'agit de toute représentation de manière visuelle:

l'aspect transfrontalier en nous intéressant aux profils des exploiteurs et les liens entre la pédopornographie et la traite des enfants. Les exploiteurs de pornographie infantile sont les producteurs, les distributeurs et les utilisateurs et ils peuvent se retrouver au sein d'une large partie de la population. Ils sont composés d'individus ou de groupes de personnes qui sont à tous les niveaux de la société qui contribuent à ces pratiques d'exploitation. Ils sont constitués pour la plus part en réseaux. Certains parlent même d'entreprises de pédopornographies.

Cette tendance ne fait que s'amplifier puisque l'accessibilité accrue de la pornographie enfantine et le niveau élevé de l'anonymat rendue possible par l'utilisation croissante de l'informatique ont développé une nouvelle catégorie de consommateurs, il s'agit d'individus qui recherchent un matériel pornographique insolite (pornographie impliquant de jeunes enfants, des animaux, de la torture, etc.). Il ne faudrait donc pas utiliser le vocable général de "pédophile", il serait plus approprié dans un premier temps, pour éviter d'éventuels amalgames, de parler d'exploiteurs d'enfants sans faire de distinction quant à leur état mental et laisser aux psychiatres le soin d'en apprécier. La pornographie infantile, est une forme de criminalité transnationale organisée. Les acteurs de cette forme de criminalité sont constitués en réseaux et sévissent dans des pays différents et leurs actions sont facilitées par l'internet. La prostitution en ligne a opéré un déplacement de la rue vers le web. Tout ce qui se faisait dans la rue était transposé dans les réseaux numériques. Internet a en effet contribué au développement de nouvelles formes de prostitution : de l'escorting, sans doute la forme la plus connue de prostitution sur Internet, au troc sexuel (échange de services divers contre des relations sexuelles), en passant par le système de sex tours (des jeunes femmes, préalablement sélectionnées par des clients sur un sites d'escorting), « se déplacent sur le territoire national», afin de se présenter à des rendez-vous fixés par SMS. Tout se passe de façon dématérialisée. Les réseaux de proxénétisme ont très vite su faire évoluer leurs méthodes et s'adapter aux conditions de l'Internet.

Cet espace virtuel favorise des pratiques pédophiles, notamment l'extorsion (contraction de « sexe » et « extorsion ») ou chantage à la webcam, une pratique, utilisée par les pédophiles, et qui consiste à se procurer des images inappropriées d'un mineur pour ensuite le menacer de

---

- un mineur se livrant à un comportement sexuellement explicite;

- une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

- des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

Une facilitation de la mise en relation des

les envoyer à sa famille ou à ses amis afin d'en obtenir de faveurs sexuelles ou monétaires[112]. Il se double le plus souvent de celui de chantage à la webcam[113]. On note un engouement des délinquants pour ce nouvel espace qui offre des avantages pour tous les secteurs et, plus spécifiquement, pour le secteur prostitutionnel. La première caractéristique d'Internet est l'anonymat, renforcé par l'utilisation de « pseudos ». Du fait de cette assurance de « discrétion », « très rapidement, les réseaux criminels ont utilisé Internet » afin de se créer et « de pouvoir recruter »[114]. Cet anonymat, outre le fait qu'il permet aux délinquants de monter des réseaux criminels, a aussi pour effet de stimuler l'achat de services sexuels auprès de la clientèle. Selon Christiane Feral-Schuhl, avocate et ancienne Bâtonnière de Paris, « il est peut-être plus difficile de se promener dans la rue que de se cacher chez soi […] protégé par un écran, avec toujours ce sentiment d'impunité»[115]. Les clients de la prostitution apprécient donc la discrétion qu'offre Internet. Le faible coût d'accès et la facilité avec laquelle sont fixés les rendez-vous participent à une mise en relation simple et rapide des personnes sur Internet. La grande visibilité, la banalisation dans la présentation des prestations proposées facilite bien le passage à l'acte.

La vente et la traite des enfants, la prostitution et la pornographie impliquant des enfants sont des pratiques étroitement liées. Ainsi, la vente et la traite des enfants à des fins sexuelles n'est qu'une ramification de la prostitution qui va elle-même généralement de pair avec la production d'images, de vidéos et autres formes de matériel sexuel explicite impliquant des enfants.

---

[112] Th. Vallat, « Cyber Harcèlement: le sextorsion et comment réagir aux chantages à la webcam ? », blog de Th. Vallat, avocat au barreau de Paris, 12 août 2015, http://www.thierryvallatavocat.com/2015/08/cyber-harcelement-le-sextorsion-et-comment-reagir-aux-chantages-a-la-webcam.html, consulté le 10 janvier 2015.

[113] D'une manière pratique, tout commence par une simple histoire de séduction sur Internet via un chat, un site de rencontre. A la suite d'échanges, la confiance s'installe entre les interlocuteurs dont la victime est souvent un enfant, une des cibles faciles. Il s'ensuit des discussions sur des questions privées et intimes. Le prédateur propose alors à l'enfant naïf d'allumer sa webcam pour une conversation approfondie. Il l'invite à se déshabiller et à se livrer à des actes intimes devant l'écran. Le prédateur montre toujours une fausse vidéo d'une jeune personne au physique attrayant. Le maître-chanteur enregistre la victime à son insu pendant qu'elle s'exhibe, pour ensuite la menacer si elle ne paye pas une somme d'argent exigée, ou si elle ne se livre pas à des actes intimes plus poussés devant la caméra.

[114] http://infos.fondationscelles.org/dossier-du-mois/comment-internet-a-stimule-l-echange-de-services-sexuels-n° 28, document créé le jeudi 17 avril 2014 à 15 heures, consulté le 05/03/2015.

[115] http://infos.fondationscelles.org/dossier-du-mois/comment-internet-a-stimule-l-echange-de-services-sexuels-n28, document créé le jeudi 17 avril 2014 à 15 heures, consulté le 05/03/2015.

2. Le risque d'exposition des mineurs à des contenus illicites

La notion de contenus illicites est un concept à contenu variable. Elle n'est pas définie par la loi et diversement appréciée par les systèmes juridiques. Cependant, en droit sénégalais, le décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques, pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques[116], a proposé une définition de la notion de « contenus manifestement illicites ». Selon ce texte, cette expression renvoie à des « contenus d'une gravité » avérés et dont le caractère illicite ne semble pas discutable, notamment les contenus à caractère pornographique ou faisant l'apologie des crimes de guerre ou portant manifestement atteinte à l'ordre public ou aux bonnes mœurs ». Ainsi, il est admis généralement que ces contenus illicites renvoient notamment à la diffusion de messages de nature raciste ou xénophobe et aux messages violents.

Dans le cadre du traitement de la cybercriminalité, le recours à l'approche préventive est de nos jours une véritable tendance des législations pénales contemporaines. La lutte contre l'exposition des mineurs à des contenus illicites en constitue une illustration parfaite. Le droit des transactions électroniques a mis à la charge des fournisseurs d'accès une obligation générale de mention d'un dispositif de filtrage dans les contrats les liant à leurs abonnés. Aux termes de l'article 3 1° de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, « les personnes dont l'activité est d'offrir un accès à des services au public par le biais des technologies de l'information et de la communication sont tenues de mentionner dans les contrats de leurs abonnées l'existence de moyens techniques permettant de restreindre l'accès à certains services ou au moins de les sélectionner ». Les modalités d'application de ce texte sont précisées par l'article 3 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques. Selon ce texte, les moyens techniques visés par la loi sur les transactions électroniques doivent être efficaces et accessibles en vue notamment d'identifier les erreurs commises dans la saisie des données, de les corriger le cas échéant et de rendre plus sûre la navigation des mineurs sur les réseaux. L'article 4 du décret du 30 juin 2008 précise que les fournisseurs d'accès « doivent, d'une part, assurer la mise à jour régulière de ces moyens techniques et, d'autre part, en informer les utilisateurs ». Les dispositifs de filtrage auxquels fait référence la loi sont surtout les techniques d'autorégulation que sont les dispositifs de contrôle parental expressément visés par le décret n° 2008-719 du 30 juin 2008. Ces dispositifs de contrôle parental tendant à sécuriser la navigation des enfants.

[116] JORS, n° 6439 du 22 novembre 2008.

Ils constituent des programmes qui permettent aux parents de bloquer l'accès de leurs enfants mineurs à des contenus illicites et préjudiciables. Les outils de contrôle parental peuvent être installés, soit sur le poste de travail, soit en ligne. Ils mettent souvent en œuvre plusieurs dispositifs techniques. Il peut s'agir d'un dispositif de filtrage par mot clé consistant à bloquer de l'accès des mineurs aux pages dont les adresses URL comportent des termes proscrits préalablement déterminés.

En vertu d'assurer l'effectivité des mesures techniques, le législateur sénégalais ne s'est pas contenté de les légaliser. Le droit pénal est intervenu pour sanctionner pénalement les manquements à l'obligation de mention d'un dispositif de filtrage. L'article 431-45 du Code pénal incrimine « toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale, exerçant l'activité définie à l'article 3 de la loi sur les transactions électroniques, n'ayant pas respecté les prescriptions de ce même article ». Les délinquants utilisent le réseau numérique pour commettre des infractions contre les biens.

B. Les infractions contre les biens

Les infractions contre les biens se matérialisent par les atteintes par appropriation frauduleuse et les autres atteintes aux biens de catégorie résiduelle qui accueille toutes les atteintes qui ne donnent pas lieu à appropriation. Il faudra donc, pour mieux élucider tout ceci, nous attarder sur la notion de l'escroquerie via internet (1) mais surtout la différencier avec une notion, qui pourrait prêter à confusion avec celle-ci : la fraude informatique (2).

1. Les escroqueries via Internet

L'escroquerie, dans sa conception classique, est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge[117]. Certains types

[117] A propos de l'escroquerie, le code pénal sénégalais, voir l' article 379 « quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges, et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui,… »

Article 379 bis (loi n° 99-05 du 29-1-1991) « quiconque aura reçu des avantages ou des commodités matérielles, des prestations ou se serait fait fournir des services en employant soit des manœuvres frauduleuses quelconque, soit en faisant usage de faux nom ou de fausses qualités…. »,

d'escroquerie relèvent de la criminalité financière ou « en col blanc ». La loi sur la cybercriminalité en son article 431-56 CP prévoit l'escroquerie d'information, en intégrant les informations personnelles, confidentielles ou celles qui sont protégées par le secret professionnel » dans l'objet de ce délit. Cette infraction présente le mérite de garantir la répression de pratiques frauduleuses comme le hameçonnage ou « fishing »[118].

La fraude informatique est la variante informatique de l'escroquerie au sens classique du terme. L'escroquerie consiste à soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand quelqu'un utilise à cette fin des moyens de communication modernes, le législateur considère qu'il s'agit également d'escroquerie. Internet permet, dans un délai rapide et à moindres frais, de toucher un grand nombre de victimes. Les cybers délinquants utilisent diverses astuces pour appâter les victimes[119]. Les moyens utilisés peuvent être le réseau ou les appareils de téléphones. C'est pourquoi, il est important pour faciliter la compréhension distinguer, l'escroquerie en ligne et l'escroquerie au téléphone encore appelé le porte à porte. C'est le fait d'un appelant qui se prétend être représentant d'un organisme de charité, un employé d'une entreprise de carte de crédit ou même un parent éloigné.

Des formes différentes sont utilisées pour escroquer les victimes. D'abord, dans le cadre des transactions financières, il arrive aux usagers de l'Internet de recevoir un e-mail dans lequel il lui est proposé de grosses sommes d'argent à changer ou à blanchir. L'arnaque consiste à faire croire qu'il est possible d'encaisser d'importants bénéfices excédentaires d'une instance soi-disant officielle. Cet e-mail sollicite une aide et le correspondant demande à verser de l'argent ou transmettre des documents d'entreprise, des données personnelles ou confidentielles. En échange, on promet aux victimes une participation aux bénéfices de l'ordre de 20% ou plus. Il existe, dans cette catégorie, un autre type de criminalité : le "phishing". Par ce procédé, des criminels reproduisent des sites d'entreprises ou d'organisations connues pour voler des données personnelles, des mots de passe et des sommes d'argent. Il peut s'agir d'un e-mail relatif à un avis indiquant le gain d'un gros lot

[118] L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation 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 lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. c'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques. Lorsque cette technique utilise les sms pour obtenir des renseignements personnels, elle s'appelle smishing. Source http://fr.wikipedia.org/wiki/hame%c3%a7onnage.

[119] P.A.TOURE, Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal op.cit.

à une loterie ou à un jeu de hasard. Pour réception du prix, une somme d'argent doit être d'abord versée à titre de garantie. Mais, il faut comprendre que les loteries officielles ne fonctionnent pas de cette manière car on ne reçoit qu'un prix après avoir acheté un billet de loterie, un billet à gratter ou un bulletin de loto. La loterie ne prend jamais contact avec le gagnant : ce dernier doit en prendre l'initiative. Parier n'est pas punissable. En revanche, exploiter des jeux de hasard sans une autorisation de la Commission des jeux de hasard l'est effectivement. Ensuite, il y a les héritages fictifs. Dans ce cas, un courriel d'un soi-disant organe officiel étranger ou d'un soi-disant "notaire" étranger est envoyé. Ce message précise qu'après de longues recherches, on a pu vous identifier comme étant le (seul) héritier d'une personne très riche récemment décédée. Mais attention : pour pouvoir recueillir l'héritage, vous devez d'abord verser une somme d'argent, destinée soi-disant à régler tous les frais administratifs. En réalité, il ne s'agit pas ici d'un vrai notaire, mais bien d'escrocs qui en veulent à votre argent. Enfin, le même procédé est utilisé dans les investissements exotiques. Il s'agit d'un e-mail de propositions (malveillantes) d'investissements dans des projets exotiques, avec promesses de gains astronomiques à la clé. Les escrocs tentent aussi de jouer sur vos sentiments. Dans certains e-mails par exemple, les cybers escrocs demandent à leurs victimes de verser de l'argent pour quelqu'un qui a besoin de toute urgence d'un passeport, d'un visa ou d'un autre document officiel.

Pour les apitoyer, l'e-mail décrit avec force détails les conditions de vie déplorables d'un pays situé à l'autre bout du monde. L'argent à verser servirait à payer l'intermédiaire chargé de délivrer le document. Il va de soi que cette personne ne sera jamais vu par la victime et que tout simplement perdu elle va perdre son argent. A côté de l'escroquerie via internet, il y a la fraude informatique qui a plusieurs variantes. Nous allons nous limiter à la fraude à la carte bancaire.

2. La fraude à la carte bancaire

Elle peut être considérée comme un crime transfrontalier organisé pour les raisons suivantes. La principale technique est le skimming. Le terme skimming vient de l'anglais « to skim », écrémer. Le skimming consiste à manipuler les automates et terminaux de paiement (bancomats, distributeurs de billets et terminaux de paiement dans les commerces, les stations-service, la restauration, etc.). Pour ce faire, les escrocs se servent d'un équipement spécial introduit dans les automates ou à proximité, qui copie les données contenues sur la piste magnétique de la carte bancaire, de débit ou de crédit et enregistre le code NIP. Les

malfaiteurs agissent généralement en bandes organisées. Dans certains pays comme la Suisse, le retrait d'espèces n'est pas possible avec les cartes Maestro et Post Finance Card Direct si elles ne sont pas munies de leur puce inviolable. Mais dans plusieurs pays en dehors de l'Europe, les données de la piste magnétique et le code NIP d'une carte suffisent pour retirer de l'argent. C'est pourquoi, dans les cas de skimming, l'argent est toujours retiré à l'étranger. La plupart des victimes ne constatent la fraude que lorsqu'elles reçoivent leur relevé de compte. D'abord, les informations financières sont directement communiquées à des pirates par une personne travaillant dans les banques des victimes ou par personne interposée ayant des liens avec un employé de la banque ou encore qui a volé les informations par un skimmer par exemple sont envoyées à d'autres. Ces personnes peuvent accumuler les données sur une clé USB ou n'importe quel support ou moyens et les vendent d'autres groupes. Une fois les données récupérées, ils les envois à un troisième groupe chargé de confectionner les cartes. Pour récupérer les fonds, les pirates peuvent recruter des mules qui sont des intermédiaires qui reçoivent de l'argent sur un compte créé pour l'occasion. Ensuite, l'argent est converti en cash et transféré vers l'étranger via des services de mandat international. La mule garde un petit pourcentage du montant d'argent acheminé pour « service rendu ». Enfin, avec ces fonds, les escrocs montent des entreprises fictives pour recruter d'autres mules. Ainsi, il n'est pas rare de recevoir des mails qui finissent le plus souvent dans le courrier indésirable qui prennent la forme de petites annonces du type « Emploi bien rémunéré pour faible temps de travail ». Cet exemple montre sans équivoque que les fraudes à la carte bancaire sont des comportements cybercriminels organisés. Cette organisation des réseaux se reflètent également à travers les infractions cybernétiques contre la paix publiques. Certaines de ces menaces sont tellement prévenues en grande pompe par les états de façon physique que les délinquants passent désormais par internet pour la propagande de leurs forfaits.

<u>Paragraphe 2 :</u> L'Internet, au service des menaces terroristes

Sujet très à la mode, le terrorisme exploitant le réseau d'Internet est devenu incontestablement une évidence, une réalité. Les archives criminelles d'Interpol et des forces policières dans les différents pays en témoignent. De nombreuses opérations terroristes ont été commises à travers le monde contre le réseau et les données qui y circulent. A notre sens, le Cyberterrorisme peut être analysé comme l'activité d'un groupe terroriste dont l'objet est de commettre, par le biais d'Internet, dans la sphère internationale ou nationale, des actes qui ne couvrent pas seulement une catégorie d'infractions clairement définies comme terroristes,

mais également un ensemble plus ou moins flou d'activités illicites ou licites mais en lien avec l'objectif terroriste. C'est une prolongation moderne via Internet de l'activité terroriste censée se dérouler sur le terrain réel. En conséquence, on peut constater que le terrorisme et Internet sont deux grands phénomènes du XXI^{ème} siècle. Il convient de s'interroger sur leurs interactions mutuelles. Autrement-dit, de rechercher comment le réseau Internet peut servir les réseaux terroristes. Ainsi, il apparait que l'impact de ce phénomène est majeur tant pour la sécurité que pour la liberté car le terrorisme utilise de nouveaux procédés techniques. C'est pourquoi on s'interroge sur l'existence d'une politique juridique adéquate. Pour cela justement, faudrait-il penser le bouleversement du terrorisme traditionnel (A), et puis réfléchir sur la politique juridique anti-cyberterrorisme (B).

A. Le bouleversement du terrorisme traditionnel

La révolution de la technologie et surtout celle du Net au cours de ces dernières années est bel et bien marquante. Les réseaux terroristes en sont conscients, et leur grande opportunité est de s'y adapter. Ces derniers ont vite réalisé combien Internet pouvait les aider tactiquement et stratégiquement dans leurs différentes activités. Ainsi, du jour au lendemain ce moyen de communication a été adopté par ces réseaux afin de poursuivre deux objectifs différents. Le premier d'impulser un rôle au réseau Internet dans la stratégie de communication du terrorisme (1), l'objectif second étant l'introduction de la cybercriminalité au service des mouvements terroristes (2).

1. Le rôle du réseau Internet dans la stratégie de communication du terrorisme

Certes, l'utilisation d'Internet comme moyen informationnel peut servir à de multiples activités, mais le cas le plus connu et le plus fréquent est son utilisation comme un support de média pour la diffusion de messages, de revendications d'un acte militaire, de fausses informations[120], d'images violentes, faisant l'apologie ou contestant l'existence de crimes contre l'humanité. A cette fonction médiatique, s'ajoute celle de son utilisation comme moyen de communication interne qui relie les différentes cellules implantées à travers le monde. Enfin, on assiste tout récemment à une exploitation, matérielle et morale, des nouveaux candidats à la mort. En effet, dans un monde où l'information joue un rôle stratégique, les terroristes cherchent à utiliser l'impact médiatique que peut avoir un acte, un message ou une image choc. En tant que Média des médias, Internet offre à ces réseaux terroristes une

[120] Il convient d'ajouter également, la manipulation, la diffusion de rumeurs et aussi l'acte d'espionnage, puisqu'il est devenu aisé d'intercepter illégalement des informations circulant sur Internet.

transmission rapide et une couverture presque illimitée. Aujourd'hui, force est de constater une prolifération de sites médiatiques qui n'hésitent pas à afficher leurs appartenances politiques ou idéologiques, poussées parfois à l'extrême[121]. Comme toutes les autres idées transmises par Internet, celles du terrorisme sont véhiculées aussi rapidement au moyen de sites militants plus ou moins élaborés qui apparaissent et disparaissent régulièrement. Contrairement aux autres médias, le choix d'Internet présente l'avantage de pouvoir atteindre presque tout le monde et de diffuser en intégralité les séquences de décapitations. C'est l'un de nombreux exemples où Internet nous démontre, des groupes terroristes qui, ayant la possibilité de sortir de leur cachette, utilisent les nouvelles technologies pour montrer leur résolution et détermination criminelle. Outre le besoin de s'adresser au public, ces réseaux ont besoin aussi de communiquer entre eux et de s'échanger des informations et des instructions. Ici, Internet n'est plus un média ouvert, c'est un moyen de communication interne mais qui peut jouer un rôle clé. Des exemples permettent de s'en convaincre. Rappelons l'affaire de Richard Reid qui avait utilisé Internet pour communiquer au sujet de son projet d'attentat avec un groupe terroriste basé au Pakistan[122]. Il est possible d'évoquer les aveux de Mohammad Naeem Noor Khan qui a reconnu avoir utilisé le courrier électronique pour communiquer avec d'autres terroristes[123]. Enfin, il est également possible de mentionner l'attentat de Casablanca qui a révélé la puissance inégalée des réseaux terroristes exploitant Internet et la vulnérabilité de nos sociétés. Il faut aussi noter que les caractéristiques d'Internet, l'accessibilité mondialement, la facilité du fonctionnement, la difficulté de contrôle, et la possibilité de transmission de données cryptées- dynamisent ces réseaux[124]. L'architecture même du réseau Internet, basée sur le pair à pair sans point central, est aisément conciliable avec les nouveaux modes de structure des réseaux terroristes. Dans plusieurs exemples, les forces de police ont découvert que des contacts avaient été entrepris entre les membres de groupes terroristes par le biais de messages cryptés[125] ou sténographie[126]

---

[121] Pour la première fois, des sites Internet ont été placés par les autorités américaines sur la liste des « organisations terroristes étrangères ». Ces sites racistes, appartenant aux disciples de Kahane www.newkash.org, www.kahane.org, www.kahane.net et www.kahanetzadak.com, ont fait l'objet de cette mesure, le 2 octobre 2003, pour avoir diffusé de propos extrêmement racial et violent, selon le Département d'Etat Américain des Affaires étrangères. J. SEPER, « 4 Jewish Web sites deemed Terrorist », The Washington Times, 4 October 2003, p. 1.

[122] Est l'auteur de la tentative d'attentat qui a visé le vol 63 d'American Airlines assurant la liaison Paris-Miami le 22 décembre 2001.

[123] Le conseil de l'Europe, Criminalité organisée en Europe, La menace de la cybercriminalité, op. cit., p. 186.

[124] Il n'est pas nécessaire que le site utilisé pour communiquer les instructions ait un aspect militant. Les terroristes peuvent utiliser des sites à caractère pornographique, de sport, de commerce comme couverture.

[125] D'après the Washington Post, Ben Laden pourrait avoir eu recours à de puissants moyens de cryptographie pour communiquer avec ses agents, utilisant des images contenant des messages encryptés.

circulant sur Internet. Le premier exemple concerne les attentats du 11 septembre 2001. A la veille des attentats, le service de renseignement américain a intercepté un court message en provenance d'un membre du réseau d'Al-Qaida. Ce message, traduit après les attentats, contenait : « c'est demain l'heure zéro ». Dans le second exemple, il s'agit de l'e-mail émis à Paris par Richard Reid destiné à un groupe islamiste basé au Pakistan. Ce courrier électronique a été en fait considéré par la justice américaine comme preuve à l'appartenance de Reid au réseau d'Al-Qaida, et donc à son inculpation.

Du sucre fin, de l'essence, de la poudre insecticide, un détonateur, …etc. La liste est longue, mais le processus et les ingrédients exigés pour la fabrication d'une bombe artisanale sont à la portée de tous, puisque la recette est domestique et ne coutera que peu d'argent et peu d'effort. Grace à Internet, il est possible désormais de fabriquer sa propre bombe[127]. Des sites Internet, dédiés aux « kamikazes » et « al-djihad »[128], diffusent en permanence des petites recettes populaires afin d'enseigner aux nouveaux candidats à la mort comment fabriquer eux-mêmes leurs bombes pour ensuite se faire exploser. Une visite sur ces sites démontre à quel point la fabrication d'un engin explosif, qui peut détruire la vie de centaines de personnes voire des milliers, est très facile à composer. Les kamikazes de Casablanca ont avoué devant la justice marocaine avoir surfé sur les espaces virtuels d'Internet où ils ont trouvé les bons conseils pour fabriquer une bombe, leur permettant de la réaliser eux-mêmes[129]. Plus surprenant encore, avec Internet, la fabrication d'engins explosifs s'est transformée en jeu d'enfant. L'accident, qui a failli couter la vie aux cinq enfants français, fournit une idée concrète de cette menace. En l'espèce, ces enfants ont été blessés dans l'explosion d'une bombe artisanale qu'ils ont pu fabriquer grâce aux instructions trouvées sur Internet. Il est possible également de citer l'affaire des islamistes tunisiens inculpés par la justice à Tunis pour avoir pratiquée des activités terroristes et usage subversif d'Internet. Selon les enquêteurs, les inculpés, qui appartiennent à la brigade du Prophète, ont été en possession de plans de fabrication de bombes tirés sur Internet ainsi que d'un plan d'attaque terroriste visant le poste de la garde nationale de Zarzis.

---

[126] Stéganographie ou l'art de cacher une information dans un autre. En d'autres termes, c'est l'utilisation d'autres fichiers informatiques pour transmettre l'information.

[127] Selon l'institut national de l'audiovisuel français, il est possible actuellement de recenser plus de 80 000 qui fourniraient des informations sur la fabrication et l'utilisation de bombes artisanales, d'armes radioactives ou encore bactériologiques.

[128] Récemment, un site fanatique lié au groupe Al-Qaida a annoncé l'ouverture d'une université militante, l'Université virtuelle d'Al-Qaida pour les sciences militaires. Consacrée aux différentes sciences militaires, cette université comprendra notamment les facultés de cyberguerrier et d'entrainement militaire ; sur ce sujet, voir le quotidien Pana-arabe Al-Sharq Al-Awsat, éd. Beyrouth, 20 novembre 2003, pp. 1et 4 ;

[129] Le quotidien libanais Al-Hayat, Beyrouth, 22 aout 2003, pp. 1 et 6.

2. La cybercriminalité au service du terrorisme

Parallèlement à cette tendance, qui cherche à tirer profit d'internet, que ce soit pour médiatiser les actions, les idées, ou pour communiquer clandestinement, une autre attitude existe. Celle-ci vise Internet et aspire à l'utiliser comme une arme offensive. Il y a quelques années, l'idée d'un danger d'une guerre informatique par le biais du réseau électronique appartenait à la science-fiction. Mais à peine imaginés, certains accidents «innocents» et surtout après les attentats du 11 septembre 2001 laissent penser qu'aujourd'hui rien n'est impossible.

Depuis ces événements, une transformation des actes et des moyens terroristes se met en place, ainsi qu'une apparition de nouvelles menaces nourrissent, à tort ou à raison, paniques et angoisses. La réalité a démontré que les terroristes ont très rapidement appris à utiliser et à détourné non seulement tous progrès sociaux et politiques, mais aussi technologiques. Ils ont, maintes fois, réussi à mettre Internet au service de leur discours. Mais au de-delà de ce rôle classique, Internet pourrait-il être utilisé pour une attaque auto-destructrice ? Emission de virus, intrusion dans un système informatique, piratage, sabotage. Il s'agit, bien évidemment, d'actes du hacking derrière lesquels se cachent souvent des délinquants du droit commun, qui n'ont rien à voir avec les terroristes de cette nouvelle ère. Mais est-il encore possible qu'une attaque cyberterroriste cible Internet ou la sécurité de l'information qui y circule ?

Pour l'instant, les agressions informatiques les plus fatales auxquelles on a pu assisté n'étaient que le fait des hackers. Aucun exemple n'existe probablement d'un tel attentat organisé par des terroristes. Mais cette vérité n'exclut pas pour autant l'hypothèse d'un tel scenario. Toutes ces attaques seraient nuisibles pour Internet ainsi que pour ses utilisateurs, puisqu'elles paralysent le réseau et rendent les données inaccessibles. Cela pourrait se traduire finalement par une perte considérable d'argent pour les victimes, les particuliers et les entreprises, sans évoquer la répercussion de ces attaques informatiques sur le commerce électronique. Les inquiétudes relatives au terrorisme ne datent pas d'aujourd'hui. Voilà déjà quelques années que se pose la question de savoir si les terroristes arriveront, via des manipulations informatiques, à porter des coups détruisant les infrastructures vitales pour le bon fonctionnement de nos sociétés. Le développement accéléré des technologies d'Internet, des réseaux de transmission de données, la place de plus en plus grande des ordinateurs dans la vie des sociétés sont des phénomènes qu'il n'est plus possible d'ignorer, car ils contribuent à modifier fondamentalement la stratégie, la politique, l'économie, le comportement des hommes et finalement l'art de la guerre. En réalité on assiste depuis quelques années à une modification sensible des stratégies. D'un simple moyen de propagande, on glisse vers une

arme offensive. Internet semble permettre l'organisation des attaques visant la sécurité des infrastructures indispensables au bon fonctionnement d'un Etat. Par ces caractéristiques et sa nature mondiale, il rend le maintien de la sécurité hypothétique et pose notamment des problèmes pour les pays dits « connectés » en raison de leur vulnérabilité en la matière. Dès lors, il n'est plus question de hacking ou de vol des numéros de carte de crédit. Tout un autre objectif s'installe, c'est celui de frapper très fort. Ici, la motivation est idéologique[130]. Elle consiste à utiliser Internet par le terrorisme comme une arme parmi d'autres. Il faut noter que le développement des sociétés modernes s'accompagne forcément de nouvelles vulnérabilités[131]. Un Etat dont les infrastructures sont accessibles via Internet a beaucoup à craindre, c'est la conclusion du Directeur de la Central Intelligency Agency. Celui-ci a, depuis plusieurs années, placé son pays à la merci d'une attaque informatique via le Net pouvant détruire les réseaux informatiques du gouvernement et du secteur privé ou perturber le trafic aérien, la production d'énergie[132], voire la capacité des forces militaires. Des mesures sécuritaires doivent être prises en fonction des risques et proportionnelles aux enjeux. Loin de toute politique, chaque Etat doit lutter contre tous ceux qui cherchent à l'attaquer, mais cette mesure de prévention et de répression ne peut en aucun cas, dans une société démocratique, dépasser l'objectif initial et atteindre les citoyens, déjà victimes du terrorisme.

B. La politique juridique anti-cyberterrorisme

Devant la recrudescence du phénomène du cyberterrorisme et l'essor des atteintes à la confiance publique portant sur des données numériques, il a semblé nécessaire de prévoir une modernisation de l'objet des terroristes. En ce sens, il aura fallu une impulsion en vue de promouvoir l'émergence d'une politique intrusive (1), puis en sus mettre en place le dispositif sénégalais tendant à lutter contre toutes les formes du terrorisme : vers un durcissement de l'arsenal répressif anti-terroriste (2).

1. L'émergence d'une politique intrusive

Il est clair que « le débat sur la privacy ne sera plus le même. Après ce qui s'est passé, le choc est tel que les rapports entre la protection des données du citoyen et l'Etat vont etre remis en

[130] Selon la Délégation interministérielle pour la sécurité des systèmes d'information, les motivations idéologiques peuvent être les moteurs d'actes les plus extrêmes ; voir Rapport de la Délégation, n° 650/DISSI/SCSSI, Issy-Les-Moulineaux, 28 mars 1994.

[131] John Deutch, ancien Directeur de la Central Intelligency Agency, de 1995-1997.

[132] Le 14 aout 2003, une gigantesque panne d'électricité a privé de courant New York, New-England, Michigan, Detroit et Cleveland ainsi que Toronto et Ottawa. Plus de 100 centrales électriques ont été touchées, dont 22 réacteurs nucléaires, et ont affecté aussi 50 millions personnes. Cet incident a semé la panique faisant penser à un nouveau 11 septembre.

cause »[133]. Les évènements de septembre 2001 ont profondément bouleversé le monde qui s'est senti visé par cette vague de violence inédite. Possédant un caractère unique, ces attentats frappent, pour la première fois depuis 1812, le territoire des Etats-Unis. La réaction du monde entier s'est fait rapidement sentir contre cette nouvelle forme de terrorisme. Il détourne les nouveaux mécanismes et procédés censés être préservés au service culturel et commercial. Les autorités américaines ont été les premières à se doter d'un arsenal anti-terroriste suite aux attentats. Quant à la Grande-Bretagne, elle a entrepris un vaste programme législatif. Il s'agit de la loi « Terrorism Act of 2000 », un texte d'inspiration américaine qui fait l'amalgame entre un simple acte d'intrusion informatique et du terrorisme. Il impose dorénavant aux fournisseurs de services Internet l'obligation de conserver, malgré l'interdiction posée par le « Data Protection Act » de 1984 amendé en 1998, les données de connexion et de navigation de leurs usagers. A l'image des Etats-Unis, l'Australie a voté la loi anti-terrorisme Act 2004 incriminant un certain nombre de pratiques liées à Internet. Au Canada, outre la promulgation d'une loi accordant à ces forces policières et ses services de renseignement de nouveaux pouvoirs d'investigation, un vaste chantier législatif a été mis en place. Il s'est agi de réviser certains textes en vigueur, à savoir la loi sur les droits de la personne et le Code criminel. En Afrique, au lendemain des attentats du 11 septembre 2001, plusieurs résolutions, déclarations et conventions ont été adoptées en vue de lutter contre ce phénomène international. Ces instruments juridiques ont été transposés en droit interne par la loi n° 2007-01 du 12 février 2007 modifiant le Code pénal[134]. Cette loi a introduit en droit sénégalais l'infraction de terrorisme. Mais la prise de conscience internationale du fléau du terrorisme ne saurait occulter les grandes facilités qu'offrent les TIC, et notamment le réseau Internet, aux organisations terroristes. Ces dernières ont vite pris conscience du formidable intérêt que présentent les réseaux numériques pour la propagande et la diffusion des idées terroristes.

Par ailleurs, le spectre de cyberattaques terroristes dirigées contre les infrastructures critiques de la société de l'information, qui n'épargne aucun Etat, pose aujourd'hui le débat de l'utilisation des TIC à des fins terroristes au Sénégal.

[133] Ainsi s'est exprimé le député européen Macro Cappato, membre du parti radical de la gauche italienne, devant la Commission des libertés et des droits du citoyen au Parlement européen, cité in Libération, « Le Net en liberté surveillée : les Etats cherchent à durcir leur contrôle sur le réseau », 19 septembre 2001.
[134] JORS, n° 6332 du 10 mars 2007, p. 2357.

2. Vers un durcissement de l'arsenal répressif sénégalais antiterroriste

La France s'est engagée depuis longtemps dans une politique résolue de lutte contre le terrorisme. Parfois critiquée, cette politique a reconnu des résultats incontestables, mettant fin à la montée en puissance du terrorisme surtout après les attentats des années quatre-vingt. Ces résultats ont été obtenus grâce à la mobilisation de moyens humains, budgétaires et juridiques qui ont permis d'accroitre sensiblement l'efficacité de la police et la gendarmerie d'une part, de la justice d'autre part. Pour autant, les derniers attentats frappant Londres ont rappelé que l'effort doit être maintenu, amplifié et diversifié. Ces évènements n'ont fait que révéler une réalité que beaucoup de politiques pouvaient déjà ressentir : celle de la transformation du terrorisme, devenu plus mobile et plus asymétrie. Face à cette évolution terroriste, le renforcement des moyens de lutte constitue l'une des principales priorités du Sénégal.

La multiplication des actes terroristes dans le monde ainsi que la stupeur suscitée par les attentats du 11 septembre 2001 ont incité le législateur sénégalais à apporter quelques modifications au Code pénal par l'adoption de la loi n° 2007-01 du 12 février 2007. Ce texte a intégré dans l'arsenal répressif une nouvelle catégorie d'infractions qualifiée d' «actes terroristes ». L'article 1er de la loi insère après l'article 279 du Code pénal, une section VII intitulée « Des actes terroristes ». Cependant, les rédacteurs de la loi de 2007 ne sont pas livrés à la délicate entreprise de définition du terrorisme. Ils se sont contentés d'énumérer les différents actes terroristes. Il résulte de la loi du 12 février 2007 que les actes terroristes constituent des infractions graves contre la sécurité publique, l'intégrité physique et psychique des personnes ainsi que la propriété des biens « *lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler l'ordre public ou le fonctionnement normal des institutions nationales ou internationales, par l'intimidation ou la terreur* ». L'exigence légale d'une relation de l'acte terroriste avec une entreprise individuelle ou collective ayant pour but de troubler l'ordre public ou le fonctionnement normal des institutions par l'intimidation ou la terreur constitue, d'après une doctrine autorisée, un dol spécial[135]. Selon le professeur Pradel, l'acte terroriste est *« celui qui suscite une peur collective dans la population pour l'amener à céder ou pour amener le gouvernement qui le représente à céder »*[136].

[135] J. PRADEL et M. DANTI-JUAN, Droit pénal spécial, Droit commun droit des affaires, 4e édition, édition Cujas, 2007, p. 828 ; M. L. RASSAT, Droit pénal spécial, 6e édition, Dalloz, 2011, p. 635, n° 859.
[136] J. PRADEL, « Les infractions de terrorisme, un nouvel exemple de l'éclatement du droit pénal (loi n° 86-1020 du 20 septembre 1986) », D. 1987., P. 39.

Il faut noter que la notion de cyberterrorisme renvoie également au deuxième schéma d'implication des TIC comme objet de commission d'actes terroristes. Les enjeux pénaux suscités par cette forme de cyberterrorisme, méritent toute l'attention du législateur sénégalais. En vérité, cette manifestation du terrorisme dans le cyberespace, impliquant des attaques dirigées contre les systèmes et les données stratégiques, a encore une ampleur limitée. A part la cyberattaque dirigée contre le réseau sophistiqué de l'Estonie en 2007, dont la motivation terroriste n'a pas encore été établie, aucune offensive cyberterroriste réellement efficace de cette nature n'a été jusque-là perpétrée dans le monde. Mais face à cette menace, on peut remarquer que les articles 279-1 et suivants, introduits dans le Code pénal par la loi de 2007-01 du 12 février 2007, qui énumèrent la liste limitative des actes terroristes, excluent de leur champ les atteintes aux ressources stratégiques du cyberespace, à savoir les systèmes et les données informatiques qui pourraient constituer les principales cibles du terrorisme contemporain. Au Sénégal, les nécessités de la cybersécurité exigent, dans le cadre d'une politique criminelle d'anticipation inspirée du droit français, une protection pénale de la société contre les cyberattaques par l'inclusion expresse des infractions informatiques dans les actes terroristes. Il s'agira en législation, de modifier la loi du 12 février 2007, en visant désormais dans les actes terroristes, les atteintes aux systèmes informatiques, les atteintes aux données et les autres abus (association de malfaiteurs informatiques et abus de dispositif) prévus par la loi sur la cybercriminalité et qui sont motivés par un mobile d'intimidation ou de terreur. La réforme du Code pénal et du Code de procédure pénal envisage d'ailleurs d'incriminer cette forme de cyberterrorisme.

Dans cette première partie de notre étude, il a été constaté que l'Afrique de l'Ouest est interpellée par un défi sécuritaire grandissant. Le phénomène criminel multiforme y est caractérisé par l'émergence de groupes, de réseaux ou d'associations criminelles sévissant dans plusieurs pays à la fois avec des moyens de plus en plus sophistiqués. Mais quelque soient les mesures préventives prises, les cybercriminels passent à l'acte. Il faut donc des règles de procédures appropriées pour rechercher, identifier et arrêter les criminels. Il faut adopter de nouvelles règles de procédures.

En définitive, soyons clairs, même s'il existait une panoplie de règles applicables à tout va, à chaque situation délictuelle sur le réseau Internet, il ne serait pas moins judicieux de se poser la question de leurs adaptabilités quand on sait sans doute que la plus part des Etats en Afrique ont une forte connotation analogique dans leurs système d'information, on comprend bien alors tout le problème qui se pose dans le cadre de l'adaptation des règles pénales de

formes surtout à l'ère du numérique. C'est pourquoi, nous porterons notre réflexion sur ce cas de figure précis, au chapitre second de nos travaux.

CHAPITRE II : L'ADAPTATION DES REGLES PENALES DE FORME A L'ERE DU NUMERIQUE

En droit processuel, le terme « processus » renvoie à la procédure, qui vient du verbe latin procedere, signifiant littéralement « aller de l'avant ». Il désigne une manière de faire pour aboutir à un certain résultat. En matière pénale, cette notion évoque la procédure pénale, c'est-à-dire « l'ensemble des règles relatives à la constatation des infractions ainsi qu'à l'identification, l'appréhension, la poursuite et le jugement de leurs auteurs ». De nos jours, l'importance de la procédure pénale, en tant que technique d'organisation du procès dans les grandes options de la politique criminelle, et notamment dans les orientations du droit pénal, n'est pas discutée.

En réalité, les normes procédurales pénales, en garantissant l'application effective des instruments du droit pénal de fond, constituent le passage obligé de la pénalisation à la répression judiciaire des comportements d'écart aux normes.

Aussi l'application d'une réponse appropriée à la criminalité du numérique passe nécessairement à l'aménagement des règles procédurales spécifiques aux numériques (section1). Mais malgré cette amélioration on constate la survivance de difficultés dans le processus de la répression des délinquants du numérique (section 2) d'où l'harmonisation des règles internationales pénales et la coopération des Etats pour lutter contre ce phénomène mouvant.

SECTION 1 : L'AMENAGEMENT DES REGLES PROCEDURALES SPECIFIQUES A L'ENVIRONNEMENT NUMERIQUE

La mise à disposition d'information sur notre réflexion pour une meilleure saisine de sa portée, passe par une exposition sur l'aménagement des moyens d'investigation (paragraphe1) mais cela ne suffit pas, il faut aussi interroger les cas spécifiques de l'interception de flux réseaux (Paragraphe2).

Paragraphe 1 : L'aménagement des moyens d'investigation

Dans cette partie de nos travaux, il nous sera donc permis de porter une étude sur l'encadrement meilleur des preuves en matière informatique (A) tout en analysant méthodiquement les moyens d'investigation mis à disposition (B).

A. Un meilleur encadrement des preuves en matière informatique

Pour un meilleur encadrement des preuves en matière informatique, il faut au préalable la consécration de la preuve informatique (1) mais ensuite la dématérialisation de la procédure (2).

1. La consécration de la preuve numérique

Les courriels, les messages (sms) instantanés, les enregistrements, les traces ou indices issus des machines constituent autant de preuves potentielles, il est important pour le juriste et les professionnels du secteur informatique de se mettre à jour. L'utilisation des technologies et de l'Internet par les criminels organisés amène les acteurs judiciaires à agir dans cet espace virtuel ou à interroger les technologies pour pouvoir rassembler les indices nécessaires pour apporter la preuve à charge ou à décharge[137]. Mais le recours aux techniques d'investigations numériques à elles seules ne suffisent pas. Elles doivent se conjuguer aux autres armes procédurales tout en respectant les principes fondamentaux qui gouvernent l'administration de la preuve. Avec l'impact de la criminalité sur l'espace virtuel qu'est Internet, tous les Etats doivent non seulement consacrer la preuve numérique dans leurs législations mais ils doivent mettre en place des mécanismes permettant de garantir leur valeur et force. Cela pour garantir la confiance et assurer la sécurité des systèmes d'informations. La plus part des états ont élaboré un dispositif juridique consacrant les bases d'un cyber droit pénal et d'une cyberprocédure pénale. Ils ont consacré des textes législatifs qui adaptent la procédure pénale à l'évolution de la criminalité liée aux technologies de l'information et de la communication. A ce titre, ils ont organisé les transactions électroniques, la signature électronique et la publicité par voie électronique. Ils ont également mis en place des règles de procédures donnant des moyens légaux aux enquêteurs surtout dans le traitement des infractions spécifiques aux technologies ou facilitées par celles-ci.

Au Sénégal, diverses lois ont été promulguées notamment la loi sur la cybercriminalité qui consacre dans sa seconde partie les instruments procéduraux en matière de cybercriminalité[138]. La Côte d'Ivoire et le Nigéria ne sont pas en reste. Les différents actes de

[137]Voir sur la question de la preuve numérique, Séverine Mas, Avocat au Barreau de Marseille, « L'appréhension par le droit, de la preuve sur les réseaux numériques, Approche technico-juridique », intervention, le 16 juin 2006 dans le cadre du colloque « Internet sous haute surveillance », organisé par Me Séverine Mas et le réseau d'avocats Euro-Counsels et en partenariat avec l'Ordre des avocats au Barreau de Marseille, mise en ligne sur Juriscom.net, 1er mars 2007, http://www.juriscom.net.

[138] Au Sénégal, nous pouvons citer : la loi n° 2008 – 08 sur les transactions électroniques, loi n° 2008 – 12 sur la Protection des données à caractère personnel, la loi N°2005-41 DU 20 Aout 2008 sur la CRYPTOLOGIE. La loi uniforme n°2009-16 du 2 mars 2009 relative à la lutte contre le financement du terrorisme consacre à son article

procédures posés dans cette loi seront abordés dans nos développements ultérieurs. Sur le plan institutionnel, des pays ont mis en place des services spécialisés dans la collecte de la preuve numérique. Il en est ainsi de la Côte d'Ivoire avec la Direction de l'Informatique et des Traces Technologiques, du Sénégal qui a créé une Brigade Spéciale de Lutte contre la Cybercriminalité au sein de la Direction de la Police Judiciaire, du Bénin, du Togo, du Burkina Faso, du Niger et de Nigéria. Ces structures jouent un rôle important dans la collecte de la preuve numérique, devenue incontournable dans la lutte contre la cybercriminalité. Celle-ci est un moyen permettant d'établir sur des faits la culpabilité ou l'innocence de l'accusé lors du procès. La preuve électronique est parfois difficile à collecter, la plupart des suspects font recours au chiffrement, ce qui, en l'absence de la clef de déchiffrement, rend l'accès aux preuves électroniques long et difficile. Malgré tout cela, la Police doit analyser les preuves électroniques pour permettre aux magistrats de les consulter et les comprendre pour établir les faits en vue du procès.

Aujourd'hui, la presque totalité des affaires liées à la criminalité transfrontalière organisée comportent des éléments numériques indispensables pour la recherche des malfaiteurs. Aucune activité criminelle ne peut être planifiée ou exécutée sans les auteurs fassent usage d'un téléphone ou utilise les technologies de l'information et de la Communication en général et Internet en particulier. Par exemple, la plus part des terroristes dispose de site Internet ou passent par les réseaux sociaux pour faire de la propagande ou de l'apologie du terrorisme. Ils utilisent même l'Internet pour identifier et localiser la position exacte des cibles.

L'intégration de la preuve numérique dans les enquêtes constitue un élément indispensable pour identifier, rechercher et établir les relations entre les groupes criminels. En plus, les preuves numériques exploitées peuvent aider les enquêteurs à identifier les malfaiteurs et le magistrat à soutenir l'accusation devant les juridictions de jugement et établir la culpabilité des prévenus. Des efforts restent à faire pour les pays de l'Afrique de l'Ouest dans l'encadrement de la preuve numérique sur le domaine législatif et opérationnel. La dématérialisation des échanges et l'utilisation des moyens d'anonymisation imposent une adaptation des moyens d'investigations. En résumé, la criminalité a considérablement évolué avec un recours croissant aux technologies numériques, aussi bien pour commettre l'infraction

---

intitulé « Renseignements accompagnant les virements électroniques » que tout virement électronique transfrontalier doit être accompagné de renseignements exacts relatifs au donneur d'ordre. Ces renseignements comprennent notamment le numéro de son compte ou à défaut, un numéro de référence unique accompagnant le virement. Tout virement électronique national inclut les mêmes données que dans le cas des virements transfrontaliers, à moins que toutes les informations relatives au donneur d'ordre puissent être mises à la disposition de l'organisation financière du bénéficiaire et des autorités compétentes par d'autres moyens.

que pour tenter d'empêcher l'identification de leurs auteurs. Face à ce constat, le législateur doit adapter les moyens d'investigations pour pouvoir collecter les preuves numériques.

En principe, toute preuve électronique n'est pas recevable. Et, une preuve irrecevable peut rendre impossible l'ouverture de poursuites pour des actes de criminalité transfrontalière organisée ou toute autre infraction dont la réalité est établie par des informations électroniques. Même si le droit procédural ne définit pas de règles de preuve distinctes pour la preuve électronique, un certain nombre de principes doit gouverner cette preuve. Certains auteurs parlent de la règle de la meilleure preuve, de la pertinence des preuves, de l'interdiction de la preuve par ouï-dire, de l'authenticité et de l'intégrité. D'autres, par contre, se limitent à trois principes directeurs que sont l'intégrité, la loyauté et la proportionnalité. Donc, pour une lutte efficace, les acteurs doivent intégrer ces conditions dans le cadre de leurs sous peine de faire un travail inutile. Une autre liée à l'imputabilité de la preuve est soulevée. Les enquêteurs sont donc confrontés au défi lié au respect des principes directeurs qui doivent guider la recherche de la preuve auxquels l'émergence du cyber procédure ne saurait déroger[139]. Le problème fondamental auquel les enquêteurs sont confrontés est d'ordre pratique. Il est lié à la difficulté d'établir les preuves numériques qui sont volatiles mais également la conservation des données. A cela, s'ajoute que dans son administration sous peine de nullité, on doit tenir compte de la nécessité dans un état de droit de faire l'équilibre entre les moyens coercitifs et la protection des libertés individuelles.

Le respect des principes de loyauté et de légalité de la part de tous les acteurs de la procédure notamment les officiers de police judiciaire est de rigueur. Le respect de ces principes garantit la répression sinon les malfaiteurs échapperont à la répression en évoquant des cas de nullités. Les enquêteurs doivent faire des efforts en ce sens pour n'utiliser que des preuves prévues par la loi dans le respect des droits et libertés fondamentaux. Toujours est-il que la preuve numérique pour être admissible doit avoir une force probante et il est exclu les provocations policières[140] dans certains cas comme en matière de pédopornographie. L'établissement de la vérité n'est pas l'unique objectif recherché mais qu'il doit être concilié notamment avec le respect des libertés fondamentales, le respect de la vie privée et d'autres droits. La preuve numérique doit répondre donc au moins à ces trois principes que sont

[139] M. QUEMENER ET Y. CHARPANEL, Cybercriminalité, droit pénal appliqué, pratique du droit, economica, 2010.
[140]Voir en ce sens, les arrêts Teixeira de Castro c. Portugal du 9 juin 1998, §36, et Edward et Lewis c. Royaume-Uni, Cour européenne des droits de l'homme du 22 juillet 2003, §49. .

l'intégrité, la loyauté et la proportionnalité. Ces principes ont pour objet de déterminer qui doit établir la preuve, sur quoi doit porter la preuve, comment elle doit être établie et quelle est sa force probante.

Ainsi, par souci d'efficacité, les Etats doivent renforcer les moyens d'investigations à l'environnement numérique. L'efficacité commande une dématérialisation de la procédure pour mieux s'adapter à l'environnement numérique.

2. La dématérialisation de la procédure

La procédure pénale, compte tenu des évolutions technologiques ne doit pas échapper à la numérisation, qui est « la figuration emblématique de l'immatériel. La numérisation est une technique qui autorise toutes les déclinaisons, qui permet le multimédia comme la mise en réseau, qui fait que l'information peut être soumise à tous les traitements »[141]. Pour mieux s'adapter à l'évolution du phénomène criminel, les Etats doivent intégrer le numérique à toutes les étapes des procédures. Il s'agira de procéder à la numérisation des plaintes, à des réquisitions informatiques et à la mise en œuvre de nouvelle norme par l'Intranet.

L'idée de la numérisation des plaintes permet aux citoyens de déclarer une infraction par Internet sous la forme d'une pré plainte au niveau d'un service de répression. Après cette démarche en ligne, l'internaute pourra aller au commissariat ou à la gendarmerie pour finaliser sa déclaration. En France, la procédure a été mise en test pendant un an et concernait uniquement les infractions portant atteinte aux biens et dont les auteurs ne sont pas identifiés. Les Etats de l'Afrique de l'ouest devraient mettre en place des structures ou des commissions nationales de l'informatique avec des guichets virtuels pour recueillir les plaintes du grand public. Cette mise à disposition des usagers de télé services permet d'accomplir facilement des formalités déclaratives en vue de simplifier des échanges entre les services de sécurité et les usagers. Il faut au préalable mettre en ligne des formulaires permettant l'accomplissement auprès des guichets de toutes les procédures. Il faut bien prévoir un formulaire permettant de saisir la commission de plaintes[142]. De même, plusieurs fonctionnalités à savoir l'enregistrement des dossiers, le contrôle de cohérence des données saisies, la mise à jour et le suivi des dossiers, les éditions des listes de traitements

[141] Problématiques techniques, juridiques et assurancielles de la net-economie, par J. L. SANTONI Marsh Conseil Président de la commission Juridique-Assurance du CLUSIF, page8.

[142] Voir loi de 6 janvier 1978 modifiée en Août 2004.

conformément aux dispositions législatives doivent être mises en place pour permettre l'élaboration de statistiques[143].

Pour plus de clarté et de sécurité, des services habilités à recevoir la communication de ces données doivent être crées. Dans le cadre de l'instruction d'une plainte, le responsable de l'organisme visé dans la plainte, ainsi que les organismes tiers susceptibles d'être sollicités, peuvent être également destinataires des informations utiles au règlement de celle-ci[144]. Le recours aux nouvelles technologies doit désormais être généralisé d'abord au niveau des enquêtes. Les magistrats du parquet et les Officiers de Police Judicaire doivent, sur la base d'un intranet sécurisé, être en mesure de consulter les fichiers de police et de justice concernant les affaires qu'ils traitent. Un service chargé de donner les habilitations d'accès aux dossiers judiciaires doivent être mises en place au niveau des parquets pour le suivi régulier des dossiers et la coordination des actes de polices judiciaires posés. L'exemple de l'article 48-1 du Code procédure pénale français pourrait être une source d'inspiration. Les dispositions de ce texte permettent l'accès de l'ensemble des procureurs à l'ensemble des données de tous les parquets de France. Cet intranet facilite les échanges entre le ministère de la Justice et les parquets généraux destinés à renseigner sur les procédures en cours. Cela présente un double avantage à savoir la rapidité, par rapport aux écrits et à la certitude que le message a été envoyé et reçu.

Enfin, l'intranet favorise la généralisation de l'enregistrement des auditions pendant l'enquête préliminaire ou l'instruction préparatoire. Cette généralisation permettra aux acteurs de la justice pénale de se familiariser aux techniques numériques, de comprendre les avantages et les contraintes. Le principe du recours possible de moyens de télécommunications au cours de l'enquête et de l'instruction permet de protéger certaines couches vulnérables comme les mineurs victimes en veillant à préserver les droits de la défense mais aussi les conditions d'utilisation et de diffusion des données ainsi

[143] Pour l'enregistrement des dossiers au niveau des guichets, des formulaires comportant les rubriques suivantes:
- identification du responsable du traitement (nom, prénom, adresse postale, adresse électronique, numéro de téléphone, numéro de fax),
- les principales caractéristiques du traitement déclaré conformément aux dispositions de la loi précitée,
- identification du requérant (nom, prénom, adresse postale, adresse électronique, numéro de téléphone),
- identification de l'organisme mis en cause par le requérant (nom, adresse postale),
- les éléments de contexte, fournis par le requérant, utiles à l'instruction de la plainte.

[144] Sur les déclarations en ligne voir : délibération n° 2010-65 du 11 mars 2010 portant avis sur un projet de décision du président de la CNIL relative à la mise à disposition des usagers de la CNIL de télé services pour l'accomplissement des formalités déclaratives et la transmission de plaintes (demande d'avis n° 1413225) publié au JORF n° 0084 du 10 avril 2010.

enregistrées[145]. La réquisition n'est pas un acte de procédure nouveau. Elle corresponde à un acte par lequel un magistrat ou un officier de police judiciaire impose à une personne de fournir une prestation qu'il n'est pas en mesure d'effectuer lui-même faute de moyens ou de compétences techniques nécessaires. Il peut s'agir d'une demande de communication de documents. Mais le mode de communication des réquisitions demeure pour la plupart des pays de la sous-région traditionnel c'est-à-dire les réquisitions sont des demandes faites sur papier dument revêtues du sceau officiel du service demandeur et transmises physiquement au service requis qui répond de la même manière[146]. La preuve numérique étant très volatile, présent partout et indispensable dans les enquêtes liées à la criminalité organisée, il est important de faciliter les procédures de réquisition. L'enjeu majeur pour les services d'enquêtes est la dématérialisation de la procédure[147]. Elle permettra aux enquêteurs de gagner plus de temps dans le cadre de leurs actions en ayant en temps réel les informations demandées.

Dans un contexte de dématérialisation de l'information, les législations des pays devaient prévoir la transmission par la voie télématique ou électronique de réquisitions dans le cadre des enquêtes. Ainsi, les opérateurs et les fournisseurs d'accès, d'hébergement et de services mettront rapidement à la disposition des enquêteurs les informations utiles à la manifestation de la vérité. La transmission de ces informations sous forme numériques[148] permettra de gagner non seulement du temps dans l'action mais éviter la disparition ou le dépérissement des preuves. Les réquisitions par voie télématique permettent à l'officier de police judiciaire d'accéder directement, par la voie d'un réseau de communication télématique ou informatique,

[145] En France, sont ainsi actuellement prévus les enregistrements systématiques des auditions de mineurs victimes, loi du 15 juin 2000 et celles des personnes soupçonnées de crimes et loi du 5 mars 2007, article 64-1 et suivants Code de procédure pénale.

[146] Sur la question des réquisitions judiciaires, voir les dispositions du code de procédure pénale en matière de réquisition, notamment en ses articles 52,149 à 163 et 755.

[147] La dématérialisation des procédures pénales (Allemagne, Canada, Espagne, Italie, Pays-Bas, Royaume-Uni), Paris, le 15 janvier 2010, http://www.justice.gouv.fr/art_pix/gt_dc_2010_dematerialisation.pdf.

[148] En France, les articles 60-1, 77-1-1 et 99-3 du code de procédure pénale, prévoient la transmission la voie télématique ou électronique de réquisitions dans le cadre des enquêtes. l'article 60-2 alinéa 1 dispose que sur demande de l'officier de police judiciaire, qui peut intervenir par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa de l'article 31 et à l'article 33 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenus dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent. l'article 60-2 alinéa 2 prévoit que l'officier de police judiciaire peut, sur réquisition du procureur de la république, préalablement autorisé par le juge des libertés et de le détention, requérir des opérateurs de télécommunication au public en ligne énoncés à l'article 6,i,1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, toute mesure visant à assurer la préservation, pour une durée n'excédant pas un an, du contenu des informations consultées par les personnes d' utilisatrices des services fournis par les opérateurs.

aux informations utiles à la manifestation de la vérité qui sont contenues dans le ou les systèmes informatiques ou traitements de données à caractère personnel administrés par l'organisme ou la personne morale faisant l'objet de la réquisition. La convention de Budapest en matière de cybercriminalité en son article 32 a apporté des éclairages sur cette question. Cet article traite de deux situations. D'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique[149]. Sur le plan de la sécurité, il est important de mettre en place pour chaque Etat une plateforme de certification et de signature électronique ou numérique, généralisée en matière de procédure pénale[150]. Au Sénégal, la loi sur les transactions électroniques prévoit diverses mesures de simplification en matière pénale et précise notamment les modalités d'application, de simplification et de clarification du droit et d'allégement des procédures.

La mise en place de plateforme de certification et signature électronique est nécessaire pour assurer la traçabilité des cyberdélinquants. La signature électronique est un élément constitutif indispensable des transactions réalisées par Internet et de la validité juridique des documents nativement électroniques. C'est, en effet, elle qui permet de garantir l'identité d'un signataire, l'intégrité et la provenance d'un document et, plus largement, l'établissement de la confiance dans les échanges numériques. Pour une mise en œuvre efficace, il faut une technique permettant l'utilisation généralisée d'un internet sécurisé, accessible dans les palais de justice, dans les services d'enquêtes et des progrès de l'information en ligne et en direct. Cette technique permettra même de contourner en partie, et légalement, la retransmission audio-visuelle des audiences en livrant, en temps réel, la transcription des débats sur des blogs diffusés sans limite. Ainsi, il sera possible de développer des modes alternatifs de règlement

[149] La question de savoir qui est la personne « légalement autorisée » pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par exemple, le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article. Pour plus de détails, voir la note d'orientation du n° 3 du Comité de la convention sur la cybercriminalité sur l'accès transfrontalier aux données (article 32), version 5 novembre 2013.

[150] Voir sur cette question la loi n° 2009-526 de simplification et d'allégement des procédures (JORF n° 0110 du 13 mai 2009).

des litiges en ligne désignés sous le terme générique de « cyber justice », alternative apparente aux juridictions traditionnelles et étatiques. Cantonnée en l'état aux litiges en matière de noms de domaine et de propriété industrielle, cette « cyber justice » pourrait à l'avenir s'intéresser au domaine pénal à la condition de prévoir des articulations pertinentes[151]. En plus de l'adaptation des procédures à l'environnement numérique, il est nécessaire de s'intéresser aux moyens d'investigations.

B. L'encadrement des moyens d'investigation

Dans ce cas de figure, une dynamique procédurale s'impose. Car, il nous faudra étudier la modernisation des techniques d'investigation (1) et porter à connaissance la création de nouvelles techniques d'investigation (2).

1. La modernisation des techniques d'investigation

La modernisation des techniques d'investigations passe par la consécration de la perquisition, de la saisie électronique et du transport des pièces à conviction.

La perquisition a pour objectif la recherche, à l'intérieur d'un lieu, d'indices pouvant établir l'existence d'une infraction. Les « perquisitions en ligne » sont des procédures permettant d'accéder à des systèmes informatiques notamment le disque dur d'un ordinateur, les clés USB, CD-Rom, et aussi des données qui peuvent être stockées dans un autre système très éloignés du lieu de la perquisition. Il s'agit en réalité d'une analyse légale de l'ensemble du matériel informatique découvert lors des contestations techniques et qui servira ensuite pour établir les preuves numériques. Ces opérations sont de plus en plus complexes et délicates compte tenu du nombre croissant de supports numériques. En effet, un disque dur saisi dans une affaire judiciaire n'a réellement de sens que si l'on sait quelle était la configuration de l'ordinateur dans lequel il a été saisi, la personne à qui il pouvait appartenir, et on ne pourra garantir l'intégrité de son contenu que s'il a été convenablement protégé de toute modification extérieure entre le moment de sa saisie et le moment de l'analyse par un spécialiste. Sans cela, l'avocat de la défense pourra très raisonnablement rejeter les conclusions tirées à partir de cet objet. Garantir la chaîne de la preuve est une des premières conditions de la bonne gestion de

[151] Voir étude de P. SAUREL et A. OYHAMBERRY, « ce que la cyber justice nous apprend de la justice des signes distinctifs », in gazette du palais, 18- 19 juin 2010.

la preuve numérique, comme ce l'est pour n'importe quel élément de preuve matériel[152]. Les perquisitions de systèmes informatiques connaissent cependant les mêmes limites matérielles et géographiques que les perquisitions opérées dans le monde physique. Ainsi une perquisition ne peut s'effectuer que pour collecter les éléments de preuve sur l'infraction dont le juge a été saisi. Cet obstacle a une portée relativement minime en la matière dans la mesure où la volatilité des éléments de preuve amenuise les chances de flagrant délit. La seule limite légale de droit de perquisitionner est celle de l'accès à des données stockées dans un système informatique situé en dehors du territoire national. S'il est préalablement avéré que ces données accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur[153]. La réserve s'entend notamment des conditions d'accès prévu par la convention sur la cybercriminalité, qui dispose que les données stockées à l'étranger ne sauraient faire l'objet d'une perquisition qu'après avoir recueilli l'assentiment de la personne légalement autorisée à divulguer ces données au moyen de ce système informatique. Pour prendre connaissance de données localisées sur un serveur situé à l'étranger, l'ouverture d'une information judiciaire permettant la délivrance d'une commission rogatoire internationale peut être requise. Elle présente cependant l'inconvénient du délai pour l'obtenir et ce temps peut être mis à profit par le délinquant pour déplacer ou faire disparaitre les données. Les perquisitions des systèmes informatiques connaissent les mêmes protections et les mêmes limites matérielles et géographiques que celles pratiquées dans le monde physique. Autrement dit, une perquisition ne peut avoir lieu que pour collecter les éléments de preuve sur l'infraction dont le juge est saisi, tout en respectant les prescriptions particulières afférentes aux locaux des entreprises de presse et de communication, au domicile d'un avocat, d'un médecin, d'un notaire ou d'un huissier. En enquête préliminaire, les perquisitions de systèmes informatiques telles que prévues par l'article 68 du Code de procédure pénale, ne peuvent avoir lieu qu'avec le consentement exprès de la personne chez qui l'opération a lieu. Enfin, dans le cadre d'une information judiciaire, l'officier de police judiciaire peut, pour les nécessités de l'exécution de la

[152] Freyssinet Eric, « La preuve numérique. Un défi pour l'enquête criminelle du 21e siècle», Les Cahiers du numérique 3/2003 (Vol. 4), p. 205-217 URL : www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm.
[153] V. articles 677-35 à 677-38 du Code de Procédure pénale.

commission rogatoire, procéder aux opérations prévues par les articles 677-35 à 677-38 du code de procédure pénale.

Le Code de procédure pénale autorise les officiers de police judiciaire à accéder au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, (…), par un système informatique implanté sur les lieux où se déroule la perquisition, à des données intéressants l'enquête en cours et stockées sur ledit système ou dans un autre système informatique dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Elles doivent s'effectuer dans le respect de l'intégrité des éléments de preuve et leur caractère irréfutable. Le Code de procédure pénale précise que les données informatiques nécessaires à la manifestation de la vérité sont placées sous-main de justice qui est une saisie juridique en vue de l'exploitation des données. Les données numériques recueillies peuvent être copiées « sur tout support ». C'est ce qu'il convient de qualifier de « saisie informatique » qui n'est pas compatible avec la saisie physique classique des supports de stockage informatique réalisée sur le lieu même de la perquisition. Les officiers de police judiciaire peuvent saisir, lorsqu'ils sont utiles à la manifestation de la vérité, tous les objets et documents ayant servi à l'infraction ou en constituant le résultat. Les supports informatiques comme les cédéroms, les clés USB, les téléphones mobiles doivent être mis sous scellés.

Actuellement, les officiers de police judiciaire sont de plus en plus confrontés à des difficultés liées au volume croissant de données numériques impossible à exploiter durant le temps de la garde à vue. Une fois la saisie effectuée en présence de la personne ayant assistée à la perquisition, il faudrait procéder à l'analyse hors sa présence. Il conviendrait d'harmoniser les cadres juridiques dans le respect du principe du contradictoire et des droits de la défense en sachant qu'en cas de contestation, une expertise pourra être ordonnée sur des données enregistrées en ayant recours à un bloqueur en écriture qui est employé pour garantir la fiabilité de la preuve numérique. Il convient, en effet, d'harmoniser la procédure de saisie et d'exploitation des données informatiques afin de tenir compte de la réalité opérationnelle. Il est impératif de clarifier les modalités de recueil de la preuve numérique tout en sécurisant la procédure par le biais par exemple de protocoles standardisés de recueil de la preuve numérique permettant de sécuriser les procédures en réduisant d'autant les risques de nullité procédurales.

2. La création de nouvelles techniques d'investigation

L'investigation numérique est un ensemble de méthodes visant à l'identification et la présentation devant une juridiction de données stockées par un procédé électronique ou magnétique. Les enquêteurs peuvent recourir à divers actes et mesures d'investigations comme les réquisitions informatiques, les interceptions de communications et mise en œuvre sur Internet, la mise au clair de données chiffrées et la conservation des données de trafic.

Dans le chapitre II intitulé de la conservation rapide de données informatisées archivées, l'article 677-35 dispose : « si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel[154]. L'Article 677-39 du même texte permet à l'officier de police Judiciaire de procéder aux mêmes opérations prévues par les articles 667-35 à 677-38 de la présente loi, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire. Cette nouvelle méthode permet aux autorités judiciaires et aux officiers de police Judicaire compétents la possibilité d'ordonner ou d'obtenir et de conserver rapidement de données électroniques stockées spécifiées dans le cadre d'une enquête ou d'une procédure pénale spécifique. Cette conservation exige que les données qui existent déjà et sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou dégrader la qualité ou l'état actuel. Elle exige que les données soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient gelées (c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes. La personne à laquelle est adressée l'injonction peut, en fonction des spécifications exactes de celle-ci, conserver l'accès aux données. L'article ne précise pas la manière dont les données doivent être conservées. Il appartient à chaque partie d'établir les modalités appropriées de conservation et de déterminer

[154] Loi 2008-11 du 25 janvier 2008 portant sur la cybercriminalité, Sénégal (JORS, n° 6406, du 3mai 2008, p. 419) *(annexe n°1).*

si, dans certains cas, la conservation des données devrait également comporter le gel de celles-ci. Il est également à travers ses dispositions autoriser la mise en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction (de la police ou du parquet, par exemple).

Dans certains États, le droit de procédure ne prévoit pas d'injonctions de conservation, les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire. La loi ne spécifie pas la manière dont la conservation doit être faite. Elle semble introduire une certaine souplesse pour faciliter la mise en œuvre par tous les moyens pour conserver les données, car la rapidité de l'intervention peut, dans certains cas, permettre d'appliquer plus rapidement les mesures de conservation. Au niveau international, on peut trouver un éclairage dans l'article 16 de la Convention de Budapest sur la cybercriminalité qui mentionne à son paragraphe 1 expressément les "données relatives au trafic" afin d'indiquer l'applicabilité particulière de ces dispositions à ce type de données, lesquelles, lorsqu'elles sont collectées et archivées par un fournisseur de services, ne sont généralement conservées dans une brève période.

Concernant l'interception de données de contenues, l'article 677-38 dispose que : « Si les nécessités de l'information l'exigent, le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel. Les interceptions des correspondances émises par la voie de l'Internet, elles obéissent soit au régime de droit commun, soit au régime spécial applicable en matière de criminalité organisée. Les procédures de perquisition dans les systèmes informatiques sont appelées à évoluer et appelle à de nouvelles techniques envisagées. En effet, la captation à distance des images et des sons (caméra et sonorisation de lieux) est aujourd'hui possible mais les enquêteurs ne peuvent avoir accès aux données informatiques que lors des perquisitions. Or certains périphériques ne laissent aucune trace des données dans les unités centrales ou les systèmes d'exploitation. Le seul moyen d'y avoir accès est donc de capter ces données à distance lorsque des périphériques sont reliés à un ordinateur. La loi donne la possibilité aux enquêteurs d'utiliser

les moyens techniques permettant de capter en temps réel les données informatiques temporairement posées telles qu'elles s'affichent pour l'utilisateur d'un système de traitement automatisé ou telles qu'il les y introduit par saisie de caractères. Le recours à ces techniques d'investigations est encadré par la loi pour éviter qu'il y ait atteinte aux libertés individuelles. Lorsque l'installation du dispositif technique nécessite que les officiers de police judiciaire pénètrent dans le lieu privé où se trouve l'ordinateur, un juge des libertés et de la détention sera saisi lorsque la mise en place du dispositif se fera en dehors des heures légales. S'agissant de la mise au clair de données chiffrées. Ce mécanisme procédural est aussi un moyen efficace dans les enquêtes judicaires voir même les enquêtes administratives. Ce mécanisme n'est pas organisé spécifiquement en droit sénégalais. En effet, le code de procédure pénale issu de la loi du 25 janvier 2008 portant sur la cybercriminalité n'a pas prévu des dispositions spécifiques à la mise au clair de données chiffrées.

Pour parvenir à leurs fins, il arrive souvent que les criminels utilisent des techniques ou des programmes de cryptage de certaines données en vue d'entraver la bonne marche des investigations. Comme procédés, les terroristes et les groupes criminels utilisent des techniques de chiffrement[155] bout à bout des informations. Cette technique permet de transmettre les données digitales en toute sécurité par le biais de n'importe quel canal de communication, y compris les réseaux ouverts comme les systèmes de communication classiques et le Web. Les messages sont chiffrés localement avant même d'être envoyés sur le réseau. Ainsi, le serveur se contente de relayer le message chiffré et c'est le client du destinataire qui le déchiffre. Cependant, il ne serait pas excessif de conclure à la nécessité de recourir à ce dispositif de procédure même si on évoque souvent son caractère illégal surtout quand les données interceptées sont des données à caractère personnel. Il ressort des dispositions de l'article 677-37 que lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

En validant la possibilité de saisie portant sur les données utiles à la manifestation de la vérité, le législateur reconnait implicitement au magistrat instructeur le pouvoir d'utiliser les

[155] Dictionnaire Le Larousse : Le chiffrement ou cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

programmes ou logiciels stockés dans le système qui permettent le décryptage des données informatiques. Or, le législateur a habilité l'officier de police judiciaire pour recourir aux moyens d'investigations prévus dans la loi sur la cybercriminalité[156]. Cependant, lorsque les données en question sont des données à caractère personnel qui ne portent pas atteinte à l'intimité de la vie privée, l'officier de police judiciaire (art. 14 CPP) en vertu de son pouvoir général d'enquête et le juge d'instruction en vertu de son pouvoir d'investigation général (art. 72 du CPP) peuvent accomplir tous les actes utiles à la manifestation de la vérité.

Pour lutter contre l'utilisation croissante du chiffrement par les cybers délinquants, il est sans aucun doute que le législateur doit autoriser les magistrats et les enquêteurs à recourir, aux techniques de déchiffrement des messages cryptées, jusqu'ici réservés aux seules forces en charge de la défense nationale, pour assurer le déchiffrement de message cryptés[157].

<u>Paragraphe 2 :</u> L'aménagement des moyens spécifiques de l'interception de flux réseaux

L'aménagement des moyens spécifiques se matérialise en deux phases d'abord par la méthode de la géolocalisation (A) enfin, celle des écoutes téléphoniques et les infiltrations (B).

A. La géolocalisation

La géolocalisation en temps réel (1) est une partie essentielle qu'il nous faudra passer au peigne fin. Enfin, la géolocalisation appréhendée par la loi de 2016 (2) est tout aussi intéressant à étudier.

1. La géolocalisation en temps réel avant la loi de 2016

La reconstitution *a postériori* des déplacements d'un individu n'est pas une mesure de géolocalisation en temps réel. Par un arrêt du 2 novembre 2016, la Cour de cassation a clarifié la distinction qui existe entre géolocalisation en temps réel et mesures de géolocalisation en temps différé. Une perquisition a été effectuée lors de l'interpellation d'un individu suspecté, dans le cadre d'une enquête préliminaire, d'avoir notamment organisé un trafic de stupéfiants. Un téléphone a été saisi dans le cadre de cette procédure. Le procureur de la République a requis, auprès d'opérateurs téléphoniques, les fadettes de ce téléphone. Il s'est pour cela appuyé sur les dispositions de l'article 77-1-1 (1) du Code de Procédure pénale français.

---

[156] C'est ce qui résulte de l'article 677-39 du Code de procédure pénale selon lequel l'officier de police judiciaire peut, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par les articles 667-35 à 677-38 de la sur la cybercriminalité.

[157] 824 Voir la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et les articles 230-1 à 230-5 du Code de procédure pénale français.

La géolocalisation appréhendée par la loi du 28 mars 2014 La loi n°2014-372 du 28 mars 2014 introduit ainsi des dispositions spécifiques sur la géolocalisation en temps réel aux articles 230-32 à 230-44 du Code de procédure pénale, la géolocalisation en temps différé continuant de relever des textes généraux sur les réquisitions. La loi établit les infractions permettant de recourir à la géolocalisation et détermine les autorités compétentes pour autoriser une telle opération ainsi que la durée de ces autorisations. Le recours à la géolocalisation en temps réel est désormais possible en cas d'investigations pour :

- les délits contre les personnes punis d'une peine d'emprisonnement supérieure ou égale à 3 ans,
- les autres crimes et délits punis d'au moins 5 ans d'emprisonnement,
- les enquêtes ou information judiciaire en recherche des causes de la mort, des causes de la disparition et enquêtes en recherche d'une personne en fuite.

Dans le cadre de l'enquête de police (flagrance ou préliminaire), le législateur est allé au-delà de la jurisprudence en autorisant le recours par le procureur de la République à un tel procédé pour une durée maximale de quinze jours consécutifs. A l'issue de ce délai, cette opération est autorisée par le juge des libertés et de la détention (JLD) pour une durée maximale d'un mois renouvelable. Au cours de l'instruction, elle est autorisée par le juge d'instruction, pour une durée de quatre mois renouvelable. Le législateur est également venu encadrer les hypothèses d'introduction dans un lieu privé (professionnel ou d'habitation) afin d'installer un dispositif de géolocalisation. Le juge des libertés et de la détention et le juge d'instruction sont les seuls à pouvoir autoriser cette opération et ce, toutefois à la condition que l'infraction soit passible d'une peine d'au moins 5 ans d'emprisonnement. Récemment, en France, la loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme autorise également le procureur à recourir aux mesures de géolocalisation pour 48 heures à compter de l'ouverture d'une information judiciaire par un juge d'instruction désigné. Certains lieux bénéficient d'une protection absolue (on ne peut y pénétrer à l'insu et sans le consentement du propriétaire ou de l'occupant) : cabinet d'un avocat ou son domicile, locaux d'une entreprise de presse, domicile d'un journaliste, domicile d'un magistrat, cabinet d'un médecin d'un notaire ou d'un huissier, d'un député, d'un sénateur ou d'un magistrat, les lieux abritant des éléments couverts par le secret de la défense nationale. Il existe par ailleurs des exceptions à l'autorisation de procéder à la géolocalisation.

Ainsi, le législateur a prévu en cas d'urgence[158] que le dispositif de géolocalisation pouvait être mis en place par un officier de police judiciaire (OPJ). Toutefois, afin d'assurer un minimum de sécurité juridique, le magistrat, informé immédiatement, peut ordonner la mainlevée de la mesure. La chambre criminelle de la Cour de cassation est très sévère s'agissant de la notification sans délai au magistrat de cette mesure mise en place en urgence. De même, l'intervention du magistrat n'est pas nécessaire pour permettre la localisation d'un téléphone portable ou d'un véhicule de la victime de l'infraction sur laquelle porte l'enquête ou la personne disparue, dès lors que l'opération a pour objet de retrouver la victime, l'objet qui lui a été dérobé ou la personne disparue et que la mesure est prise dans l'intérêt de cette dernière.

2. La géolocalisation en temps réel appréhendée par la loi de 2016

Avec l'évolution de la science et des techniques, de nouveaux modes de preuves ont été développés pour détecter et confondre les malfaiteurs. Sur ce, le législateur sénégalais, tenant compte des nombreuses évolutions technologiques et scientifiques[159], a revu le régime juridique de la preuve en conférant plus de pouvoirs aux autorités chargées d'investiguer et de juger et en créant de nouveaux moyens de preuve destinés à lutter plus efficacement contre les phénomènes criminels récents[160]. Sans aller aussi loin que ses homologues de certains pays d'Europe, notamment la France, la Belgique et l'Allemagne qui en ont profité pour instituer le fichier génétique, le dossier judiciaire numérique, les interrogatoires et auditions par visioconférence, il a autorisé les perquisitions et investigations informatiques, les interceptions électroniques et même la géolocalisation.

Ce faisant, il a étendu le champ d'application des procédures dérogatoires en se souciant peu ou prou de l'effectivité du contrôle exercé par l'autorité judiciaire, seule « gardienne de la

[158] Risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens.
[159] R. HOUIN, « Le progrès de la science et le droit de la preuve », in Revue internationale de droit comparé, vol. 5 n°1, Janvier-mars 1953. pp. 69-75.
[160] Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n°65-61 du 21 juillet 1965 portant Code de procédure pénale, JO n° 6976 du 25 novembre 2016, p. 1627 : « Des mesures normatives tendant à lutter efficacement contre le phénomène du terrorisme ont été prises dans le Code pénal et le Code de procédure pénal, en vue, d'une part, de réprimer plus efficacement les actes terroristes et leur financement, d'autre part de permettre la mise en place d'institution destinées à prévenir les actes de terrorisme. Avec l'acuité particulière que revêt le phénomène du terrorisme au regard de ses manifestations récentes aussi bien sur le plan international que dans la sous-région, il est apparu nécessaire d'améliorer certains aspects de la législation pour une plus grande efficacité de l'action judiciaire dans la lutte contre cette forme de criminalité. C'est ainsi qu'il est envisagé des réaménagements susceptibles d'améliorer le dispositif de lutte contre le terrorisme, avec notamment […] ».

liberté individuelle »[161]. L'évolution est telle que la question se pose aujourd'hui de savoir sur le terrain probatoire, comment dans ce tourbillon de réformes, la matière pénale parvient-elle à concilier l'impératif de protection de l'ordre public avec la nécessaire préservation des droits et libertés des justiciables? Si le législateur, prenant en considération les nombreuses évolutions technologiques, est amené à créer de nouveaux moyens de preuve afin de lutter efficacement contre les formes les plus graves de criminalité, il lui appartient, d'abord et avant tout, de se soucier de l'effectivité du contrôle exercé par l'autorité judiciaire, seule « gardienne de la liberté individuelle ». Il est dès lors, nécessaire de penser sérieusement la place et le rôle du juge des libertés et de la détention dans le dispositif répressif sénégalais afin que ces coups de boutoirs donnés aux libertés fondamentales au nom d'une certaine efficacité de la répression[162] ne compromettent pas durablement le grand équilibre de la procédure pénale sénégalaise. La volonté du législateur sénégalais de rendre effective et efficace la répression des actes terroristes et actes assimilés, a conduit à faciliter l'obtention des preuves par un élargissement des pouvoirs d'investigations des magistrats et officiers de police judiciaire. Les preuves pénales ont été renouvelées et diversifiées avec en arrière fond l'apparent souci de préserver les droits et libertés individuels. C'est ce qui explique le maintien, certes fragile mais nécessaire, du socle classique en matière de preuve pénale. Mais il faut aussi préciser que les actes d'investigation doivent être exercés dans les conditions et dans les limites fixées par les textes qui les prévoient[163].

B. Les écoutes téléphoniques et les infiltrations

Nous analyserons tour à tour les écoutes téléphoniques (1) et les infiltrations (2).

1. Les écoutes téléphoniques appréhendées par la loi de 2016

Les écoutes téléphoniques, ou interceptions, désignent les opérations par lesquelles sont captées, enregistrées et transcrites les correspondances émises par la voie des télécommunications. Dans le souci de protéger les droits et libertés malgré la nécessité de la prévention ou de la répression, la loi autorise les interceptions téléphoniques comme procédés d'investigation criminelle, malgré leur caractère attentatoire à la vie privée. En effet, face aux nouveaux visages du phénomène criminel qui menacent les fondements des Etats, les

[161] H. MATSOPOULOU, « Les nouveaux moyens de preuve au service de la criminalité organisée. – À propos de la loi n° 2016-731 du 3 juin 2016 », J.C.P, G. n° 25, du 20 juin 2016, 707.
[162] M. KONATE, Le temps et le procès pénal au Sénégal, Thèse de doctorat, Université Cheikh Anta Diop de Dakar, 2017, pp. 95 et s.
[163] F. EL HAJJ CHEHADE, Les actes d'investigation, Thèse de doctorat, Université du Maine, 2010, pp. 140 et s.

interceptions de correspondances téléphoniques ou émises par voie électronique peuvent être prescrites par le juge d'instruction. Cependant, il ne doit le faire qu'avec beaucoup de réserve, d'une main tremblante, en soulignant en particulier la nature exceptionnelle de ce moyen d'investigation et en imposant sa description explicite et détaillée par la loi[164]. Ce qui veut dire que les interceptions téléphoniques sont légitimes pour défendre l'Etat contre les menaces terroristes et la délinquance organisée, mais que des garanties doivent permettre d'éviter l'arbitraire. Cela signifie que le système doit reposer sur une loi précise, viser une personne déterminée suspectée d'avoir commis des infractions particulières. Le processus doit respecter les droits de la défense, prévoir des conditions de temps et de lieux précises et définir les procédés de transcription[165]. En somme, il est loisible de dire que les intrusions étatiques dans l'intimité des personnes ne peuvent être légitimes, dans une société démocratique, qu'à la double condition d'avoir été prévues par une loi claire et précise et d'être nécessaires à la préservation d'un des buts légitimes, notamment la poursuite d'auteurs d'infractions pénales. C'est grâce à cette réserve que sont possibles les perquisitions, les écoutes téléphoniques et les sonorisations en droit sénégalais. Le législateur s'est efforcé de réglementer expressément ces situations extrêmement dangereuses pour les droits fondamentaux et de mettre en conformité la législation avec les impératifs posés par les Conventions internationales.

Pour bien insister, l'article 9 in fine de la loi n° 2016-33 relative aux services de renseignement prescrit que toute mesure de contrainte devrait respecter la légalité et être proportionnelle à la gravité de chaque menace. Le principe de proportionnalité apparaît donc comme un instrument de contrôle des mesures qui portent atteinte aux libertés et droits fondamentaux[166]. Dans un arrêt du 24 avril 1990, la cour européenne des droits de l'homme a jugé que les écoutes téléphoniques, telles qu'elles étaient pratiquées avant la loi n° 91-646 du 10 juillet 1991, ne répondaient pas aux exigences de l'article 8 de la Convention européenne des droits de l'homme. Cette convention pose plusieurs règles en la matière, dont la nécessité d'une durée limitée des écoutes et des conditions d'établissement bien spécifiques des procès-verbaux.

---

[164] CPP du Sénégal, Art. 90-16.

[165] N. FRICERO, Droit européen des droits de l'homme, Gualino, 2007, p. 90.

[166] M.Y. DIALLO, « Le contrôle de proportionnalité dans la jurisprudence constitutionnelle en Afrique », Annales Africaines, nouvelle série, vol. 2, n° 7, décembre 2017, pp. 255 et s; F.J. AIVO, « Contribution juridictionnelle à la protection des droits fondamentaux », in Afrilex mai 2016 ; K. HOUNAKE, « L'exigence de proportionnalité dans la jurisprudence de la Cour constitutionnelle du Bénin », RTSJ, janv-juin 2015, pp. 155 et s. ; B. KANTE, « Les droits fondamentaux constituent-ils une nouvelle catégorie juridique en Afrique ? », in Mélanges J.-F. FLAUSS, L'homme et le droit, Paris, Pedone, 2014, pp. 445 et s. ; M. M. SY, La protection constitutionnelle des droits fondamentaux en Afrique : l'exemple du Sénégal, Harmattan 2007.

2. L'infiltration

Par infiltration, on entend le mode d'établissement de faits infractionnels qui consiste en la surveillance par un agent officiel, de la police judiciaire ou des douanes, de personnes suspectées d'avoir commis un crime ou un délit en se faisant passer auprès de ces personnes pour un coauteur, un complice ou un receleur. Cette pratique est subordonnée à l'autorisation du procureur de la République ou, après avis préalable de ce dernier, à celle du juge d'instruction saisi. Elle est réservée aux crimes et aux délits qui prévoient la possibilité d'y recourir.

En matière de cybercriminalité, les plaintes et dénonciations sont fort rares : les victimes participent à l'infraction et les tiers restent muets[167]. Ainsi, privée de plaintes et dénonciations, la police judiciaire ne doit pas se contenter d'être passive. Elle va devoir rechercher activement les preuves, dès qu'elle soupçonne des faits de crime terroriste ou assimilé. La spécificité de la lutte contre cette forme de délinquance justifie que les enquêteurs disposent de moyens adaptés et intrusifs, soit par le renforcement des actes d'enquête classiques, soit par l'utilisation de prérogatives spécifiques. L'un des principaux apports de ces nouvelles lois a consisté dans la mise en place d'une nouvelle procédure pénale dérogatoire ayant vocation à s'appliquer, de manière générale, à des infractions nombreuses et diverses, dont le seul point commun est d'avoir été commises, tentées ou préparées en bande organisée. Ainsi, la loi sur les Services de renseignement, a créé de nouvelles méthodes d'investigation, qui ne sont ordinairement pas possibles dans les enquêtes de droit commun. A l'enquête réactive traditionnelle succède donc, pour la criminalité organisée, une enquête proactive faite de provocations[168]. Les enquêteurs sont ainsi autorisés à surveiller, sur l'ensemble du territoire national[169], les personnes et les objets, les biens et les produits dont il existe des raisons plausibles de penser qu'ils ont un lien avec les infractions terroristes, la criminalité organisée ou les trafics internationaux, bref les infractions visées aux articles 279-1 à 279-19 du Code pénal sénégalais.

Ils peuvent également procéder aux opérations policières d'infiltration afin de surveiller des personnes suspectées de commettre un crime ou un délit relevant du terrorisme et actes d'appui en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices

[167] J. PRADEL, Procédure pénale, 15ème éd., Cujas, 2010, p. 369.

[168] C. BRANTS, S. FIELD, « Les méthodes d'enquête proactives et le contrôle des risques », Déviance et Société, 1997, vol. 21, n° 4, pp. 401-414 ; J. PRADEL « De l'enquête pénale proactive : suggestions pour un statut légal », D 1998, chr., p. 57.

[169] Loi n° 2016-33, Art. 7, al. 1. 126 Loi n° 2016-33, Art. 10.

ou receleurs grâce à une identité d'emprunt et en commettant si nécessaire des infractions pénales, de manière à recueillir les preuves de l'infraction[170]. Dans ces hypothèses, on ne fait aucune distinction selon que la mesure s'inscrit dans le cadre des enquêtes de police ou de l'information judiciaire. L'idée étant d'identifier les ententes criminelles de manière à les prévenir ce qui n'est pas sans exposer le droit de chacun au respect de sa vie privée.

Parmi les prérogatives spécifiques à la criminalité organisée figurent, en outre, les sonorisations, la localisation et la surveillance[171]. L'installation et l'exploitation de ces dispositifs techniques ayant pour objet la captation, la transmission et l'enregistrement, sans le consentement des intéressés, de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux publics ou privés doivent se faire avec l'autorisation et sous le contrôle du procureur de la République[172]. Ce qui veut dire que ces procédés ne sont possibles que dans le cadre des enquêtes préliminaires ou de flagrance. Or, une telle perception peut paraître restrictive, car il est d'avis que ces procédés peuvent être autorisés par le juge d'instruction dans le cadre d'une information judiciaire[173]. Cette analyse trouve appui dans l'interprétation de l'article 72, al. 1 CPP qui dispose « Le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité ». Le renforcement des pouvoirs d'enquête en matière d'actes terroristes et actes assimilés n'est donc pas négligeable vis-à-vis du droit fondamental au respect de sa vie privée et de son domicile[174]. Que faut-il penser de ces nouveaux moyens de preuve ? A première vue, l'ensemble de ces mesures pourrait satisfaire aux nécessités de la répression en matière de criminalité du numérique. De plus, la loi exige le respect du critère de proportionnalité, puisque les opérations en cause doivent être justifiées par la gravité des infractions ayant donné lieu à l'ouverture d'une enquête[175].

---

[170] Loi n° 2016-33, Art. 22, al. 2 « les services compétents de l'Etat fournissent à ces personnels les documents administratifs nécessaires pour leur procurer les identités d'emprunt. La délivrance de ces documents est enregistrée sur des registres et fichiers spéciaux protégés par le secret ».

[171] Loi n° 2016-33, Art. 10.

[172] Loi n° 2016-33, Art. 8, al. 1 : « Les entités d'enquête peuvent, avec l'autorisation et sous le contrôle du procureur de la République compétent, recourir aux moyens d'investigation prévus à l'article 10 ».

[173] A. BONNET, « La licéité du recours à la surveillance par géolocalisation », note sous Cass. crim. 21 nov. 2011, JCP G 2012, n° 3; M. MAAS, « Est-il prévisible que le juge d'instruction ait un coup d'avance sur le législateur ? », Droit pénal 2012, n°1, comm. 12.

[174] C. RIBEYRE, « Etat d'urgence et procédure pénale : le juge pénal compétent pour contrôler les perquisitions administratives - A propos de : Cass. crim., 13 déc. 2016, n° 16- 84.794 et 16-82.176 », Droit pénal n° 3, mars 2017, étude 6.

[175] Loi n° 2016-33, Art 9 « Pour l'exécution des missions qui leur sont assignées, les services de renseignement apprécient la consistance des moyens opérationnels à mettre en œuvre. Ils s'assurent cependant de la légalité des moyens employés et de leur proportionnalité à la gravité de chaque menace ».

Section 2 : Une survivance des difficultés malgré l'amélioration des règles procédurales

Ces difficultés qui feront l'objet de cette sous partie sont dues à l'universalité du réseau Internet (paragraphe 1) et à l'internationalité des comportements cybercriminels (paragraphe2).

Paragraphe 1 : Les difficultés tenant à l'universalité du réseau Internet

D'abord, le réseau numérique est en perpétuel évolution à travers sa configuration (A), ensuite, sa virtualité est aussi source de difficultés (B).

A. L'évolution et la configuration de l'Internet

Nous examinerons tour à tour l'évolution de l'internet (1) et la configuration du réseau internet (2).

1. L'évolution de l'internet

Les technologies de l'information et de la Communication sont nées à la suite d'une longue évolution de la science fondamentale et de la recherche militaire. Les développements technologiques qui ont conduit à l'Internet ont été conçus par des institutions gouvernementales, des Universités, ou des centres de recherche publics. Comme ancêtre de l'Internet, il y a l'ARPA (Advanced Research Projects Agency) mis en œuvre au Pentagone qui donné naissance l'ARPANET et par la suite World Wide Web a été créé par Tim Berners-Lee[176], un programmeur travaillant au CERN de Genève.

En France, le travail sur les réseaux a démarré par la mise en œuvre du réseau Cyclades. Ce réseau avait adopté la technologie de transmission de données par datagramme similaire à celle de l'Arpanet mais il n'était pas relié à l'Arpanet. Des 1972, un groupe de travail a été mis en place afin d'étudier une architecture permettant l'interconnexion des réseaux. Et en 1973, Vint Cerf et Bob Kahn inventèrent le concept d'Internet.

Au Sénégal, l'avènement de la société sénégalaise de l'information est le fruit d'une longue évolution. Le pays s'est connecté officiellement à Internet en 1996[177], pour aboutir à la

[176] T. B.-L. CONNU sous S.T. J. BERNERS-LEE, KBE (tim berners-lee né le 8 juin 1955 à Londres) est un citoyen britannique surtout connu comme le principal inventeur du world wide web. En juillet 2004, il est anobli par la reine ELISABETH II pour ce travail et son nom officiel devient sir Timothy John Berner-Lee. Depuis 1994, il préside le world wide web consortium (w3c), organisme qu'il a fondé.

[177] la société nationale de télécommunications, filiale de la multinationale française, France télécom, avait mis en place une ligne spécialisée à 64kbps reliant le Sénégal aux usa, avant de signer avec la société américaine MCI un accord permettant la connexion internationale à l'internet. C'était un coup d'envoi de l'ère

libéralisation des télécommunications en 1997 et à la mise en place de l'intranet gouvernemental et l'élargissement de la bande passante[178].

La vision de l'e-Sénégal a vite placé notre pays au cœur de la société de l'information, ce qui lui a valu de se voir confier le volet TIC dans le cadre du NEPAD[179].

Au début de l'année 2004, le gouvernement sénégalais décide de bâtir un intranet commun à plusieurs de ses ministères. Son objectif est de dynamiser les relations inter- et intra-administrations, tout en offrant des fonctionnalités diversifiées de gestion et de travail collaboratif. Les développements réalisés pour le compte d'une administration peuvent effectivement être réutilisés librement par d'autres sans frais de licence ou d'investissements contre-productifs. Les prestataires choisis pour la mise en œuvre de cet intranet gouvernemental[180] global sont Nuxeo[181], spécialiste des services autour de Zope, et la société sénégalaise Touch technology. Nuxeo intervient dans un premier temps pour la phase de consulting et d'analyse des besoins, pour les intranets, les annuaires et la gestion du courrier. Le premier déploiement a lieu en avril 2004, sur 4 ministères, au sein de l'ADIE (Agence de l'Informatique de l'Etat)[182] et de la présidence. L'objectif, à terme, est de couvrir l'ensemble des institutions et ministères rattachés au gouvernement.

Le choix d'une plate-forme logicielle libre est par ailleurs vu par le gouvernement sénégalais comme un avantage pour la montée en compétence des équipes locales. "Il s'agit d'un vecteur de développement durable. En effet, à l'issu de ce projet, un véritable transfert de

---

commerciale d'internet au Sénégal, avec comme premier fournisseur d'accès télécom plus, dont le premier client fut la présidence de la république. Sur l'ensemble de ces questions, voir P. A. TOURE, le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal, harmattan, 2014, page 17. Voir également A. TOP, »1996-2006, dix ans de connexion du Sénégal à internet », batik, n°80, mars 2006, éditorial.

[178] Sur l'évolution de l'internet au Sénégal, il faut dire que l'État du Sénégal a engagé une première phase de libéralisation du secteur des télécommunications, en promulguant la loi 96–03 portant Code des Télécommunications. Cette loi permit de séparer pour la première fois, la fonction réglementaire, exercée au nom de l'État par le ministre chargé des Télécommunications, et la fonction d'exploitation des réseaux et services, confiée à des opérateurs agissant dans le cadre de concessions, d'autorisations ou de manière libre. La Sonatel a bénéficié, dans ce cadre, d'une concession pour l'établissement et l'exploitation d'un réseau de télécommunications. Depuis sa première connexion officielle au réseau Internet en 1996, le Sénégal contemporain n'a cessé d'accomplir des avancées considérables dans le secteur des TIC. Par la suite, la Sonatel introduit sur le marché sénégalais l'internet avec l'offre «Sentoo» gérée par sa succursale Sonatel Multimédia et la téléphonie mobile avec l'offre «ALIZE» commercialisée par sa filiale Sonatel Mobiles.

[179] P. A. TOURE, op, cit, p.16

[180]"L'intranet permet de partager des informations avec l'intégration des fichiers bureautiques - et d'utiliser des services de communication : web mail, forums, agendas partagés, etc. au sein d'espaces de travail numériques. Il met aussi à disposition un outil de gestion des courriers entrants et sortants de l'administration"

[181] 583 Nuxeo nuxeo ep est un logiciel de gestion de contenu d'entreprise libre développé par la société nuxeo, qui fournit également de l'assistance, et une communauté de contributeurs.

[182] Agence de l'informatique de l'Etat

compétences sera mis en place afin de permettre aux équipes locales de maîtriser la technologie et de développer autour des outils mis à disposition", note-t-on au gouvernement. "L'objectif est d'élargir la communauté des utilisateurs et des développeurs PS et d'apporter de véritables compétences techniques sur le sol africain", déclare de son côté Stéfane Fermigier, directeur général de Nuxeo.

Aujourd'hui, trois autres opérateurs de téléphonie se sont ajoutés à la SONATEL. Il s'agit des sociétés TIGO, SUDATEL et qui est implanté dans la région de Matam, qui ont fini par placer la vision du e-Sénégal au cœur de la stratégie globale déclinée par le Plan Sénégal Emergent(PSE) qui a identifié l'accélération de la diffusion des TIC comme un des fondamentaux de l'émergence[183]. Cette évolution justifie la configuration du réseau internet.

2. La configuration du réseau internet

Les comportements criminels commis dans les cyberespaces ont pour la plupart un caractère transfrontalier du fait de la structuration et de la configuration de l'Internet. Il est composé d'un ensemble de réseaux informatiques reliés entre eux par un protocole de communication commun (protocole TCP/IP), de manière à constituer un gigantesque réseau mondial. Internet, «le réseau des réseaux», outre le World Wide Web (www), inclut de nombreux services tels que le courrier électronique, les forums de discussion, l'IRC (Internet Relay Chat), le TCP (Transmission Control Protocol), Gopher, Telnet, visioconférence, etc. L'Internet relie tous les ordinateurs du monde entre eux, aujourd'hui, on peut dire tous supports informatiques, à l'image du téléphone qui permet de converser avec toute personne dont on connaît le numéro. Internet est un système mondial d'échange de documents électroniques comme les textes, les fichiers, les images, les sons et les séquences audiovisuelles, au moyen de sites web. Les courriers électroniques, les messageries instantanées, les groupes de discussion et le téléchargement de toute sorte de document peuvent se faire et s'échanger à partir de n'importe quel endroit etc. Cet espace virtuel ou cyberespace est un lieu dépourvu de murs au sens concret du terme, voire de dimensions physiques. Les données accessibles au niveau mondial sont structurées sous la forme d'un support visuel et traversable. C'est une économie

[183] P.A.TOURE, Le traitement de la cybercriminalité devant le juge : L'exemple du Sénégal, harmattan 2014, p.16.Voir également, plan Sénégal émergent, p.80.

fluide de l'information centrée sur les électrodes du commerce transnational, qui fournissent une interface neurologique directe[184]. Un tel espace électronique est un monde imaginaire[185].

Dans le monde réel, le cyberespace est l'endroit où les conversations téléphoniques ordinaires ont lieu, où les courriers électroniques[186] vocaux et les messages électroniques texte sont stockés et échangés. Dans cet espace des graphiques, créés par l'ordinateur, sont transmis et transformés, le tout sous la forme d'interactions, d'une part entre les innombrables utilisateurs et d'autre part, entre les utilisateurs et l'ordinateur lui- même[187]. Le cyberespace se présente comme un espace indéfini. Un espace virtuel[188] d'ordinateurs tous reliés entre eux grâce à des réseaux qu'explorent les « cybernautes », dont les systèmes nerveux sont directement branchés sur les réseaux grâce à une prise fixée sur leur crâne[189]. Le cyberespace comporte beaucoup de caractéristiques qui prennent de l'importance lorsqu'on envisage la problématique de sa régulation. Il peut être considéré comme une « illusion », c'est « une hallucination consensuelle »[190]. Il peut être considéré aussi comme une réalité dans « un monde virtuel». Un monde d'ordinateurs en réseaux de télécommunications, de logiciels et de données informatiques, avec une présence sentie dans un monde physique, c'est donc une «réalité virtuelle »[191]. Le cyberespace est un espace complexe à comprendre[192]. Il est à la fois naturel et artificiel. Naturel de par sa source qui est le monde réel. En même temps, il est un espace artificiel, car le langage utilisé est artificiel. Il est en outre celui des mathématiques qui commence par le codage fondamental (0,1) et en finissant par des équations

[184] UNESCO : Les dimensions internationales du droit du cyberespace, economica, 2000 p. 161 ; voir Également A. SERGE KABLAN : la normalisation technique et juridique des contrats électroniques. Disponible sur : http://www.forac.ulaval.ca/

[186] L'e-mail présente des analogies avec le courrier postal traditionnel, désormais rebaptisé « snail mail »par les internautes, du point de vue du secret qui doit entourer les correspondances. Pour envoyer un message électronique du destinataire, et, grâce à l'utilisation d'un logiciel adéquat, ce message sera acheminé jusqu'à la boite du correspondant. Ce type de communication est donc, rapide et relativement fiable. Bien sûr, le degré de convivialité est moindre devant un écran d'ordinateur qu'avec un combiné téléphonique, mais les internautes ponctuent leurs messages de ce qu'on appelle les « smilles ».

[187] TRIBE: the constitution in cyberspace: law and liberty beyond the electronic frontier, http://cyborgresources.us,consulté le 15/04/2014).

[188] Selon le philosophe PIERRE LEVY « est virtuelle une entité déterritorialisée, capable d'engendrer plusieurs manifestations concrètes en différents moments et lieux déterminés, sans être pour autant elle-même attachée à un endroit ou à un temps particulier ». Sur la nature de cyberespace voir http://www.archipress.org/levy/index.html consulté le 14/11/2014.

[189] P. TRUDEL : quel droit pour la cyber-presse, la régulation de l'information sur internet (paris, légipresse), [mars 1996] ; voir aussi M. FRISON – ROCHE : le droit de la régulation (paris, Dalloz), [2001], n° 7, p. 610 ; voir aussi E. BROUSSEAU : l'autorégulation nécessite-t-elle un cadre institutionnel ? (revue économique), [octobre 2001], vol. 52, hors-série.

[190] W. GIBSON : NEUROMANCIEN (Paris, coll. j'ai lu), [1992] n° 23,25.

[191] UNESCO : les dimensions internationales du droit du cyberespace (Paris, economica), [2000] p. 237.

[192] Voir dans ce sens L. LESSIQ : code and other laws of cyberspace (N.Y., LESSIG), 1999 p. 65.

mathématiques de plus en plus élaborées[193]. Ces équations sont comme le germe d'une infinité d'images dont la plupart n'ont pas de correspondance dans le monde naturel.

Le cyberespace ne résulte pas d'une conception consciente globale, et n'est certainement pas guidé par une idée simple ou un plan. C'est un « réseau» où des idées disparates sont constamment façonnées en de nouvelles fonctions, de nouvelles structures, de nouveaux protocoles qui sont ajoutés au système existant. C'est un système sans principes de base ni formats de conception définis et immuables[194]. Ces considérations montrent sans aucun doute le caractère transfrontalier de l'internet et des crimes qui y sont commis. La criminalité via internet est ainsi mondialisée.

B. La virtualité : source de difficultés

Notre réflexion dans cette partie de nos travaux, portera considérablement, sur la délinquance virtuelle (1) mais aussi, sur la virtualité de la preuve numérique (2) qui nous permettra en somme d'avoir une vision élargie sur la virtualité et ses sources de difficultés.

1. La délinquance virtuelle

Partout où ils se trouvent, les criminels peuvent communiquer en surfant, chatant ou en utilisant les messageries électroniques pour véhiculer n'importe quel message. Ils transmettent des messages en temps réel et la réception instantanée accélère le rythme de la communication. En quelques clics rapides, les délinquants peuvent naviguer de page en page, de site en site, de ville en ville, de pays en pays et de continent à continent. Par exemple des sites comme Google Earth permettent aujourd'hui une visite virtuelle en trois dimensions de la plupart des grandes villes du monde, tout en demeurant sur sa chaise. Par des promenades virtuelles et des voyages à distance, on peut accéder à des lieux qui demeuraient jusqu'alors inaccessibles au plus grand nombre. Les lois de la physique sont bouleversées. Au-delà d'un effacement des barrières géographiques et d'une confusion grandissante entre espace matériel

[193]Disponible sur: le concept CET, http://www.boson2x.org/article.php3; Voir également D. COSTELLO ET S. LIN: error control coding: prentice-hall computer applications in electrical engineering series (Londres, prentice hall), [1982].

[194] voir sur ce point C. HEBRARD, Le village virtuel 3D (mémoire, Montpellier 3), [2000] p. 4 et s ; B. DEFFAINS : économie et ordre juridique de l'espace virtuel, dans E. BROUSSEAU, N. CURIEN (dir), économie de l'internet (revue économique) hors-série, [2001] ; Voir aussi J. DIONIS DU SEJOUR, Rapport n° 612 fait au nom de la commission des affaires économiques, de l'environnement et du territoire sur le projet de loi N° 528 pour la confiance dans l'économie numérique. Disponible sur http://www.assembleenat. fr/12/rapports/r0612.asp> consulté le 03/03/2016) ; A. JOYANDET et P.HERISSON, l'entrée dans la société de l'information, rapport d'information n° 436, mission commune de l'information sur l'entrée dans la société de l'information, septembre 1997. Disponible sur <http://www.senat.fr/rap/r96-436/r96-436.html

et espace virtuel, le dispositif technique sur lequel repose Internet contribue lui aussi à brouiller les repères spatiaux naturels de l'homme. Lorsqu'un nostalgique du nazisme décide, à partir d'un pays où la liberté d'expression n'a pas de limite, d'inonder le monde entier de messages de caractère raciste, il peut, en utilisant les possibilités qu'offrent les nouvelles technologies de l'information et de la communication, se faire entendre sur tous les points du globe. Les messages seront donc nécessairement reçus dans un pays où on considère que la liberté d'expression ne peut autoriser certains excès notamment la provocation à la haine raciale. Si les autorités de ce pays décident d'engager des poursuites, il leur faudra au préalable résoudre un problème de taille : localiser l'auteur des messages et le territoire à partir duquel il les a mis en ligne. Il ne s'agit certes pas d'un problème insurmontable, mais il faut tout de même reconnaitre que la tâche des autorités chargées de l'enquête ne sera pas aisée, compte tenu de la relative fiabilité des moyens techniques de repérage qui sont actuellement disponible.

A supposer ce problème résolu, il faudra faire face à d'autres difficultés lorsque l'auteur présumé des messages et le site émetteur sont localisés à l'étranger. Dans une telle hypothèse il y a des fortes chances que les éléments de preuve se trouvent aussi à l'étranger. Or, le principe de la souveraineté des Etats s'oppose à ce que l'activité des autorités judiciaires ou policières relevant d'un Etat puisse s'exercer en dehors des frontières de cet Etat. Une « perquisition » des systèmes automatisés de traitement de l'information situés à l'étranger serait impensable. Il ne reste qu'une solution ; solliciter de l'Etat sur le territoire duquel est situé le site (commission rogatoire internationale, communication transfrontalière de pièces etc.). Mais on mesure immédiatement la faiblesse d'une telle solution. On voit mal un Etat s'engager dans une entreprise d'entraide judiciaire ou policière qui conduit à la répression d'un agissement qu'il juge parfaitement licite. La diversité des règles apparait, là aussi, comme un facteur d'impunité de ceux qui se livrent à des activités illicites en utilisant les nouvelles technologies. En attendant une meilleure harmonisation des législations, les autorités chargées des enquêtes n'ont d'autres ressources que d'utiliser elles aussi les mêmes méthodes que les délinquants, mais à des fins tout à fait différentes. C'est ce qui explique le recours de plus en plus fréquent aux nouvelles technologies pour les besoins des investigations. Mais cette solution est, compte tenu de l'environnement, d'une efficacité très limitée.

2. La virtualité de la preuve numérique

La preuve numérique représente toute information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire. Les entreprises doivent fournir un document électronique qui puisse être retenu comme preuve par les tribunaux. Les outils numériques, tels que les courriels, la signature électronique et les documents numériques, constituent des éléments de preuve nécessaire à la défense d'un professionnel en cas de mise en cause.

Support de la nouvelle société de l'information et de la communication, outil de travail mais également de loisir, le numérique est « partout ». Devenu la mémoire virtuelle de l'homme, le numérique constitue un terrain d'investigation privilégié, une source d'information intarissable. Le principe de la liberté des preuves en procédure pénale a offert au numérique la possibilité de jouer un rôle majeur : parfois preuve de l'infraction, de son imputabilité à un auteur et/ou de son identité, il est devenu incontournable. Ce constat est toutefois limité, ce principe ne signifiant pas que l'on puisse agir de n'importe quelle manière, à sa guise quels que soient le lieu et l'heure ; la preuve numérique devant être recherchée et recueillie dans les règles de l'administration de la preuve. Soumise à l'intime conviction du juge, la donnée numérique devra également revêtir des garanties d'intégrité et de fiabilité, avant d'être considérée comme une « preuve ».

Au Sénégal, l'écueil de la preuve électronique est subordonné à la réunion des conditions d'imputabilité et d'intégrité prévues par l'article 37 de la loi sur les transactions électroniques. En vertu de ce texte, l'écrit électronique ne vaut preuve, au même titre que l'écrit sur support papier, qu'à condition que « puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans les conditions de nature à en garantir l'intégrité ». L'équivalence fonctionnelle entre l'écrit électronique est donc admise sous réserve du respect de ces deux conditions cumulatives. En définitive, ces observations imposent que, les caractères généraux de la preuve numérique et son rôle probatoire attendu soient étudiés afin d'envisager comment cette nouvelle preuve se conforme au régime probatoire pénal. La fugacité des données informatiques et numériques multiplie les difficultés de recueil et de conservation de la preuve et la nature immatérielle de ces données entraine un effacement problématique des frontières entre sphère privée et sphère professionnelle notamment dans l'activité des salariés. Cette nature immatérielle oblige aussi à reconsidérer les notions de souveraineté étatique, face à l'extraterritorialité des données qui ne sont pas toujours constituées dans le pays de commission de l'infraction : la cybercriminalité s'épanouit dans des réseaux numériques complexes et pose des questions juridiques nouvelles pour les pénalistes. Confrontés à toutes

ces difficultés, nous pourrions être tentés de dire que le droit s'épuise à poursuivre la preuve numérique dont les frontières s'échappent toujours plus loin.

La justice est-elle condamnée à faire un travail inutile et vain en matière de preuve ? Sur ce point, nous pouvons affirmer que la preuve numérique est effectivement en perpétuelle construction et que, même si elle s'élabore moins rapidement que la technique qui évolue à grande vitesse, le cadre juridique de la preuve numérique dans le litige est le droit de la preuve. Or, les attentes des justiciables, des avocats et des juges sont les mêmes pour la preuve numérique et les autres preuves : cette preuve doit être fiable et crédible. Pour que la preuve numérique soit fiable, ou solide comme disent les anglo-saxons à propos de l'admissibilité de la preuve recueillie lors de la discovery, il est impératif que les données soient réunies selon une méthodologie acceptée par tous. Pour qu'elle soit crédible, elle doit résister à la discussion : l'expert doit alors tout remettre en œuvre pour que les parties puissent débattre de toutes les questions posées par cette preuve numérique. La convention signée en 2009 par la Cour d'appel de Paris, les barreaux des neuf tribunaux du ressort et l'Union des compagnies d'experts près la cour d'appel de Paris demande aux experts de remettre aux parties un document de synthèse avant qu'elles n'émettent leurs observations, afin de favoriser la discussion et épuiser le débat technique lors du temps de l'expertise. C'est à l'aune de cette discussion contradictoire que le juge se convaincra de la pertinence des conclusions expertales.

Dans les réseaux électroniques, la problématique de la preuve est l'une des questions les plus complexes du droit du cyberespace. Lorsque les cyberdélinquants utilisent les réseaux électroniques à des fins délictuelles, la nature dématérialisée de l'objet de l'activité infractionnelle (données informatiques, système d'information, programmes), ne manque pas d'entrainer une dilatation des repères des techniques traditionnelles d'investigation judiciaire (perquisition, saisie, mesures conservatoires, etc.) conçues pour la recherche d'éléments matériels. De nos jours, l'avènement du « cloud computing » ou « informatique des nuages » offre aux entreprises une solution de délocalisation et d'externalisation de leurs serveurs et des données qui y sont contenues, à l'aide de logiciels spécifiques fournis par les fournisseurs de services de « cloud computing ». Cette nouvelle technologie pose de nouveaux enjeux à l'enquête judiciaire[195]. Comment les services répressifs vont-ils pouvoir localiser les données dans les « nuages » ? Comment identifier le prestataire assurant le stockage des données

[195] A. SEGER, « Le cloud computing, les défis rencontrés par les autorités de répression », in « Coopération contre la cybercriminalité », conférence Octopus Interface, 23-25 mars 2010 : http://www.coe.int.

nécessaires à la manifestation de la vérité ? Face à ces enjeux stratégiques, le législateur pénal sénégalais de 2008 a entrepris d'élargir les pouvoirs d'investigation des juges d'instruction, en esquissant une politique d'instrumentalisation des TIC à des fins probatoires.

Paragraphe 2 : Les difficultés tenant à l'internationalité des comportements cybercriminels

Le processus du développement technologique est comparable à la construction d'une cathédrale, chaque nouvel arrivant laisse un bloc au sommet des fondations antérieures, de sorte que chacun peut dire qu'il a construit la cathédrale. Aujourd'hui la criminalité sur les réseaux est étudiée en droit pénal international comme une manifestation de la criminalité transnationale donc transfrontalière même si une infraction commise sur les réseaux peut présenter qu'un caractère national. Ainsi, nous constatons des difficultés tenant à l'internationalité du réseau Internet dont nous allons d'abord étudier ces fondements (A), avant d'analyser ensuite que pour une politique efficace de lutte contre la cybercriminalité les Etats doivent renforcer la coopération internationale (B).

A. Les fondements de l'internationalisation des comportements cybercriminels

Par internationalisation, il faut entendre l'essor quasi généralisé des comportements liés à la cybercriminalité. L'acte se développe instantanément dans plusieurs pays. L'internationalisation des comportements cybercriminels s'explique par la dématérialisation de l'espace (1) et la connectivité généralisée des réseaux internet (2).

1. La dématérialisation de l'espace

La dématérialisation peut s'expliquer par la transformation d'un traitement de documents réels en traitement numérique c'est-à-dire en données numériques. Cette dématérialisation de l'espace entraine la dématérialisation des comportements cybercriminels. Une modification de la perception, que l'homme a de la réalité, s'est vite opérée, et plus précisément des notions d'espace-temps qui se répercute à son tour sur les rapports que l'être humain entretiennent avec les traditions commémoratives et les lieux qui leur sont consacrés. Internet a conduit à une dématérialisation en opérant un déplacement de la mémoire humaine vers la mémoire informatique. La manipulation directe des objets visuels à l'écran par la main, l'hypertexte, les icônes, les simulations graphiques interactives de phénomènes complexes, l'interconnexion générale des documents, les moteurs de recherche, les forums en ligne et les mondes virtuels multi participants représentent les premiers pas d'une avancée qui se

poursuivra dans les années et les siècles à venir. Il s'agit d'une mutation des infractions à la loi pénale qui sont non seulement virtuels mais transfrontaliers. Le Web sémantique exprime l'intelligence collective de l'humanité mondialisée interconnectée dans le cyberespace[196]. Les Technologies de l'Information et de la Communication ont fait presque oublier le caractère novateur et disruptif, et la redéfinition radicale que celles-ci entraînent des rapports de l'homme numérique avec l'espace et le temps.

Aujourd'hui, il est possible de consulter des sites Web, grâce à l'existence d'une multitude de liens hypertexte et, plus généralement, de ce que l'on appelle des « signes passeurs ». Ce «passages d'un univers à un autre » à force de clics provoque à long terme une «désorientation » que l'on relève sans équivoque[197]. Les Technologies de l'information et de la Communication ont neutralisé l'espace et le temps par la création d'un espace virtuel sans limites ou du moins dont les limites sont inconnues. Le cyberespace a ainsi mené vers une globalisation du crime par une interaction des criminels qui sont établis dans les quatre coins du monde. Cette interaction permet aux réseaux des cybercriminels de planifier leurs actions sans contact physique. Ils sont difficiles à localiser et l'interaction continue dans le cyberespace, a facilité l'interconnexion des réseaux de cybercriminels[198]. De ce fait, la navigation dans la profondeur de la nature « virtuelle» est source d'un nouveau type de criminalité. La causalité dans le cyberespace est différente de celle, locale, régissant le niveau macro physique et de celle, globale, régissant le niveau quantique. La causalité dans le cyberespace est une causalité en boucle ouverte, due à l'interface homme-cyberespace- temps. L'être humain découvre en lui-même un nouveau niveau de perception grâce à son interaction avec l'ordinateur, et l'ordinateur affine ses potentialités par l'interaction avec l'être humain[199]. La connectivité est généralisée.

---

[196] PIERRE FISCHOF, Le Web et l'intelligence collective, utopie ou réalité, Un Web sémantique «humanitaire» peut-il exprimer l'intelligence collective ? La Lettre d'ADELI n°56 – ÉTÉ 2004.

[197] Sur le concept de « signe passeur », voir SOUCHIER et al. 2003.

[198] B. STERN : vers la mondialisation juridique ? Les lois helms-burton et d'amato kennedy (paris, rgdip), [1996], p. 979-1003. En effet, « la mondialisation, ce n'est pas simplement l'amplification des échanges, c'est la mise en compétition des systèmes économiques et sociaux. Toute la question est de savoir si ce phénomène est de nature à valoriser le système non marchand (culturel) des sociétés ou si au contraire de la prise en compte des systèmes sociaux dans la compétition conduira à considère ceux-ci comme des coûts ». Z. LAIDI : malaise dans la mondialisation (paris, textuel), [2001], p. 45-47 ; voir également s. berger : notre première mondialisation (paris, seuil), [2003] ; L. YAGIL : internet et les droits de la personne (paris, les éd du cerf), [2006] ; le temps : comment l'intelligence collective peut surgir sur le net (entretien avec PIERRE LEVY), [22 février 2001].

[199] Dans cette optique la United states district court for the Northen district of California a déclaré le 7 novembre 2001 dans l'arrêt Yahoo que : « le réseau internet permet d'offrir toute information, tout produit ou tout service à chaque internaute et de transformer les espaces juridiques nationaux en frontière de papier ».

2. Une connectivité générale

La connectivité généralisée a fait de l'internet un espace «de territorialité » c'est-à-dire un réseau sans frontière terrestre, « un espace en dehors des territoires sous souveraineté des Etats ». Elle s'explique par l'existence de normes ouvertes et de systèmes d'adressage permettant de transférer les données numériques par paquets sur une architecture de réseau distribué. Le réseau procure une connectivité généralisée. Il entraine la mondialisation des activités criminelles du fait des logiciels ouverts et évolutifs accessibles à l'ensemble des utilisateurs. Il s'y installe dés lors de multiples activités économiques et le « commerce électronique[200] » en est un exemple.

L'avènement des TIC en réseau rend possible une dissociation complète entre l'information et son support physique. Il s'agit là de l'étape ultime d'un mouvement dont l'origine est fort ancienne et qui n'a cessé de rendre plus lâche le lien entre contenus et contenants. Les réseaux numériques permettent en effet la circulation de contenus d'information – textes, sons, images débarrassés de la gangue de tout contenant : l'information est ainsi en train de devenir un bien économique autonome.

On peut déjà juger de ses effets potentiels en observant les secteurs en avance, comme celui de l'édition musicale, fortement déstabilisé par le foisonnement des échanges pair à pair (peer to Peer)[201] de fichiers MP3. On prend alors la mesure de la remise en cause des modèles

[200] On appelle « commerce électronique » (ou e-commerce) l'utilisation d'un média électronique pour la réalisation de transactions commerciales. La plupart du temps il s'agit de la vente de produits à travers le réseau internet, mais le terme de e-Commerce englobe aussi les mécanismes d'achat par internet (pour le b-to-b). le client effectuant des achats sur internet est appelé cyberconsommateur. le e-commerce ne se limite pas à la seule vente en ligne, mais englobe également :

- La réalisation de devis en ligne
- Le conseil aux utilisateurs
- La mise à disposition d'un catalogue électronique
- Un plan d'accès aux points de vente
- La gestion en temps réel de la disponibilité des produits (stocks)
- Le paiement en ligne
- Le suivi de la livraison
- Le service après-vente

Dans certains cas, le commerce électronique permet un haut niveau de personnalisation des produits, notamment si le site de commerce électronique est couplé avec le système de production de l'entreprise (par exemple cartes de visites, objets personnalisés tels que t-shirts, tasses, casquettes, etc.).

Enfin, pour les services et produits électroniques (fichiers mp3, logiciels, livres électronique, etc.), le commerce électronique permet de disposer de son achat dans un temps très court voire instantané.

[201] Le pair à pair ou pair-à-pair (traduction de l'anglicisme peer-to-peer, souvent abrégé « p2p ») est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur. Le pair à pair peut être centralisé (les connexions passant par un serveur central intermédiaire) ou décentralisé (les connexions se faisant directement). Il peut servir au partage de fichiers en pair à pair, au calcul distribué ou à la

économiques classiques par cette « libération » de l'information: un mouvement de bascule s'opère dans la transition menant de « l'ancienne économie », dans laquelle les coûts fixes de création et d'édition des contenus étaient faibles relativement aux coûts variables de leur reproduction et de leur diffusion. L'Internet consacre la convergence entre deux types de communication auparavant séparés : la « communication adressée » de personne à personne, du type courrier ou téléphone et la « communication flottante », de point à masse ou de point à groupe[202], du type télévision, presse, publication, conférence, etc. L'Afrique plus précisément la région Ouest africaine a connu également le développement des Technologies de l'Information et de la Communication avec la politique de dématérialisation des procédures et la floraison des activités numériques, l'e-commerce est un exemple dont profitent les criminels pour perpétrer des actes délictuels comme le vol, le piratage et les atteintes aux systèmes d'information.

En un mot, la dématérialisation de l'espace et la connectivité généralisée des réseaux internet entraine une mondialisation et interconnexion des comportements des cybercriminels. A cet effet, les infractions qui se commettent dans le cyberespace se caractérisent par leur pluri localisation. D'où l'intérêt de renforcer la coopération internationale contre la cybercriminalité.

B. Un nécessaire renforcement de la coopération internationale contre la cybercriminalité

Dans le cadre de la lutte contre la cybercriminalité, le procédé le plus adapté est la coopération entre les Etats et les autorités judiciaires[203]. Cette technique d'internationalisation devrait passer par un renforcement de la coopération juridique internationale (1) qui est de nature à favoriser une intensification de la coopération juridique internationale (2).

---

communication. Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, en y partageant simplement des objets – des fichiers le plus souvent, mais également des flux multimédia continus (streaming), le calcul réparti, un service (comme la téléphonie avec Skype), etc. la particularité des architectures pair-à-pair réside dans le fait que les données puissent être transférées directement entre deux postes connectés au réseau, sans transiter par un serveur central. il permet ainsi à tous les ordinateurs de jouer directement le rôle de client et serveur (voir client-serveur). On appelle souvent nœud les postes connectés par un protocole réseau pair-à-pair.

[202] La société de l'information, rapport N. CURIEN ET P.-A. MUET, commentaires de E. COHEN, M. DIDIER, compléments de G. BORDES, G. BREGANT, M. CAMPANA, A. CRAWFORD, E. EVENO, I. FALQUE-PIERROTIN, D. FORAY, R. HEITZMANN, D. LATOUCHE,F. LENSEIGNE, K. REVCOLEVSCHI, P. ROUSSEL,J.-M. SALAÜN, M. VILLAC, D. ZMIRO,la documentation française. Paris, 2004.

[203] V. MALABAT, ibid. : « Pour la criminalité, disons ordinaire, la voie de l'internationalisation doit donc être plus raisonnable, plus praticable : c'est la coopération pénale »

1. L'amélioration de la coopération juridique internationale

A l'heure de l'avènement du « cybermonde », « lieu étrange, en tout cas, qui n'est nulle part et partout »[204], la lutte contre la déviance des réseaux ne saurait s'accommoder d'une conception autarcique du traitement de la criminalité. Le professeur Delmas-Marty évoque à ce sujet « l'illusion de l'autonomie parfaite » entre les systèmes pénaux[205]. La cybercriminalité, revêtant souvent un caractère international, la riposte de la communauté des Etats doit également s'organiser au plan international de façon coordonnée et concertée. L'articulation de réponses nationales au phénomène, encouragée par les documents pertinents de la société de l'information, est certes nécessaire. Mais elle serait dépourvue de sens si elle devait être exclusive. Déjà, la loi sénégalaise n° 2008-10 du 25 janvier 2008 portant loi d'orientation relative à la société de l'information, qui a consacré les principes généraux du droit de la société de l'information, a posé dans son article 85 un principe de coopération. Ce texte dispos que « l'édification d'une société de l'information à dimension humaine est une entreprise commune qui requiert une coopération et un partenariat entre toutes les parties prenantes au triple plan national, régional et international ». L'amélioration de la coopération internationale[206] est indispensable à l'efficacité de la cyber-répression. L'on a même parlé de la nécessité de l'élaboration d'une « politique criminelle mondiale »[207] en vue de la naissance d'un « droit pénal mondial du cyberespace »[208]. La coopération pénale internationale évoque la coopération entre les Etats, c'est-à-dire la coopération interétatique destinée, par une sorte de « souveraineté partagée », à mettre les dispositifs pénaux « en relation, à faire communiquer entre eux[209]. Face aux enjeux stratégiques suscités par la lutte internationale

---

[204] M. VIVANT, « Cybermonde : Droit et droits des réseaux », JCP, 1996, éd. G., I, 3969, n° 1.

[205] M. DELMAS-MARTY, Les forces imaginaires du droit (II), le pluralisme ordonné, édition du Seuil, 2006, p.17.

[206] Sur l'ensemble de cette question V. La coopération juridique internationale, Actes de la 6e Journée nationale du Droit, LGDJ, 1994, notamment, le rapport du professeur C. CHAMPAUD, L'expertise, p. 23 : la coopération juridique internationale « est fondée sur l'échange de savoir et de savoir-faire en matière juridique (…) elle se traduit par l'harmonisation des législations nationales, par l'élaboration d'un droit commun qui emprunte, syncrétiquement, aux différents droits en relation des règles et ces méthodes qui paraissent préférables chaque fois à celles du droit interne » ; également, M. MASSE, « Des figures asymétriques de l'internationalisation du droit pénal », RSC, octobre/décembre 2006, p. 757 : « La coopération constante la division du monde entre les Etats souverains et coexistence de systèmes juridiques nationaux. Son objectif est de mettre ces systèmes en relation, de les faire communiquer entre eux. La mise en communication s'établissant sur la base de la méfiance secrétée par la souveraineté de chacun ».

[207] M. QUEMENER et Y. CHARPENEL, Cybercriminalité ; Droit pénal appliqué, Economica, Paris, 2010, p. 232, n° 1124.

[208] J.P. MIGNARD, Cybercriminalité et cyberépression, entre désordre et harmonisation mondiale, thèse, Paris I, 2004, p. 11 et 572.

[209] M. MASSE, « Des figures asymétriques de l'internationalisation du droit pénal », RSC, octobre/décembre 2006, p. 755 ; V. également, C. GARCIN et N. MEZERREB (dir.), L'entraide judiciaire internationale en matière pénale : études des demandes émises et reçues par la France en 1995, Université Jean Moulin, Lyon 3,

contre la cybercriminalité, les techniques de coopération pénale doivent nécessairement s'adosser sur des instruments pertinents de coopération juridique, gage d'une harmonisation internationale de la répression de ce phénomène criminel.

En droit pénal international, il est classique d'analyser exclusivement les dispositifs de coopération internationale sous l'angle des structures formelles de la coopération répressive, c'est-à-dire des instruments normatifs permettant le rapprochement des législations des différents Etats. Cependant, la coopération juridique contre la cybercriminalité présente certaines spécificités, en raison de la diversité des modèles de coopération répressive existants. Face au développement du fléau de la criminalité informatique, plusieurs instances internationales ont été amenées à appréhender ce phénomène. Il s'agit notamment des Nations unies, de la CEDEAO, de l'Union africaine, de l'Union européenne, du Conseil de l'Europe, de l'Union internationale des télécommunications (UIT) et de l'Organisation de coopération et de développement économique (OCDE)[210]. Certaines organisations communautaires ont envisagé un système de coopération de nature contraignante, alors qu'à l'échelle internationale se développe, à partir du modèle onusien, une approche non coercitive d'intégration normative. L'identification du cadre institutionnel pertinent de coopération contre la cybercriminalité constitue un préalable à la négociation de l'instrument juridique de lutte contre ce phénomène. Cette problématique suscite de nombreuses interrogations : à quelle échelle institutionnelle les instruments de prévention et de lutte contre la cybercriminalité devraient-ils être négociés ? L'espace normatif communautaire constitue-t-il le cadre pertinent de la négociation de l'instrument de lutte contre le phénomène cybercriminel ? Force est de constater que le paysage des modèles institutionnels de coopération contre la délinquance du cyberespace est caractérisé par un enchevêtrement d'approches normatives, sortes de « hiérarchies discontinues alternatives et inversées » ou de « pyramides inachevées »[211]. Cette situation laisse a priori une impression de « désordre normatif »[212]. Quoi qu'il en soit, le caractère transnational de la délinquance numérique, postulant un effort international concerté des Etats, a, d'une part, mis en relief l'insuffisance des modèles communautaires de coopération et a, posé à la communauté internationale le défi de la construction d'une approche internationaliste de coopération contre le cybercrime.

Centre de recherche de l'Institut d'études judiciaires, ministère de la Justice, 2000, p. 10 : « Une lutte efficace en matière de délinquance internationale implique une étroite collaboration entre les Etats ».

[210] M. QUEMENER et J. FERRY, Cybercriminalité. Défi mondial, 2e édition, Economica, 2009, p. 267 et s ; M. QUEMENER, « Lutte contre la cybercriminalité. Où en est-on des instruments internationaux ? Expertises, mars 2011, p. 96.

[211] M. DELMAS MARTY, Pour un droit commun, Le Seuil, coll. « La librairie du XX siècle », 1994, P. 91-113.

[212] D. DELMAS-MARTY, Trois défis pour un droit mondial, Le Seuil, coll. « Essai », 1998, p. 92.

En Afrique, la cybercriminalité été pendant longtemps considérée comme une délinquance spécifique aux pays développés, surtout en raison de la faiblesse du taux de pénétration des TIC. Il en était résulté une absence d'encadrement juridique du phénomène par les espaces communautaires africains. Maitre Kalina n'a pas hésité à écrire qu'en Afrique « au désert numérique s'ajoute donc, effectivement, un véritable désert juridique l'un expliquant l'autre »[213]. Cependant, les avancées réalisées par beaucoup de pays africains, à l'image du Sénégal, en matière de réduction de la fracture numérique, ainsi que la menace que constitue la criminalité informatique pour la sécurité des réseaux, ont fini par faire naitre une prise de conscience des enjeux liés à la lutte contre cette forme de criminalité en Afrique.(…)

Il faut noter qu'en raison du caractère transnational et délocalisé de la cybercriminalité, le Sénégal a besoin d'un instrument juridique international et contraignant pour s'inscrire dans la croisade contre ce phénomène multiforme[214]. C'est ce qui a fait dire au professeur Ndiaw Diouf que, « face aux graves menaces que font peser sur la communauté internationale les agissements de cette nature (cybercriminalité), la collaboration des Etats mous parait indispensable. Elle pourrait prendre la forme d'une convention universelle répressive »[215].

Or, la profusion des modèles de coopération a donné naissance à une variété d'instruments de lutte contre la cybercriminalité. Il s'agit des recommandations des Nations unies, des directives et règlements de l'UEMOA, de la CEDEAO, de la CEMAC/CEEAC et de la convention de Budapest sur la cybercriminalité. Il s'est ainsi très vite posé la question du choix, parmi les mécanismes juridiques existants, de l'instrument pertinent de lutte contre les agissements cybercriminels. Dans le cadre de l'Union Africaine (UA), les ministres en charge des TIC ont proposé un Projet de Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace, intégrant des dispositions relatives à la lutte contre la cybercriminalité. Cependant, les limites et les lacunes de cette proposition ont permis de mieux comprendre la nécessité pour le Sénégal d'adhérer à la convention Européenne sur la cybercriminalité. Un instrument africain de prévention et de lutte contre la cybercriminalité présente le mérite de favoriser l'harmonisation des stratégies de lutte contre la

[213] L. KALINA, « Afrique et cybercriminalité : sortir du désert juridique », 3mars 2006 : http : //www. Blogg.org/blog-35519-themes-seminaire_afrique_et_cybercriminalité-64801.htlm (consulté le 15 avril 2019)

[214] Sur l'exigence d'un instrument juridique international pour l'environnement cyberpatial, A.M BALSANO, « Un instrument juridique international pour le cyberespace ? Analyse comparative avec le droit de l'espace atmosphérique », in « Les dimensions internationales du droit du cyberespace », UNESCO, Economica, 2000, p. 159 et s.

[215] Nd. DIOUF, « Infraction en relation avec les nouvelles technologies de l'information et procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale », Rev. sen. Dr. Aff., n° 2, 3, 4, 2003-2004, p. 70.

cybercriminalité dans les Etats. Ce projet aura eu le mérite « politique » de constituer un instrument juridique contre la cybercriminalité élaborée et mis en œuvre par des Africains.

Ne risque-t-il pas d'être « un mécanisme juridique de trop » ? Il est légitime de le penser. L'échelle continentale (Union Africaine) choisie pour négocier l'instrument de lutte contre la criminalité informatique ne nous semble pas être à la mesure de la dimension planétaire du phénomène, qui dépasse les frontières des Etats africains. Aussi, le projet de Convention Africaine ne prévoit aucun mécanisme de coopération judiciaire (modernisation des mécanismes d'entraide, extension de champ de l'extradition, point de contact en matière de cybercriminalité, etc.) de nature à faciliter la création d'un « espace judiciaire africain » de lutte contre ce phénomène.

La mise en place de cet espace judiciaire de coopération permettra-t-elle de dissiper les difficultés rencontrées par les juges africains dans la conduite des investigations judiciaires tendant à la répression des comportements cybercriminels présentant un caractère d'extranéité ? En matière de perquisition et de saisie électronique, une étude a déjà montré que lorsque les éléments de preuves sont éparpillés au-delà du continent africain, le juge se heurtera aux difficultés classiques d'étendre ses opérations en dehors du continent africain, faute d'un cadre de coopération judiciaire international approprié[216]. L'analyse des dispositions transitoires du projet de Convention de l'UA[217] révèle que ce texte ne constitue pas un instrument juridique ayant une dimension internationale, comme la Convention européenne de Budapest. En effet, le projet de Convention africaine, ouvert à la signature, à la ratification ou à l'adhésion des Etats membres de l'Union africaine[218], ne comporte aucune disposition prévoyant une possibilité d'adhésion par un Etat non membre de l'union. Le projet de Convention de l'UA sur la cybersécurité est instrument africain de lutte contre la cybercriminalité. Or, la cybercriminalité n'est pas un phénomène criminel africain, mais un fléau international. Dès lors, l'instrument devant servir à la riposte contre cette délinquance doit, pour être efficace, être négocié à l'échelle internationale.

[216] A. KABORE, La problématique des perquisitions et saisies en ligne en Afrique de l'Ouest : état des lieux et perspectives. Cas du Burkina Faso, du Mali, du Sénégal et du Togo, mémoire, master, droit du cyberespace africain, Saint-Louis, 2006-2007, p. 58 : « Une convention adoptée, à l'échelle africaine nous parait d'un secours peu fort. En effet, aussi large que puisse être un tel instrument, il ne résoudra pas assez efficacement la question des enquêtes en général, et celle des perquisitions et saisies en ligne, particulièrement (…). Le problème en cause n'est pas propre au continent africain, il est global, c'est-à-dire mondial ».
[217] V. art. IV-2 et s. du projet de Convention africaine de l'UA.
[218] V. art. IV-2 du projet de Convention de l'UA.

Il faut donc reconnaitre que le choix de la création d'un instrument juridique à l'échelle africaine, pour méritoire qu'il soit, ne semble pas procéder d'une démarche pragmatique orientée vers la lutte efficace contre la délinquance numérique.

Cependant, la voix de l'adhésion à la Convention de Budapest sur la cybercriminalité pourrait utilement être explorée par le Sénégal. L'avènement du phénomène cybercriminel a entrainé une globalisation des risques qui pose à la communauté internationale le défi de la construction d'un ordre mondial contre ce fléau. Dans le champ juridique, la quête de cet ordre international contre le cybercrime semble conduire à une « double instance »[219]. D'une part, dans le cyberespace, la « multilocalité » des comportements criminels a sonné le glas du paradigme du « pluralisme de séparation ». Ce phénomène a mis en relief « l'utopie de l'isolement ». Le professeur Delmas-Marty a écrit à ce propos que « les progrès technologique entrainent (ou rendent visibles) la globalisation des effets résultant de risques (…) d'emblée planétaires. Ici encore, l'autonomie des systèmes nationaux semble affaiblie »[220].

En réalité, la clôture des systèmes pénaux est devenue illusoire à l'heure où l'internationalisation de la criminalité « multiplie les interdépendances »[221]. D'autre part, des divergences de vue entre les Etats sur les valeurs à protéger dans l'univers numérique, opposant les Etats-Unis, le Japon et le Canada à certains pays européens, ont été constatées lors des négociations précédentes l'élaboration de la Convention sur la cybercriminalité. Cette situation a mis en lumière les dangers d'une unification des systèmes répressifs, sorte de « pluralisme de fusion ». Il s'agit au fond d'une unité juridique qui, souvent, dissimule une inquiétante « intégration hégémonique »[222]. Pour sortir de l'impasse et trouver des éléments de réponse à la complexité de la criminalité du cyberespace, il est impossible d'explorer « la voie du pluralisme ordonnée ». Cette option passe par un processus d'intégration juridique entre les systèmes répressifs des Etats. Le processus d'intégration pénale parfaite, utilisée par les systèmes de l'OHADA[223], est symbolisé par la stratégie de l'unification. La voie de l'unification se traduit par une identité normative effaçant les différences entre systèmes.

---

[219] M. DELMAS-MARTY, Les forces imaginantes du droit (II), le pluralisme ordonné, éditions du Seuil, 2006, p. 9.
[220] M. DELMAS-MARTY, op. cit., p. 21.
[221] M. DELMAS-MARTY, « Le pluralisme ordonné et les interactions entre ensembles juridiques », D. 2006, Chron. P. 951.
[222] Sur cette question, M. DELMAS-MARTY, op. cit., p. 17 et s.
[223] Nd. DIOUF, « Actes uniformes et droit pénal des Etats signataires du traité de l'OHADA : la difficile émergence d'un droit pénal communautaire des affaires dans l'espace OHADA » :http://www.ohada.com; du même auteur, « La place du droit pénal dans le droit communautaire », Nouvelles annales africaines, n° 1, 2007, p. 161.

Cette technique d'interaction juridique, sources d'iniquités et « d'impérialisme juridique », ne semble pas adaptée à la stratégie de lutte contre la criminalité de la société de l'information. La cyber-répression internationale exige, pour des raisons d'efficacité, un dialogue entre ensembles normatifs dans le pluralisme. Dans la société de l'information, l'hypothèse réaliste de l'intégration imparfaite[224] par l'harmonisation pénale semble plus propice à un processus d'internationalisation pluraliste privilégiant, non pas la primauté d'un seul système, mais les interactions entre différents ensembles pénaux[225].

La convention sur la cybercriminalité a adopté le système d'intégration qu'est l'harmonisation pour assurer l'internationalisation des ensembles pénaux contre le phénomène contemporain de la cybercriminalité. On peut lire dans son préambule que les Etats membres du Conseil de l'Europe et les autres Etats signataires sont convaincus de la nécessité de mener « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'amélioration de la coopération internationale ». L'élaboration de cette « politique pénale commune » s'est articulée autour de deux grands axes stratégiques propres au processus d'harmonisation. Il s'agit, d'une part, de l'adoption de normes pénales substantielles minimales et, d'autre part, du rapprochement des règles de procédure pénale.

Quoi qu'il en soit, l'harmonisation des systèmes pénaux, qu'implique l'accroissement de la coopération interétatique contre le phénomène de la criminalité des réseaux, présente le mérite de mieux faciliter la coopération internationale entre les instances judiciaires.

2. L'intensification de la coopération judiciaire internationale

Dans le cadre de la lutte contre la criminalité des réseaux, l'accroissement de la coopération entre les Etats (coopération juridique internationale), par l'intégration des systèmes pénaux, n'a d'autre objet que de favoriser des rapports de coopération entre les autorités judiciaires chargées du traitement de la cybercriminalité (coopération judiciaire internationale). En d'autres termes, l'intégration normative internationale doit impulser l'intégration judiciaire internationale. La nature transnationale du phénomène cybercriminel conduit souvent le juge pénal à rechercher des preuves dans un système ou un réseau situé hors de son territoire ou même à solliciter l'accomplissement d'un acte d'instruction à l'étranger. Or, en raison du

[224] S. MANACORDA, « L'intégration pénale indirecte : une première définition », in G. GIUDICELLI-DELAGE et S. MANACORDA (dir.), « L'intégration pénale indirecte », Société de législation comparée, 2205, p. 22.
[225] M. DELMAS-MARTY,

principe de la souveraineté des Etats, l'exercice par la juridiction répressive de ces pouvoirs d'investigation en territoire étranger est subordonné à l'autorisation de l'Etat requis. D'où la nécessité d'une coopération judiciaire entre les Etats. En vertu du principe de coopération posé par l'article 8 de la loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la société de l'information, en liaison avec les organismes d'intégration et dans le respect des engagements internationaux, l'Etat développe et met en œuvre « une politique de coopération judiciaire et sécuritaire orientée vers la sécurité des personnes et des ressources de la société de l'information et de lutte contre la cybercriminalité ».

En matière pénale, la coopération judiciaire internationale, encore appelée « entraide répressive internationale »[226], au sens large, est définie comme « l'exécution par l'Etat requis, au besoin par la coercition, de mesures propres à faciliter la poursuite et la répression des infractions pénales dans l'Etat requérant, à la demande de celui-ci »[227]. Cette coopération est judiciaire en ce qu'elle « est ordonnée pour les besoins d'une procédure pénale ouverte ou terminée »[228]. La collaboration judiciaire entre les Etats peut prendre plusieurs formes : l'extradition, l'entraide proprement dite (commission rogatoires internationales, recherche de preuves, échanges de renseignements, etc…). Malgré l'importance stratégique du renforcement de la coopération judiciaire dans le cadre de la lutte contre le cybercrime, le Projet de Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace n'a prévu aucun mécanisme de coopération judiciaire (modernisation de l'entraide judiciaire, rationalisation de l'extradition, etc.). Cette situation n'est pas de nature à faciliter l'éclosion d'un espace de coopération judiciaire contre la cybercriminalité en Afrique. Tout au plus, l'article III-14 du Projet de Convention de l'Union Africaine a mis à la charge des Etats membres qui ne sont pas liés par une convention d'assistance mutuelle en matière de cybercriminalité l'obligation « d'encourager la signature des conventions d'entraide judiciaire en conformité avec le principe de la double incrimination tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre organisations des Etats membres sur une base bilatérale et multilatérale. » C'est la raison pour laquelle la stratégie de modernisation des techniques de coopération judiciaire en matière de cybercriminalité sera

[226] A. HUET et R. KOERING-JOULIN, Droit pénal international, PUF, coll. Thémis, 2005, p. 329.
[227] R. ZIMMERMANN, La coopération judiciaire internationale en matière pénale, 2e édition, Bruyant, Bruxelles, 2004, p. 5, n° 1 ; V. également, C. GARCIN ET N. MEZZEREB (dir.), L'entraide judiciaire internationale en matière pénale : étude des demandes émises et reçues par la France en 1995, Université Jean Moulin, Lyon 3, Centre de recherche de l'Institut d'études judiciaires, ministère de la justice, 2000 »
[228] R. ZIMMERANN, ibid.

faite à la lumière de la Convention de Budapest qui a jeté les bases d'une véritable politique de modernisation de la coopération judiciaire contre la cybercriminalité.

Pour assurer l'efficacité de l'action judiciaire internationale contre la cybercriminalité a posé dans son article 23 des principes généraux régissant l'entraide répressive internationale. D'abord, il s'agit du principe général de l'intensification de la coopération internationale. En vertu de ce principe, les Etats « coopèrent dans la mesure la plus large possible les unes les autres, aux fins d'investigations ou de procédures » concernant les cyberinfractions. Il s'agit « de réduire autant que faire se peut les obstacles à la circulation rapide et sans problème, au plan international, de l'information et des preuves »[229]. Ensuite, à l'image du dispositif de droit procédural, l'obligation de coopérer a une portée très large. Elle concerne non seulement les infractions pénales liées à des systèmes et données informatiques, mais elle s'applique aussi à la collecte des preuves sous forme électronique de faits se rapportant même à une infraction ayant des liens lointains avec la cybercriminalité. Il en est ainsi d'une escroquerie dont la preuve nécessite la collecte d'indices numériques[230]. Enfin, la convention a posé le principe général selon lequel le dispositif de coopération judiciaire qu'elle prévoit ne se substitue pas aux « instruments internationaux pertinents sur la coopération internationale en matière pénale » applicables dans les Etats parties[231]. Elle ne fait que les renforcer pour les besoins de la lutte contre la cybercriminalité. Il faut noter qu'en droit international pénal, l'entraide répressive se manifeste à toutes les étapes de l'instance pénale internationale, « avant, pendant et après le déroulement du procès pénal »[232].

Les exigences de la répression internationale de la cybercriminalité, ainsi que la nécessité de la création d'un espace judiciaire mondial, ont déterminé les rédacteurs de la Convention sur la cybercriminalité à élaborer une véritable politique criminelle d'aménagement des mécanismes classiques de l'entraide judiciaire internationale. Devant le constat de « l'inévitable dialogue des juges »[233], cette nouvelle option stratégique s'est articulée, d'une part, autour d'une rationalisation du régime de l'extradition judiciaire et, d'autre part, autour d'un mouvement d'intensification du processus de l'entraide judiciaire.

---

[229] Rapport explicatif de la Convention de Budapest, n° 242.
[230] En ce sens, H. BONNARD, « La répression de la cybercriminalité », JCP, éd. E., 12 septembre 2002, Cash. Dr. entr., n° 4, p. 44 : « Selon la convention européenne, l'entraide internationale devrait s'étendre à la lutte contre les infractions qui n'ont d'autre lien avec Internet que de pouvoir être prouvées sous une forme électronique »
[231] Rapport explicatif de la Convention de Budapest, n° 244.
[232] A. HUET et R. KOERING-JOULIN, Droit pénal international, PUF, coll. Thémis, 2005, p. 329.
[233] G. GIUDICELLI-DELAGE, « Les jeux de l'interprétation entre discontinuités et interactions, l'inévitable dialogue des juges », in « Champ pénal », Mélanges en l'honneur du professeur Reynald Ottenhof, 2006, p. 18.

L'extradition constitue un instrument très efficace de collaboration internationale. Le président Laity Kama écrivait déjà en 1970 qu'elle « réalise la forme la plus développée de la solidarité répressive internationale »[234] dans la lutte contre la criminalité internationale. L'extradition est définie comme « le mécanisme juridique par lequel un Etat (Etat requis), sur le territoire duquel se trouve un individu, remet ce dernier à un autre (Etat requérant) afin qu'il le juge (extradition à fin de jugement) ou lui fasse exécuter une peine extradition à fin d'exécution) »[235]. Pour l'Etat requis (Etat qui reçoit la demande d'extradition), on parle d'une extradition passive. Alors que concernant l'Etat requérant, il s'agit d'une extradition active[236]. La technique de l'extradition peut donc intervenir à partir du moment où un individu est recherché par la justice jusqu'au moment où il a exécuté la peine à laquelle il a été condamné. La vieille institution de l'extradition fut conçue comme un simple « acte de courtoisie internationale » entre deux Etats. La conclusion d'un grand nombre de traités bilatéraux et multilatéraux d'extradition entre Etats devait donner naissance à un véritable droit extraditionnel[237]. La mise en œuvre de ce mécanisme est désormais considérée comme l'exécution d'une obligation internationale des Etats signataires[238]. Le droit de l'extradition est caractérisé par la diversité de ses sources normatives constituées des conventions internationales et de normes nationales.

Le Sénégal a conclu dans le cadre de l'Union Africaine et Malgache (UAM) une convention multilatérale d'extradition du 12 septembre 1961[239]. La CEDEAO, dont le Sénégal est membre, a adopté le 06aout 1994 une convention relative à l'extradition en vue de « donner aux juridictions nationales l'instrument permettant l'arrestation, le jugement et l'exécution des sanctions à l'encontre de délinquants qui fuient le territoire d'un Etat membre pour chercher refuge dans le territoire d'un autre ». En droit positif sénégalais, en vertu du caractère supplétif de la loi n° 71-77 du 28 décembre 1971 relative à l'extradition[240], lorsque le Sénégal n'est pas lié à l'Etat requérant par un traité d'extradition ou en cas de silence de l'accord

[234] L. KAMA, « Commentaire de lois, loi n° 71-77 du 22 décembre 1971 relative à l'extradition », Rev. Sén. Dr., mars 1970, p. 113.
[235] A. HUET et R. KOERING-JOULI, ibid.
[236] Sur les différentes formes d'extradition, G. LEVASSEUR et H. BONNARD, « Extradition, notions générales », J-Cl. Dr. inter., art. 689 à 696, fasc. 405-B-2, 3, 1989, p. 5, n° 4.
[237] G. LEVASSEUR, « Les avatars du droit et de la pratique », Rev. fr. dr. adm., 1984, p. 146 ; du même auteur, « Coup d'œil sur l'évolution de l'extradition en droit positif français depuis la 2e Guerre mondiale », Mélange en l'honneur du doyen Bouzat, 1980, édition, Pédone, p. 49 ; dans le même sens, H. SCHULTZ, « Les problèmes actuels de l'extradition », RIDP, 1974, p. 496.
[238] En ce sens, une vieille jurisprudence française, Cass. crim., 3 aout 1888, DP 1889, 1, 173 ; Cass. crim. 15 décembre 1960, Bull. crim., n° 591.
[239] JORS, 12 septembre 1961, p. 900 et s.
[240] JORS, n° 42O7 du 05 février 1972, p. 176.

d'extradition, les modalités de l'extradition sont régies par la loi du 28 décembre 1971. Ce texte constitue donc le droit commun de l'extradition[241]. En tout état de cause, l'extradition, acte d'un gouvernement souverain, en dépit des réformes dont il a fait l'objet, reste profondément marqué par ses liens avec les techniques du droit international public[242]. Ce lien de filiation avec le droit public a eu des incidences sur le fonctionnement du système extraditionnel qui est caractérisé par une lourdeur et un formalisme, « symbole d'une conception de la coopération figée depuis le début du XX^{e} siècle »[243].

Dans la Convention de Budapest sur la cybercriminalité, le besoin d'efficacité dans la coopération répressive a justifié, d'une part, un élargissement du champ des infractions extraditionnelles et, d'autre part, un assouplissement des conditions de l'extradition. Il faut préciser que les traités internationaux constituent la principale source du droit extraditionnel. En raison de ce principe de la primauté des instruments juridiques internationaux de l'extradition sur les sources du droit interne, beaucoup d'Etats subordonnent la mise en œuvre du mécanisme extraditionnel à l'existence de relations conventionnelles avec les Etats requérants[244]. En droit sénégalais, la loi n° 71-77 du 28 décembre 1971 relative à l'extradition s'applique essentiellement à l'extradition passive (le Sénégal : Etat requis), le dispositif décrit par ce texte étant constitué de procédures et de réponse à une demande d'extradition[245].

Cependant, le problème reste entier dans l'hypothèse de l'extradition active, c'est-à-dire lorsque le Sénégal adresse une demande d'extradition à un pays étranger. En effet, tous les Etats ne disposent pas d'un droit commun de l'extradition ayant vocation à s'appliquer en l'absence d'accord d'extradition. Ainsi, en l'absence de convention d'extradition liant le Sénégal à ces Etats, le champ de l'extradition active risque de connaitre des restrictions préjudiciables à la répression internationale de la cybercriminalité. Compte tenu de la nature planétaire du cybercrime, les autorités judiciaires sénégalaises risquent d'achopper sur une décision de refus d'extradition d'un Etat non lié au Sénégal par une convention

[241] A. DIOP, « La coopération interétatique au Sénégal », Rev. Jur. Pol. Ind. Coop., 1983, n° 1, XV° Congrès de l'IDEF, Le Caire, 20-27 novembre 1982, p. 257 ; »La loi n° 71-77 du 28 décembre 1977, qui ne porte pas atteinte aux conventions existantes, crée en somme un droit commun de l'extradition ».

[242] En ce sens, G. LEVASSEUR, « Les avatars du droit et de la pratique de l'extradition », Rev. fr. dr. adm., 1984, p. 145 ; G. LEVASSEUR et H. BONNARD, « Extradition, notions générales », J-Cl. Dr. inter., art. 689 à 696, fasc. 405-B-2, 3, 1989, P ; 7, n° 13.

[243] M. MASSE, « L'entraide judiciaire internationale, version française (loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité) », RSC, 2004, p. 473.

[244] En ce sens, J. BIGAY, « Extrader ou punir », Rev. dr. pén. crim., janv.-fév. 1980, n° 1 et 2, numéro spécial, « Extradition et terrorisme », p. 119.

[245] M. MASSE, « L'entraide judiciaire internationale, version française (suite). Loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité », RSC, 2005, p. 952.

d'extradition[246]. La Convention de Budapest a eu le mérite d'apporter des éléments de réponses à ces difficultés, par l'adoption d'une stratégie d'extradition du champ des cyberinfractions extraditionnelles. Elle a, en effet, prévu une possibilité d'extradition même entre les Etats impliqués par le mécanisme et a aménagé les modalités de l'extradition en cas de signature d'un accord entre ces Etats. Mais si le mécanisme de l'extradition judiciaire constitue l'instrument majeur de la solidarité internationale, il reste que l'amélioration de la lutte contre la criminalité du cyberespace exige une intensification des mécanismes de l'entraide répressive entre les Etats.

L'entraide judiciaire internationale dont il est question ici, est entendue au sens strict. Selon la doctrine, il s'agit de « l'ensemble des moyens par lesquels une autorité étatique, dite autorité requise, prête le concours de sa force publique ou de ses institutions judiciaires à l'instruction, au jugement ou à la répression d'une infraction par une autorité judiciaire, dite requérante »[247]. Ainsi entendu, l'entraide judiciaire transnationale n'est qu'une forme de solidarité répressive internationale, à côté de la technique de l'extradition. Le préambule de la convention de Budapest a rappelé déjà que la lutte contre la criminalité des réseaux « requiert une coopération internationale en matière pénale accrue, rapide et efficace ». Il ne fait pas de doute que de tels objectifs ne sauraient s'accommoder de l'approche traditionnelle du droit de l'entraide judiciaire, source de lenteurs et de lourdeurs procédurales. Aussi, les rédacteurs de la Convention ont-ils pris en compte la fugacité des comportements cybercriminels, pour impulser un mouvement d'accélération du processus de l'entraide judiciaire, tout en veillant à la modernisation de ses techniques.

[246] Il faut préciser que, dans la pratique de l'entraide internationale, même en l'absence d'accords liant les Etats, la courtoisie internationale peut constituer un fondement à l'exécution d'une demande d'entraide.

[247] B. AUBERT, « Ensuite judiciaire (matière pénale) », Rép. Intern., Dalloz, septembre 2002, n° 5 ; également la définition de M. LUISA CASONI et R. ROTH, « L'entraide internationale, moteur de l'évolution du droit pénal ? », in « Politique, police et justice au bord du futur », Mélanges en l'honneur de Lode Van Outrive, Harmattan, 1997, p. 147 ; « L'entraide pénale est ici définie comme l'ensemble des procédures de coopération entre Etats visant à favoriser l'aboutissement d'une poursuite pénale dans l'Etat dit requérant ou à l'exécution d'une sentence pénale, objectifs dont la réalisation nécessite un acte de coopération d'un autre Etat (l'Etat requis) ».

CONCLUSION

Les technologies de l'information et de la communication constituent un fabuleux outil de collecte, de stockage, de traitement et de transmission de l'information dans tous les domaines, qu'il s'agisse du champ structuré du savoir, de la gestion des entreprises, de la médecine, des transports et même des relations personnelles. Elles ont connu ces dernières années un essor tel qu'elles sont devenues, compte tenu de leur diversité et de leur perfectionnement, omniprésentes dans les différentes formes d'activité humaine.

Hélas ! Cette irruption des technologies de l'information et de la communication dans la vie quotidienne des individus engendre également des méfaits, en raison de l'usage qu'en font certaines personnes mal intentionnées pour porter atteinte aux biens d'autrui ou à certaines valeurs essentielles auxquelles notre société est particulièrement attachée à savoir la dignité humaine, l'honneur ou la vie privée. Notre activité réflexive au service de la gouvernance de la répression du numérique aura exigé l'articulation d'un véritable mouvement de politique pénale. Notre étude a permis de confirmer le degré d'ouverture de ce mouvement de modernisation de la politique pénale qui, à la différence des approches classiques, caractérisées par un monopole étatique dans l'organisation des réponses à la criminalité, intègre la participation d'une pluralité d'acteurs dans le cadre d'une véritable démarche de politique criminelle participative. Cette nouvelle approche constitue un aspect de la Co régulation pénale de la cybercriminalité. Elle se déplace en réalité au confluent des options de politique criminelle législative et judiciaire et des enjeux liés à l'implication des instances privées et internationales dans la lutte contre la cybercriminalité. La cyberstratégie de modernisation du droit criminel, impulsée par le mouvement d'expansion du champ de la politique criminelle proposée, présente le mérite de favoriser la gestation d'une nouvelle discipline du droit pénal au Sénégal. Il s'agit d'un cyberdroit pénal protecteur des valeurs cardinales de la société sénégalaise de l'information véritable bras séculier d'une politique criminelle du cyberespace. Il n'est pas question pour nous de théoriser l'autonomie du droit pénal du cyberespace dans l'univers du droit pénal, libre aussi bien dans la conception de ses notions et dans la fixation de ses objectifs. Cette nouvelle discipline pénale ne s'émancipe pas, en réalité, de la philosophie originelle du droit criminel orienté vers la protection des valeurs essentielles de la société.

Le combat contre ce phénomène criminel appelle une multiplicité de réponses et de stratégies adaptées d'ordre sécuritaires, juridiques, politiques, économiques, sociales et culturelles appropriées mais également la mise en place de nouvelles politiques criminelles. Il a été noté,

certes, en Afrique de l'Ouest un nombre important de textes juridiques, de stratégies et d'instruments de coopération pertinents mais ils demeurent insuffisamment appliqués. Le législateur sénégalais en prenant en compte le phénomène du numérique a apporté de grandes innovations dans l'arsenal pénal sénégalais. La loi sur la sur la cybercriminalité a fini par favoriser la gestation d'un véritable cyberdroit pénal au Sénégal, régulateur d'une société sénégalaise de l'information à dimension humaine inclusive ouverte, dérogatoire à bien des égards des principes du droit pénal commun. Mais il faut aussi noter, à un phénomène criminel international, il faut une réponse de politique criminelle également internationale. Ainsi, la nature planétaire de la cybercriminalité exige une mobilisation de la communauté internationale contre ce phénomène qui ignore les balises physiques des frontières étatiques. La mise en œuvre effective de cette volonté politique devrait inscrire le Sénégal dans la croisade internationale contre la criminalité du cyberespace qui constitue une sérieuse menace pour la sécurité des réseaux et le développement de la société de l'information.

Il est évident qu'aujourd'hui, la gestion de la sécurité ne peut plus être réservée exclusivement à l'Etat. La criminalité est devenue un fléau global, il faut une approche globale autrement dit il faut impliquer tous les acteurs de la société. C'est cette conjugaison des forces vives des nations qui pourra améliorer les politiques de prévention et de répression de la criminalité.

BIBLIOGRAPHIE

Ouvrages généraux

ANCEL (M.), La défense sociale nouvelle (Un mouvement de politique criminelle), Paris, Cujas, 1954, 2ème éd. 1966, 2ème éd. 1981.

AUDIT (B.), Droit international privé, Economica, 4° éd., 2006.

ASCENSIO (H.), DECAUX (E.) et PELLET (A.), droit international pénal, 2éme édition, Pédone, 2012.

BOULOC (B.), Procédure Pénale, Dalloz, Paris, 22éme édition, 2010, 1074 pp.

CARBONNIER (J.), Sociologie juridique, 2ème éd., PUF, Paris 2004.

CONTE (Ph.), Droit pénal Spécial, Paris, Litec, 3e édition, 2007, p. 323, n° 555

DELMAS-MARTY (M.), les grands systèmes de politiques criminelles, Thémis Droit Privé, PUF, 1992.

DESPORTES (F.) et **LAZERGES-COUSQUER (L.)**, Procédure pénale, Economica, 2009

MERLE (R.) et **VITU (A.)**, Traité de droit criminel, problème généraux de la science criminelle, droit pénal général, Tome I, CUJAS, PARIS, 6° éd. 1988, n° 277, p. 372.

PRADEL (J.), Droit Pénal général, Cujas, Paris, 18e édition, 2010.

PRADEL (J.), Procédure pénale, 15ème éd., Cujas, 2010, p. 369.

RASSAT (M.L.), Droit pénal spécial, 6e édition, Dalloz, 2011, p. 635, n° 828.

Ouvrages spécialisés

JABER (A), Les infractions commises sur Internet, Harmattan octobre 2009, p. 311.

MACREZ (F.), Créations informatiques : bouleversement des droits de propriété intellectuelle. Essai sur la cohérence des droits, Paris, Litec, 2011, p. 20, n° 7.

PARKER (D.-B), Combattre la criminalité informatique, Economica, OROS, Paris, 1985.

TOURE (P.A.), Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal Harmattan 2014, p. 616.

Articles, études et documents

AGHROUM (Ch.) et **RITZ (J-Ph),** « La lutte contre la cybercriminalité », in « Techniques d'enquêtes dans l'environnement électronique », Séminaire ADIE, Dakar, 8-9 septembre 2008.

AMMAR (D.), « Preuve et vraisemblance. Contribution à l'étude de la preuve technologique », RTD civ, juillet-septembre, 1993, p. 449.

ARRIGO (P.), « La cybercriminalité : vers une régulation internationale de l'Internet ? », Gaz. Pal. 14 au 16 octobre 2001.

BEAUSSONIE (G.), « La protection pénale de la propriété sur l'information », Dr. pén., n° 9, septembre 2008, études, p. 32-33.

BELLOIR (Ph.), « L'application des règles de procédure pénale aux infractions commises sur Internet, (2e partie) », Expertises, juillet 2002, p. 256.

BELLOIR (Ph.), « Perquisition et saisie en matière de lutte contre la cybercriminalité », RLDI, n° 60, mai 2010, 1995, p. 71.

BOURE (Ph.), « Internet et la lutte contre la cybercriminalité », Gaz. Pal. 22-23 janvier 2003, p. 62.

BOUZAT (P.), « Vol de disquette et du contenu informationnel de certaines d'entre elles », RSC, avril-juin, 1990, p. 346.

CAMARA (I..), Le statut juridique de la contrefaçon des phonogrammes et œuvres littéraires et artistiques du Sénégal, Dakar, EDJA, mars, p. 10.

CAPELLER (W.), « Un net pas très net », in « L'immatériel et le droit », Arch. Phil. Dr, n° 143, p.

CATALA (P.), « Ebauche d'une théorie juridique de l'informatique », D. 1984, Chron. p. 97.

CELIS (J. C de), « La politique criminelle à la recherche d'elle-même », in archives de politique criminelle, n° 2, pédone, 1997, p. 3.

CIOLINO-BERG (D.), « Vol d'information sur Internet », Comm. com. Novembre 2003, p.22.

CISSE (A.), « Cybersécurité : les moyens juridiques de protection », in « Bâtir un espace numérique de confiance en Afrique », *Conférence régionale africaine sur la cybersécurité, Yamoussoukro, du 17 au 20 novembre 2008.*

CISSE (A.), « Cybersécurité et cybercriminalité : cohérence terminologique et harmonisation des cyberlégislations africaines », « Réunion ad hoc d'experts sur un cadre légal harmonisé des TIC en Afrique centrale », Libreville (Gabon), du 28 novembre au 2 décembre 2011.

CISSE (A.), « Droit sénégalais », in A. CASSESE et M. DELAMAS-MARTY, « Juridictions nationales et crimes internationaux », P.U.F, Paris, 2002, p. 439.

CISSE (A.), « Quel cadre juridique pour le Sénégal ? Éléments de synthèse », Séminaire « Informatique et libertés, quel cadre juridique pour le Sénégal ? » A.D.I.E, Dakar 29 et 30 août 2005.

CISSE (A.), La réflexion sur les éléments constitutifs et avant projets de lois sur la société de l'information, Rapport Général, Séminaire « Informatique et libertés, quel cadre juridique pour le Sénégal ?», Dakar, 29 et 30 août 2005, p. 207.

DELMAS-MARTY (M.), Modèles et mouvements de politique criminelle, Paris, Economica, 1983.

DIALLO (M. Y.), « Le contrôle de proportionnalité dans la jurisprudence constitutionnelle en Afrique », Annales Africaine, nouvelle série, vol. 2, n° 7, décembre 2017, p. 255 et s.

DIOP (M. C) (dir.), Le Sénégal à l'heure de l'information, technologies et société, Edition Karthala, Paris, 2002.

DESBOIS (H.), Le droit d'auteur, Dalloz, 1ère édition, 1950, n° 50 et s.

DEVEZE (J.), « A propos de l'évolution des délits contre les biens », in « Libre droit », Mélanges en l'honneur de Philippe LE TOURNEAU, Dalloz, 2006, p. 359.

DEVEZE (J.), « Le vol des biens informatiques », JCP. 1985, I, 3210, n° 5.

DEVEZE (J.), « Les qualifications pénales applicables aux fraudes informatiques », in VIIIe Congrès AFDP, « Le droit criminel face aux technologies modernes de la communication », Paris, Economica et ADI, 1986, p. 197.

DESJEUX (X.), « Logiciel, originalité et activité créative dans la loi du 3 juillet 1985 », Expertise, p. 32.

DIOUF (Nd.), « Infractions en relation avec les nouvelles technologies de l'information et procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale », Rev. Sen.dr.aff., n° 2, 3,4, 2003-2004, p.63

DIOUF (Nd.), « La procédure pénale à l'épreuve des nouvelles technologies de l'information», Rev. Ass. Sén. dr. pén, n° 5, 6,7 et 8, 1997-1998, p.13.

DJOMGA (Ch. D.), La contrefaçon des logiciels dans l'espace OAPI. Etude comparée de l'accord révisé et des législations du Sénégal, du Gabon, de la Cote d'Ivoire et du Cameroun, Editions ISIS, Yaoundé, octobre 2011, p. 18 et s.

FALL (Nd.), Le droit pénal africain à travers le système sénégalais, E.D.J.A, 2003.

FALL (Nd.), « L'abus de confiance en droit sénégalais », La Balance, Journal de l'Union des Magistrats sénégalais, août 2002, p. 12.

FAYE (A.), « Le suspect dans les enquêtes de police », Rev.Ass.sén.dr.pén., année 2010, n° 9, p. 19.

FRANCON (A.), « Les sanctions pénales de la violation du droit moral », in mélanges Brust, Litec, 1997, p. 171.

GAVIN (G.), « Vers une sanction pénale du droit moral », RIDA avril 1961, p. 171.

GUEYE (A. L.), « Quelques aspects de la preuve en droit sénégalais », in « La preuve devant le juge », XVII° Congrès de l'I.D.E.F, Bruxelles 31 septembre 06 octobre 1984, Rev.jur.pol.ind.coop, 1985, n°1, p. 236 et s.

HOUIN (R.), « Le progrès de la science et le droit de la preuve », in Revue internationale de droit comparé, vol. 5 n° 1, Janvier-mars 1953. Pp. 69-75.

HUET (A.), « Le droit pénal international et Internet », P.A, 10 novembre 1999, p. 39.

JACOPIN (S.), « Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse », Dr. pén, avril 2001.

LATREILLE (A.), « Logiciel, objets de propriétés », RLDI, n° 49, mai 2009, p. 38.

LAZERGES (Ch.), Introduction à la politique criminelle, harmattan, 2000 p.7.

LAZERGES (Ch.), « La défense sociale nouvelle a 50 ans. L'actualité de la pensée de Marc ANCEL », RSC 2005, pp 165 et s.

LEVASSEUR (G.), « La politique criminelle d'elle-même », in archives de politique criminelle, n° 2, pédone, 1997, p. 3.

LUCAS (A.), **DEVEZE (J.)** et **FRAYSSINET (J.)**, Le droit de l'Informatique et de l'Internet, P.U.F, 2001.

LUCAS (A.), « Les programmes d'ordinateurs comme objets de droits intellectuels », JCP, éd. G. I, n° 3081.

LUCAS DE LEYSSAC (M. P.), « Une information seule est-elle seule susceptible de vol ou d'une autre atteinte juridique aux biens », D. 1985. Chron. P. 51, n° 48 et 49.

MACREZ (F.), « Logiciels : le cumulard de la propriété intellectuelle » in J.-M. BRUGUIERE (dir), L'articulation des droits de propriété intellectuelle, Paris, Dalloz, 2011, p. 45.

NDIAW (D.), Les infractions en relation avec les nouvelles technologies de l'information et procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale », Rev. Sen.dr.aff., n°2, 3, 4, 2003-2004, p. 63.

NZOUABETH (D.), « La tolérance en matière pénale au Sénégal », Annales africaines, Nouvelle série, vol. 2, Décembre 2017, n° 7, CREDILLA, p. 161.

OUATTARRA (A.), La preuve électronique. Etude de droit comparé. Afrique, Europe, PUAM, 2011.

PRADEL (J.), « Les infractions relatives à l'informatique », Rev. Inter. Dr. comp., 1990 n°2, p. 815.

PRADEL (J.), « Les infractions de terrorisme, un nouvel exemple de l'éclatement du droit pénal (loi n° 86-1020 du 20 septembre 1986) », D. 1987., p. 39.

PRADEL (J.) et FEUILLARD (C.), « Les infractions commises au moyen de l'ordinateur », Rev. dr. pén. et crim, 1985, p. 317.

QUEMENER (M.), « Réponses pénales face à la cyberpornographie », Act.Jur.pén, mars 2009, p. 107.

QUEMENER (M.) et FERRY (J.), Cybercriminalité. Défi mondial, 2e édition, Economica, 2009.

SAKHO (A.), « la protection de la propriété intellectuelle et l'Afrique ADPIC-Bangui 1999 », Africajuris, n° 40 du 07 au 13 novembre 2002, p. 8.

SAUREL (P.) et **OYHAMBERRY (A.),** « Ce que la cyber justice nous apprend de la justice des signes distinctifs » in gazette du palais, 18-19 juin 2010.

SCHUHL (C.), Cyberdroit, le droit à l'épreuve de l'Internet, Dalloz, 4e édition, 2008.

TOURE (P.A.), « Cyber stratégie de répression de la cybercriminalité au Sénégal », in « Les techniques d'enquêtes dans l'environnement électronique », séminaire Dakar, 8 et 9 septembre 2008, p. 5.

TOURE (P.A.), « Cinq ans de droit pénal de technologies de l'information et de la communication (2008-2013) : chronique de jurisprudence sénégalaise », bull. inf. cour sup., n° 7-8, décembre 2015.

TOURE (P.A.), « La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité », in Conférence sur la coopération contre la cybercriminalité organisée par le Conseil de l'Europe, 23 au 25 mars 2010 à Strasbourg : http://www.coe.int.

TRUCHE (P.), La pénalisation à l'épreuve du temps, des décisions judiciaires et politiques, Paris, le seuil, pouvoirs, 2009/1-n° 128, p. 121 et s.

VERON (M.), Droit pénal spécial, Paris, Sirey, 11e éd. Juin 2006, p. 293.

VIVANT (M.), et **J.-M. BRUGUIERE**, Droit d'auteur, 1ère éd., Dalloz, 2009, p. 178.

VIVANT (M.), « L'investissement, rien que l'investissement. A propos des arrêts de la cour de justice du 9 novembre 2004 », RLDI, 2005, 3. p. 41 et s.

WAFO (D.), « La protection par le droit d'auteur du logiciel en Afrique noire : le pénible éveil », Penant, n° 818, mai à septembre 1995, p. 156 et s.

Mémoires

KABORE (A.), La problématique des perquisitions et saisies en ligne en Afrique de l'Ouest : état des lieux et perspectives. Cas du Burkina Faso, du Mali, du Sénégal et du Togo, Mémoire, Master, « Droit du cyberespace africain », Saint-Louis, 2006-2007.

THEVENET (C.), Cyberterrorisme, mythe ou réalité ?, mémoire, Marne-La-Vallée, 2005.

TOURE (P.A.), Le traitement de la cybercriminalité devant le juge Sénégalais, mémoire DEA, Saint-Louis, 2005.

Thèses

AUPECLE-GUECHENEY (N.), Les infractions pénales favorisées par l'informatique, thèse, Montpellier, 1984.

BEAUSSONE (G.), La prise en compte de la dématérialisation des biens par le droit pénal : contribution à l'étude de la protection pénale de la propriété, Thèse Toulouse I, 2009.

CASILE (J.-F), Le code pénal à l'épreuve de la délinquance informatique, Thèse, Aix-Marseille, 2002.

CHAWKRI (M.), Le droit pénal à l'épreuve de la cybercriminalité. Etude comparative de la politique criminelle face aux NTIC, thèse Lyon III, 2006.

CHEHADE (F. EL. H.), Les actes d'investigation, Thèse de doctorat, Université du Maine, 2010.

DIOUF (Nd.), La situation des parties au procès pénal pendant l'instruction préparatoire, Thèse Paris 1 (Sorbonne), 1992.

EL CHAER (N.), La criminalité informatique devant la justice pénale, Thèse Poitiers, 2003.

GUEYE (P.), Les politiques criminelles à l'épreuve de l'évolution de la criminalité transfrontalière organisée en Afrique de l'Ouest, thèse, Dakar, 2016.

KONATE (M.), Le temps et le procès pénal au Sénégal, Thèse de doctorat, Université Cheikh Anta Diop de Dakar, 2017, pp. 95 et s.

MALONGA YOUNASS (J.P.), La répression des agissements liés aux nouvelles technologies de l'information : L'exemple du Congo, thèse, Dakar, 2003.

MIGNARD (J.P.), Cybercriminalité et cyberépression, entre désordre et harmonisation mondiale, thèse, Paris I, 2004.

TOURE (P. A.), Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal, Thèse Doctorat, Saint-Louis (Sénégal), 2010.

LEGISLATIONS

-Traité relatif à l'harmonisation en Afrique du droit des affaires (JO OHADA n° 4 du 1er novembre 1997, p. 1).

- Acte uniforme de l'OHADA relatif aux contrats de transport de marchandises par route du 22 mars 2003 (JO OHADA, n° 13, 31 juillet 2003, p. 3 et s.).

-Acte additionnel A/SA du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des technologies de l'information et de la communication (TIC).

-Acte additionnel du 2 octobre 2009 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.

-Accord du 24 février 1999 portant révision de l'Accord de Bangui du 02 mars 1977 instituant une Organisation africaine de la propriété intellectuelle relatif à la propriété littéraire et artistique (OAPI).

- Directive C/DIR/1/08111 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

- Directive n° 07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communication électronique au sein de la CEMAC.

- Constitution du 7 janvier 2001 (JORS, n° 5963 du 22 janvier 2001).

-Loi uniforme n° 2008-48 du 3 septembre 2008, relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement (JORS, n° 6453, du 7 février 2009, p. 120).

- Loi n° 65-61 du 21 juillet 1965, portant Code de procédure pénale (JORS, n° 3777 du 25 aout 1965, p. 1265 et s.).

- Loi n° 65-60 du 21 juillet 1965 portant Code pénal (JORS, n° 3767 du 6 septembre 1965, p. 1009 et s.).

-Loi n° 71-77 du 22 décembre 1971, relative à l'extradition (JORS, n° 4207 du 05 février 1972, p. 176).

-Loi n° 73-52 du 04 décembre 1973 relative à la protection du droit d'auteur (JORS, n° 4333 du 29 décembre 1973, p. 2270).

-Loi n° 90-06 du 26 juin 1990 portant réglementation bancaire (JORS, n° 5361 du 28 juillet 1990, p. 361 et s.).

-Loi n° 2001-15 du 27 décembre 2001 portant Code des télécommunications (JORS, n° 6030, du 16 février 2002, p. 868 et s.).

-Loi n° 2007-04 du 12 février 2007, modifiant le Code de procédure pénale relative à la lutte contre les actes de terrorisme (JORS, n° 6332 du 10 mars 2007, p. 2375).

- Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques (JORS, n° 6404 du 26 avril 2008, p. 395).

- Loi n°2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information (JORS, 6406 du 03 mai 2008, p. 419 et s.).

-Loi n°2008-11 du 25 janvier 2008, portant sur la cybercriminalité (JORS, n° 6406, du 3 mai 2008, p. 419) (annexe n° 1).

-Loi n° 2008-12 du 25 janvier, sur la protection des données à caractère personnel (JORS, n° 6406, du 3 mai 2008, p. 434).

-Loi n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement, JORS n° 6984 du samedi 07 janvier 2017.

-Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 1965 portant Code pénal, JORS n° 6975 du vendredi 25 novembre 2016, pp. 1614 et s.

Décret n° 65-557 du 21 juillet 1965 portant Code des contraventions (JORS du 23 aout 1975, p. 954 et s.).

CHRONIQUES, NOTES ET OBSERVATIONS DE JURISPRUDENCE

CS Ch. crim. (Sénégal), n° 65 du 17 décembre 1986, Raoul Richa c/MP, arrêt inédit.

CS Ch. crim. (Sénégal), n° 39 du 30 avril 1980, Saliou I. Ndiaye c/MP, arrêt inédit.

CS Ch. crim. (Sénégal), n° 78 du 1er avril 2010, affaire Robert Tabet, inédit.

CA Dakar, n° 680 du 16 avril 2007, affaire de la Clinique du Cap, inédit.

CA Dakar, Ch. Corr, n°307 du 17 avril 2009, affaire du navire Lobella.

CA Dakar, n° 978 du 13 décembre 2010, affaire Fulgence BAHI, inédit.

CA Dakar, n° 365 du 25 mars 2011, affaire PALUCCI, inédit.

TH Thiès n° 1603, 23 décembre 2005, affaire « Mor Todjangué », inédit.

TRHC Dakar, n° 1981 du 9 mai 2006, affaire de la Clinique du Cap, inédit.

TRHC Dakar, n° 5310 du 21 novembre 2006, affaire Madiambal Diagne, inédit.

TRHC Dakar, du 19 juillet 2007, affaire « Résidence Saint James », inédit.

TRHC Dakar, n° 179 du 1er avril 2008, affaire Robet Tabet, inédit.

TRHC Dakar, n° 4241 du 18 septembre 2009, affaire Pneuméca, inédit.

TR Thiès, n° 269 du 26 avril 2010, affaire SENELEC c/SEPAM, inédit.

TRHC Dakar, n° 1087 du 22 mars 2011, affaire América David, inédit.

TRHC Dakar, du 17 avril 2012, affaire du système Wari, inédit.

TRHC Dakar, n° 1780 du 2 mai 2012, affaire Kouakou Kouadio, inédit.

TRHC Dakar, 4e ch. n° 385 du 21 juin 2012, affaire de la société Kajas, inédit.

TR Thiès, n° 505/2012 du 18 septembre 2012, affaire de l'Agence New-Look Business, inédit.

TR Saint-Louis, n° 141 du 28 février 2013, affaire du système Wari Saint-Louis, inédit.

TRHC Dakar, n° 458 du 04 juin 2013, affaire Leral.net, inédit.

WEBOGRAPHIE

Bulletins sur la criminalité technologique, http//.www.remp.grc.gr.ca

CHAMBET (Patrick), Le cyber-terrorisme, http://www.chambet.com.

CHAWKRI (M.), « Le vol d'information : quel cadre juridique aujourd'hui ? » :http://www.droit-tic.com/pdf/volinformation.pdf

CISSE (A.), Gouvernance internationale d'Internet : normes et Institutions Diplomacy and cyberespace - Seminar, Rome, vendredi 4 juillet 2003. www.unpan.1.un Cybercrime : http//wwwcybercrimes.net

CISSE (A.), Introduction au droit du cyberespace, Cours Master « Droit du cyberespace africain » http ://www.saintlouis.u-strasbg.fr

COLY (A. J.), « Protection internationale des logiciels informatiques : la législation sénégalaise à la traine » http://www.osiris.sn/article905.html.

DIOUF (Nd.), Procédure pénale et technologie de l'information et de la communication (TIC), Cours, Master, « Droit du cyberespace africain », Saint-Louis, 2006-2007 : www. saintlouis.u-strasbg.fr

GUISSE (Ch. Mb.), « Sabotage et destruction du site Nettali.com : Le parquet aux trousses d'un cheval de Troie » : http://www.osiris.sn/article3464.htlm

LO (M.), « La lutte contre la cybercriminalité : les premières décisions de la justice sénégalaise » : http://www.pressafrik.com/La-lutte-contre-la-cybercriminalité-lespremières-décisions-de-la-justice-sénégalaise_a40664.html

SARR (L.P.), « La cybercriminalité en droit sénégalais à l'épreuve de l'anonymat dans le cyberespace » : http://www.droit-technologie.org

TOURE (P.A.), « La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité », in Conférence sur la coopération contre la cybercriminalité organisée par le Conseil de l'Europe, 23 au 25 mars 2010 à Strasbourg : http://www.coe.int

VERBIEST (Th.), Criminalité informatique, comment la réprimer ? www.club.internet.fr;

TABLE DES MATIERES