2006/211

République du Sénégal

Un Peuple-Un But-Une Foi

Ministère de la Justice

Centre de Formation Judiciaire

(Section Magistrature)

MEMOIRE DE FIN DE FORMATION

THEME :

Le droit pénal sénégalais et la lutte contre la cybercriminalité

Présenté par :

Ndèye Ami KAMARA
Auditrice de Justice/CFJ

Sous la Direction de :

M. Jean Aloise NDIAYE
Magistrat, Auditeur à la Cour Suprême

Année académique 2007-2009

Dédicaces

Je dédie ce mémoire :

A mon défunt père,

Massamba KAMARA.

A mon grand frère,

Djibril KAMARA.

Que Dieu les accueille en son Paradis.

Remerciements

Je remercie :

- Ma mère **Adja Marème Soda DIOP** pour son amour, sa bonté, pour tous les sacrifices qu'elle fait et fera pour ses enfants. Que Dieu lui prête longue vie.

- Mon encadreur Monsieur **Jean Aloise NDIAYE** Magistrat, Auditeur à la Cour Suprême pour sa collaboration, sa rigueur et sa disponibilité qui ont contribué à la réalisation de ce mémoire.

- A mes frères et sœurs et toute la famille KAMARA.

- A mon père Abdoul Aziz KAMARA, ma grand-mère Aminata SENGHOR, Maodo SAMB, Ndeye Fatou KAMARA, Tata Soda NDIAYE, Tata Anna Semou FAYE, Khady Kamara, Khoudia MBENGUE, Nafi MANDIAN, Bébé SOKHNA, Fatou THIAM née Mme WADE.

- A tous mes amis : Samba DIOUF, Marianne Ndiaye, Faty Diadji SECK, Fatou CISSE, Mareme GUEYE, Farma FAYE, Rokhayatou DIONE, Ndeye Khansou CAMARA, Amary NDOUR, Diabel NDIR, Pape Diamane DIOUF, Alibo MANGA, Ndeye Fatou DIOUF, Nabou SECK , Awa TAMBEDOU, Rawane DIOP, guorgui ndiaye, Mame Fatou LEYE, Tony DIEYE.

- L'ensemble du personnel du Centre de Formation Judiciaire et tous ceux qui, de près ou de loin, ont participé à la réussite de ce mémoire.

SOMMAIRE

INTRODUCTION

Les rapides progrès des techniques de l'information et de la communication (TIC) marquent un tournant majeur de la civilisation humaine. Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information notamment l'internet grâce auquel toute personne peut avoir accès à la totalité des services d'information électronique, ou qu'elle se trouve sur la planète.

L'espace informationnel vient désormais s'ajouter à l'espace terrestre, maritime et aérien dont la protection et la sécurité entrent naturellement dans le champ des compétences régaliennes de l'Etat. Espace virtuel par sa structure et la nature même des informations qu'il véhicule, le cyberespace a des incidences sur la vie quotidienne notamment en ce qui concerne l'espace l'accès à la connaissance, les communications entre les personnes, le commerce , l'exercice de la citoyenneté (le vote électronique), l'administration (e-gouvernement)[1] et le travail en ligne (e-travail).

Cependant les grandes découvertes technologiques ont engendre presque toujours, à coté des progrès économiques qu'elles procurent à l'humanité, des retombés négatives parmi lesquelles figure en bonne place la criminalité. La révolution numérique plus particulièrement internet est de plus en plus le lieu virtuel de commission d'agissement, de comportements répréhensibles de toutes sortes, attentatoires tant aux intérêts des particuliers qu'à ceux de la chose publique.

Cette nouvelle forme de délinquance appelée « cybercriminalité » constitue une sérieuse menace pour la sécurité des réseaux et le développement de la société de l'information.

Le terme cybercriminalité demeure difficile à conceptualiser, car il n'est l'objet d'aucune définition légale. Les experts de l'Organisation pour la Coopération et le Développement Economique (OCDE) définissent la cybercriminalité comme « tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement

[1] www.jo.gouv.sn

automatique de données et/ou de transmissions de données ». Selon l'Organisation des Nations Unies (ONU), la cybercriminalité doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », et dans une acception plus large « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».

Le Xe Congrès des Nations Unies sur le crime et le traitement des délinquants, a défini la cybercriminalité comme "toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique. Il englobe, en principe toute infraction susceptible d'être commise dans un environnement électronique.

Ce nouveau phénomène criminel peut être défini comme l'ensemble des comportements infractionnels liés à l'utilisation des technologies de l'information et de la communication c'est-à-dire l'ensemble des infractions directement liées aux technologies de l'information et de la communication ou celles dont la commission a été facilitée ou liée à l'utilisation de ces technologies.

L'irruption de ce nouveau phénomène appelé cybercriminalité a contribué à brouiller les repères du système pénal dont les réponses traditionnels et permanentes, conçues et élaborées pour un environnement matériel et national, se sont vite révélées inappropriés et inadaptées pour saisir cette nouvelle réalité de l'ère numérique.

Ainsi , l'examen de la législation pénale sénégalaise a permis de constater son inadaptation par rapport aux spécificités de la délinquance numérique aussi bien en droit substantiel qu'en droit procédural .

Face aux profondes mutations du 3eme millénaire, au développement vertigineux des TIC , à la convergence et à la mondialisation croissante des réseaux informatiques ,le Sénégal a compris très tôt que le rôle primordial de tout Etat de droit à l'ère numérique est de participer en temps réel et avant qu'il ne soit trop tard , tant au plan interne qu'au plan international à la mise en place d'un arsenal juridique . L'élaboration de nouvelles dispositions législatives et réglementaires spécialement adaptées au cyberespace assurera non seulement la protection des intérêts nationaux mais encore et surtout la sécurité que tous les

citoyens sont légitimement en droit d'attendre en cas de crimes et délits commis à l'aide des réseaux informatiques.

Si la communication en ligne des informations, idées et données est libre, il n'en demeure pas moins qu'elle ne devrait s'exercer que sous réserve du respect de la dignité de la personne humaine, de l'intimité de l'usager, de la liberté individuelle et de la propriété d'autrui, du pluralisme de l'expression et des autres droits humains.

La confidentialité, l'intégrité et la disponibilité des systèmes doivent être prises en considération de façon permanente et non négligeable, de même que les réseaux et données informatiques, la sauvegarde de l'ordre publique, de la sécurité intérieure et de la défense nationale.

Les agissements frauduleux par et à l'intérieur des systèmes, réseaux et données informatiques justifient le cyber stratégie de lutte sans merci envisagée au Sénégal contre de tels comportements aux conséquences néfastes incalculables réalisées en un temps record.

A cet effet, l'encadrement du développement des TIC au Sénégal a été la création de l'Agence Informatique de l'Etat (ADIE). Le décret n° 2004-1038 du 23 juillet 2004 lui donne compétence d'impulser l'action publique en matière de traitement et de diffusion de l'information en conformité avec les normes juridiques et techniques internationales en matière de qualité, de disponibilité, de sécurité et de performance.

C'est ainsi que sur le plan national et international à travers un cadre législatif et réglementaire des mesures relatives à la rapide détection , à l'investigation , a la poursuite , à la collecte des preuves électroniques , à la surveillance des télécommunications et des correspondances , à la piraterie , à l'accès sans droits aux systèmes informatiques , à l'interruption illégale , à la détérioration , la suppression et falsification des données , à la perquisition , la saisie, collecte et interception des données , à la compétence juridictionnelle , à l'extradition et à l'entraide judiciaire ont été envisagées et retenues en vue de leur incorporation dans le corpus juridique sénégalais.

Il faut souligner le réalisme et le cyber protectionnisme initié par l'ADIE dont il faut saluer le travail de titan effectué après un cyber audit stratégique de l'environnement juridique ayant aboutit a une loi d'orientation sur la société de l'information , une loi sur les

transactions électroniques , une loi sur les données caractère personnel et la présente loi sur la cybercriminalité , une loi sur la cryptologie et a des décrets d'application .

L'inauguration récente de l'Intranet gouvernemental le 15 mars 2005, a fini de convaincre sur les progrès considérables réalisés par le Sénégal dans le secteur des technologies numériques, le plaçant ainsi au cœur de la société de l'information.

La loi N°2008-11 du 25 janvier 2008 portant sur la cybercriminalité a permis l'adoption de nouvelles infractions spécifiques au TIC assorties des sanctions adéquates et l'aménagement de la procédure pénale classique, par rapport aux TIC, permettront à coup sur non seulement un habillage juridique sécurisant, comblant les zones de non droit, mais encore et surtout une parade contre les cyber malveillants qui n'ont pas besoin de visa pour évoluer dans le cyberespace

Une économie nouvelle fondée sur des échanges supranationaux immédiats voit le jour et à coté des usages légitimes des nouvelles technologies se développement inévitablement des abus. Le droit pénal peut suivre le rythme de ces évolutions techniques qui offrent des moyens extrêmement perfectionnés d'employer a mauvais escient les services du cyberespace , de porter atteinte a des intérêts légitimes et donc circonscrire les déviances liées au détournement criminel de l'utilisation des nouvelles technologies. En cela réside l'intérêt d'un tel sujet.

Le droit pénal sénégalais permet-il une prise en charge de la lutte contre la cybercriminalité ? En d'autres termes, les agissements cybercriminels sont elles effectivement réprimées par le droit pénal sénégalais ?

En l'état actuel du droit sénégalais, il faut se féliciter que presque tous les comportements ressortissant de la cybercriminalité sont insérés dans les textes répressifs de droit positif. La démarche stratégique de traitement de la cybercriminalité devant le juge a consisté à apporter la réponse de politique pénale la plus appropriée et la plus adaptée à ce phénomène cybercriminel.

Ce qui justifie ainsi d'une part, l'élaboration d'une stratégie méthodique de modernisation des incriminations de l'arsenal juridique et l'amélioration de la procédure de répression de la cybercriminalité devant l'autorité judiciaire sénégalaise .

D'autre part, la participation méthodique du législateur sénégalais s'est confrontée à de nombreuses difficultés qui rendent pénible cette lutte contre la cybercriminalité mais n'empêche que certaines solutions peuvent être apporté tant au plan communautaire qu'international en vue d'assurer une politique de répression tangible.

En conséquence, notre activité réflexive nous amènera à analyser d'une part, l'existence d'un cadre juridique normalisé dans la lutte contre la cybercriminalité (chapitre I) avant d'étudier d'autre part, la mise en œuvre pratique de la lutte contre la cybercriminalité (chapitre II).

CHAPITRE I : L'EXISTENCE D'UN CADRE JURIDIQUE NORMALISE DANS LA LUTTE CONTRE LA CYBERCRIMINALITE AU SENEGAL

Les technologies numériques (Internet en particulier) sont utilisées comme instruments de commission d'actes infractionnels. La législation pénale sénégalaise a vite révélé des insuffisances et une désuétude exigeant un réaménagement du droit pénal substantiel et procédural des technologies de l'information et de la communication (TIC).

L'inadaptation de la législation pénale sénégalaise face à l'apparition de nouveaux comportements d'écart aux normes suscitées par l'essor des TIC a permis l'actualisation de la politique criminelle qui s'est manifestée par la modernisation des instruments de répression de la cybercriminalité (section I) et l'amélioration de la procédure de répression de la cybercriminalité (section II).

SECTION I : LA MODERNISATION DES INSTRUMENTS DE REPRESSION DE LA CYBERCRIMINALITE

Un droit pénal spécifique dérogatoire aux principes du droit pénal commun et qui a pour but l'adaptation des mécanismes du droit pénal de fond aux particularismes de la cybercriminalité a abouti à une loi[2] sur la cybercriminalité qui a mis l'accent sur l'adoption d'un nouveau dispositif répressif spécifique aux TIC (paragraphe I) et l'adaptation des incriminations traditionnelles aux TIC (paragraphe II).

Paragraphe I : L'adoption d'un nouveau dispositif répressif spécifique aux TIC

Le droit pénal substantiel consacré par la loi sur la cybercriminalité est caractérisé par l'adoption de nouvelles incriminations spécifiques à la cybercriminalité (A) et la création de nouvelles sanctions pénales adaptées à la cybercriminalité (B).

A- L'adoption de nouvelles incriminations spécifiques à la cybercriminalité

Dans le cadre de la lutte contre la cybercriminalité, le législateur sénégalais s'est doté d'une législation spécifique aux TIC qui s'articule autour des infractions portant atteintes aux systèmes et données informatiques et les infractions informatiques (1), celles portant atteintes aux personnes (2), celles liées aux activités des prestataires techniques de services de communication au public par voie électronique (3) et les infractions liées au commerce électronique et a la publicité par voie électronique (4).

---

[2] Loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité, voir recueil du droit sénégalais de la société de l'information .

1. Les infractions portant atteintes aux systèmes et données informatiques et les infractions informatiques

a. Les infractions portant atteintes aux systèmes informatiques

Dans le cadre de la lutte contre la cybercriminalité, le législateur a posé comme condition préalable l'existence d'un système informatique qu'il définie comme « tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme [3] ».

La protection pénale des systèmes informatiques peut-être garantie en politique criminelle sénégalaise par la pénalisation des atteintes à la confidentialité, à l'intégrité et a la disponibilité des systèmes informatiques.

Les atteintes à la confidentialité des systèmes informatiques sont prévues par les articles 431-8 et 431-9 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

L'article 431-8 de la loi dispose que « Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique ... » et « est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.».La sanction s'applique a celui qui aura accéder frauduleux à un système informatique.

La constitution matérielle de l'infraction est alternative, puisqu'elle peut être constituée par deux actes différents qui sont respectivement : la pénétration dans un système contre le gré du maître du système, en forçant ou en contournant le dispositif de sécurité et la procuration d'un avantage quelconque pour soi même ou pour autrui.

L'article 431-9 de la loi sanctionne « Quiconque se sera maintenu ou aura tenté de se maintenir frauduleusement dans tout ou partie d'un système informatique».Cet article sanctionne le fait pour un individu non habilité, d'avoir accédé par hasard ou par erreur à un système, ou bénéficiant d'une autorisation de connexion limitée dans le temps, qui reste dans le système au lieu d'interrompre la connexion.

Les atteintes à l'intégrité des systèmes informatiques sont prévues par l'article 431-10 de la loi susvisée qui dispose qu'« encoure une sanction pénale quiconque aura entravé ou faussé ou aura tenté d'entraver ou de fausser le fonctionnement d'un système informatique». Il sanctionne d'une part, l'entrave au fonctionnement du système c'est-à-dire les comportements réalisés au moyen d'actions positives, ayant pour résultat d'empêcher l'aboutissement du traitement informatique. Exemple infections informatiques[4] (virus informatiques, vers informatiques, bombes logiques, chevaux de Troie ...) qui sont des programmes destinés à perturber le fonctionnement normal du système informatique. Et d'autre part, l'action de fausser le fonctionnement du système qui est l'action sur le système

[3] Art 431-7 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité, JO N°6406 du samedi 03 mai 2008.
[4] Mohamed N. Salam «le piratage informatique : définition et problèmes juridiques », www.lb.refer.org.

qui, sans empêcher son fonctionnement, lui fait produire un résultat différent de ce qui était escompté.

Les atteintes à la disponibilité des systèmes informatiques sont sanctionnées par l'article 431-11 de la même loi qui dispose qu' « encoure une sanction pénale la personne qui aura accédé ou tenté d'accéder frauduleusement, introduit ou tenté d'introduire frauduleusement des données dans un système informatique ». Il ressort de cet article que l'accès frauduleux à un système informatique est considéré comme une infraction, de même que l'introduction frauduleuse de données dans un système informatique (opération technique élémentaire consistant à incorporer des caractères magnétiques nouveaux dans un système). La tentative des atteintes aux systèmes est réprimée comme les délits principaux.

A la lecture de ses articles l'infraction sera établie si d'une part, la personne a "agit sans droit", et d'autre part si elle a agit intentionnellement[5]. Les actes visés ne sont punissables que s'ils sont commis "sans droit", "frauduleusement" ou dans "l'intention de nuire", ces trois termes étant équivalents. Ces termes sont ici utilisés par opposition aux "personnes autorisées" qui échappent à l'incrimination. Il s'agit de toute personne ayant le droit, en vertu d'un contrat ou d'une loi, ou l'autorisation légale, d'utiliser, d'administrer, de contrôler, de tester, d'effectuer des recherches scientifiques légitimes ou d'exploiter de toute autre manière un système d'information et qui agit conformément à ce droit ou à cette autorisation.

Le délinquant doit en outre avoir agi "intentionnellement". Ainsi, l'employé qui par négligence imprudence ou incompétence altère, modifie ou détruit un fichier ne saurait être inquiété par ces dispositions[6].

Ces textes sanctionnent l'intention qui résulte en l'espèce de la conscience de s'introduire dans un espace privé, sans droit, ni autorisation préalable du Maître du système.

Dans l'affaire « Boom-E-RANG» le Tribunal Correctionnel de Lille a déduit l'élément intentionnel du délit d'accès frauduleux du fait que «les prévenus ont accédé à des systèmes de traitement automatisé de données en ayant parfaite conscience qu'ils le faisaient sans droit: les maîtres des systèmes n'ayant, par définition, pas donné d'autorisation permettant à des utilisateurs de s'introduire dans leurs serveurs afin d'y déposer des fichiers contrefaisants ou de venir copier de tels fichiers[7]». En cas de commission de ces infractions, une peine variant de six (6) mois à cinq (5) ans ou une amende de 1.000.000 à 10.000.000 FCFA peuvent être prononcée par le Tribunal. Mais une protection efficace et complète des systèmes informatiques recommande également au Sénégal, la pénalisation des atteintes aux données informatiques.

---

[5] KALINA MENGA Lionel Droit pénal et tic.

[6] Rapport explicatif de la convention de Budapest n° 38.

[7] Voir en ce sens Trib. Corr. Paris, 5 novembre 1996, Expertises, n° 202, fév. 1997, p. 81.

[5] Art 431-7 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

b. Les infractions portant atteintes aux données informatiques

La notion de données informatisées[8] se définit comme « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ». En ce sens la donnée informatisée est la représentation numérisée de l'information. La protection pénale des données informatiques s'étend a la protection générale des données informatiques à laquelle devra s'ajouter une protection spécifique aux données informatisées, encore appelées données à caractère personnel.

Le législateur sénégalais a mis en place un système de protection générale des données informatiques. En effet, l'article 431-12 de la loi sur la cybercriminalité prévoit que « est passible de sanction pénale quiconque aura intercepté ou tenté d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique... ».

Ainsi l'interception frauduleuse de données informatisées assurant la garantie du secret des données est considérée comme une infraction, conformément au principe du secret des correspondances électroniques posé par l'article 13 de la constitution de 2001.

L'endommagement, l'effacement, la détérioration, l'altération, la détérioration, la modification frauduleuse de données informatisées est sanctionnée par la loi[9]. La tentative des atteintes aux données est réprimée comme les délits principaux.

Comme toutes les infractions informatiques, l'atteinte aux données est un délit intentionnel qui suppose que soit établie la volonté de nuire. Le délinquant doit en outre avoir agi "intentionnellement" et" sans droit ". Ces textes sanctionnent l'intention qui découle en l'espèce de la conscience de s'introduire dans un espace privé, sans droit, ni autorisation préalable.

La protection pénale spécifique des données à caractère personnel exige comme condition préalable l'existence de données à caractère à caractère personnel[10].

Aux termes de l'article 431-17 de la loi sur la cybercriminalité « encoure une sanction pénale quiconque aura, même par négligence, procédé ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel». Cet article sanctionne la mise en œuvre des traitements de données à caractère personnel en violation des formalités légales préalables.

---

[9] Art 431-13 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

7 Art 4 de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel. JO N°6406 du samedi 03 mai 2008.

Le non-respect de la mise en demeure de cesser le traitement de données à caractère personnel adressée par la Commission des Données Personnelles (CDP) est punit par la loi[11].

Les articles 431-19 et 431-20 de la loi sur la cybercriminalité forme la mise en œuvre des traitements de données à caractère personnel en violation des normes simplifiées ou d'exonération établies par la CDP[12] et celles, hors des cas autorisés, incluant le numéro d'inscription des personnes au répertoire national d'identification des personnes physique[13].

La mise en œuvre des traitements de données à caractère personnel en violation de l'obligation de préserver la sécurité des données[14], la collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite[15] et la violation du droit d'opposition de la personne concernée[16] est considérée comme une infraction a la loi.

Le législateur réprime la mise et la conservation sur support ou en mémoire informatique de données sensibles[17] et données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté[18] .

La mise en œuvre des traitements illicites de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé[19] et la conservation des données à caractère personnel au-delà de la durée nécessaire à leur finalité[20] est sanctionnée par la loi.

Enfin, le traitement de données à caractère personnel à des fins autres qu'historiques, statistiques ou scientifiques au-delà de la durée nécessaire à leur finalité[21], le détournement de finalité de données à caractère personnel[22], la divulgation illicite de données à caractère personnel[23] et l'entrave à l'action de la Commission des Données Personnelles[24] est punit par la loi .

L'atteinte aux données informatiques nécessite seulement un acte matériel de commission, le juge n'a pas besoin de l'élément intentionnel pour sanctionner l'auteur de l'infraction.

La production, la vente, l'importation, la détention, la diffusion, l'offre, la cession la mise à disposition d'un équipement, programme informatique, dispositif ou donnée conçue ou spécialement adaptée pour la commission d'infractions informatiques ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie

---

[11] Art 431-18 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[12] Art 431-19 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[10] Art 431-20 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

[14] Art 431-21 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[15] Art 431-22 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[16] Art 431-23 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[17] Art 431-24 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[18] Art 431-25 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[19] Art 431-26 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[20] Art 431-27 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[21] Art 431-28 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[22] Art 431-29 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[23] Art 431-30 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.
[24] Art 431-31 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

d'un système informatique est punit des peines prévues pour l'infraction elle-même au sens de l'article 431-32 de la loi sur la cybercriminalité.

A l'instar des infractions ci-dessus visées, la peine d'emprisonnement varie entre six (6) mois et sept (7) ans et d'une amende 500.000 à 10.000.000 FCFA. Ainsi des infractions informatiques sont aussi prévues et réprimées par la loi.

c. Les infractions informatiques

Les infractions informatiques concernent les infractions ordinaires qui sont souvent commises au moyen d'un système informatique. Le législateur a prévu comme infractions informatiques le faux informatique (1) et la fraude informatique (2).

1) Le faux informatique

Le faux informatique[25] ou falsification est le fait de produire ou fabriquer un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales. Ces textes ont pour objet d'instituer une infraction qui soit le pendant de la falsification des documents sur papier. Elles visent à combler les lacunes du droit pénal se rapportant à la falsification classique, laquelle requiert la lisibilité visuelle des déclarations contenues dans un document et ne s'applique pas aux données enregistrées sur support électronique. La manipulation de données enregistrées ayant force probante peut avoir des conséquences aussi graves que les actes traditionnels de contrefaçon si elle induit un tiers en erreur.

La falsification informatique consiste à créer ou modifier sans autorisation des données enregistrées de façon qu'elles acquièrent une valeur probante différente et que le déroulement de transactions juridiques, qui est fondé sur l'authenticité des informations fournies par ces données, puisse faire l'objet d'une tromperie.

Les intérêts juridiques protégés sont la sécurité et la fiabilité des données électroniques qui peuvent avoir des conséquences pour les relations juridiques. Cette disposition s'applique aux données équivalant à un document public ou privé ayant des effets juridiques.

L'élément matériel est l'introduction non autorisée de données exactes ou inexactes qui créent une situation qui correspond à la fabrication d'un faux document. Les opérations ultérieures d'altération (modifications, changements partiels), d'effacement (le fait de sortir des données figurant sur un support) et de suppression (le fait de retenir et de cacher des données) correspondent en général à la falsification d'un document authentique.

---

[25] Art 431-14 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

L'expression «à des fins légales» s'applique également à des transactions et documents juridiques qui sont légalement pertinents. Il en sera notamment ainsi, de l'imitation ou de la falsification d'une signature électronique qui créeraient des effets indus à l'égard du véritable titulaire de la signature ou de la suppression, la modification d'un e-mail ou de tout autre document contractuel transmis par la voie électronique qui serait susceptible de modifier radicalement l'issue d'un procès.

Les manipulations informatiques devraient en principe être punies du seul fait de leur commission volontaire et consciente, contrairement au faux, l'intention frauduleuse ou le dessein de nuire étant déductibles de la conscience de fausser l'appréciation juridique d'un document.

L'usage de faux informatique[26] en connaissance de cause des données falsifiées est aussi réprimé par la loi. Ce texte exige en plus une intention frauduleuse ou une intention pernicieuse similaire pour que la responsabilité pénale puisse être engagée. Une peine d'emprisonnement de un (1) an à cinq (5) et une amende de 500.000 FCFA ou l'une des deux peines seulement peut être prononcée. La fraude informatique est aussi considérée comme une infraction informatique.

2) La fraude informatique

La fraude informatique[27] par contre consiste en l'obtention frauduleuse, pour soi-même ou pour autrui, d'un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique. Par « avantages quelconques », il faut entendre un préjudice économique ou matériel.

La révolution technologique a multiplié les possibilités de commettre des infractions économiques telles que la fraude, notamment l'escroquerie aux cartes de crédit. Les actifs représentés ou gérés par des systèmes informatiques (fonds électroniques, dépôts) sont devenus la cible de manipulations au même titre que les formes traditionnelles de propriété.

Ces infractions consistent pour l'essentiel en des manipulations à l'entrée du système, c'est-à-dire en introduisant dans l'ordinateur des données inexactes, en des manipulations de programmes ou en d'autres ingérences dans le traitement des données. Cet article a pour objet de rendre passible d'une sanction pénale toute manipulation abusive au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété. Afin de veiller à ce que toutes les manipulations pertinentes possibles soient prises en compte, les éléments constitutifs que sont l'introduction, l'altération, l'effacement et la suppression sont complétés par l'acte général d'atteinte au fonctionnement d'un système informatique. Les manipulations informatiques frauduleuses sont incriminées si elles occasionnent directement à autrui un

[26] Art 431-15 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité
[27] Art 431-16 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

préjudice économique ou matériel et si le délinquant a agi dans l'intention d'obtenir un avantage économique illégitime pour lui-même ou pour autrui[28].

L'expression préjudice économique ou matériel correspond à une notion très large qui englobe l'argent et les immobilisations corporelles ou incorporelles ayant une valeur économique.

L'infraction doit être commise intentionnellement avec pour but de porter illégitimement atteinte à la propriété d'autrui. Il en sera ainsi de la plupart des infractions informatiques motivées par l'appât du gain. On pense notamment à la fabrication de la fausse carte de crédit, de l'escroquerie en ligne ou simplement du téléchargement non autorisé de fichiers musicaux sur internet[29].

L'élément général d'intention s'applique à la manipulation ou à l'ingérence informatique causant un préjudice économique ou matériel à autrui. L'infraction exige également une intention frauduleuse spécifique ou autrement malhonnête en vue d'obtenir un avantage économique pour soi-même ou pour autrui. La peine d'emprisonnement de un (1) an à cinq (5) et une amende de 500.000 FCFA ou l'une des deux peines seulement peut être prononcée. Il existe aussi des infractions qui portent atteintes aux personnes.

2. Les infractions portant atteintes aux personnes

Ces infractions sont relatives à la pornographie infantile (a) et aux actes de nature raciste et xénophobe (b).

a. La pornographie infantile

La notion de pornographie infantile[30] est définie comme 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[31] se livrant à un comportement sexuellement explicite. La pornographie enfantine vise à renforcer les mesures de protection en faveur des enfants, notamment leur protection contre l'exploitation sexuelle, en modernisant le droit pénal de façon à restreindre plus efficacement l'usage des systèmes informatiques dans le cadre de la commission d'infractions sexuelles à l'encontre d'enfants.

De nombreuses incriminations sont prévues par la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité. Ces dispositions incriminent les différents aspects de la production, de la possession et de la diffusion de pornographie enfantine.

---

[28] KALINA MENGA Lionel Droit pénal et tic.

[29] Idem même auteur.

[30] Art 437-7 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[31] Art 276 du code de la famille.

La plupart des États incriminent déjà la production traditionnelle et la diffusion physique de pédopornographie[32], étant donné que l'Internet est de plus en plus utilisé comme instrument principal pour l'échange de ce matériel.

On s'accorde largement à reconnaître que ce matériel et les pratiques en ligne qui lui sont associées, telle que l'échange d'idées, de fantasmes et de conseils entre pédophiles contribuent à appuyer, encourager ou faciliter les infractions sexuelles commises à l'encontre d'enfants.

Le législateur sénégalais érige en infraction le fait de produire de la pornographie enfantine en vue de la diffuser par le biais d'un système informatique. Cette disposition a été jugée nécessaire pour combattre à la source les dangers que courent les mineurs[33]. Il en est de même pour le fait d'offrir, de mettre à disposition, de diffuser ou de transmettre de la pornographie enfantine par le biais d'un système informatique[34]. Le fait de procurer, d'importer ou d'exporter une image ou une représentation est aussi prévu par les textes[35].

La possession de la pornographie enfantine dans un système informatique ou dans un moyen de stockage de données informatiques, comme une disquette ou un disque optique compact est considérée comme une infraction pénale[36]. Le fait de posséder de la pornographie enfantine stimule la demande de ce matériel. Un moyen efficace de mettre un frein à la production de pornographie enfantine consiste à rendre passible de sanctions pénales le comportement de chaque maillon de la chaîne allant de la production à la possession. Il en est de même pour celui qui facilite l'accès à des images, documents ou une représentation de pornographie infantile a un mineur[37]. Néanmoins, ces infractions doivent être commises par le biais d'un système informatique.

Il convient de préciser que le législateur n'a pas prévu dans ce type d'infraction l'élément intentionnel, ce qui implique donc que la personne qui commet ce délit peut être sanctionnée même en l'absence d'intention et elle est lourdement réprimée par la loi même lorsqu'elles ont été commises par une bande organisée. En cas de commission de ces infractions, une peine d'emprisonnement de cinq (5) à dix (10) ans et une amende de 5.000.000 à 15.000.000 FCFA ou l'une des deux peines seulement sera prononcée.

Cependant, les infractions se rapportant au contenu ne se limitent pas seulement à la pornographie infantile. Les infractions portant atteintes aux personnes s'étendent aussi aux actes de nature raciste ou xénophobe.

---

[32] Sur cette définition voir le rapport explicatif de la convention de Budapest n°91 et suivants

[33] Voir Jean Aloise NDIAYE, « La protection des mineurs dans l'internet », mémoire de DEA de droit Economique et des Affaires, Université Gaston BERGER .

[34] Art 431-34 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[35] Art 431-35 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[36] Art 431-36 al 1 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[37] Art 431-36 al 2 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

b. Les actes de nature raciste ou xénophobe

La haine, la discrimination ou la violence peuvent être dirigées contre une personne ou un groupe de personnes, en raison de leur appartenance à un groupe caractérisé par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ou qui incite à de tels actes[38]. Le racisme et la xénophobie étant des manifestations de l'intolérance en tant qu'ils prêchent la confrontation des peuples sur la base de distinctions moralement et juridiquement douteuses, préoccupent la communauté internationale en ce qu'ils constituent des freins à la construction d'un monde harmonieux. A ce titre, la lutte contre le racisme et la xénophobie a fait l'objet de nombreux instruments juridiques tant nationaux que régionaux ou internationaux[39].

Toutefois, comme pour la pédopornographie, l'apparition de réseaux de communication globale comme Internet a offert des outils modernes et puissants pour diffuser plus facilement et plus largement ces affirmations vénéneuses en prenant à défaut les dispositifs répressifs en place. Il fallait donc prévoir au plan interne une réponse juridique adéquate à la propagande de nature raciste et xénophobe diffusée par le biais des systèmes informatiques. Dans cette logique la loi sur la cybercriminalité en son article 431-38 sanctionne la création, le téléchargement, la diffusion ou la mise à disposition sous quelque forme que ce, soit d'écrits, de messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique. Cette incrimination vise la diffusion ou toute autre forme de mise à disposition du public d'écrits, d'images ou à toute autre représentation d'idées ou de théories, de nature raciste et xénophobe, dans un format tel qu'il puisse être conservé, traité et transmis par le biais d'un système informatique[40].

La menace et l'insulte par le biais d'un système informatique, de commettre une infraction pénale grave, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion sont punies par la loi[41]. En effet la menace se renvoie à une intimidation qui provoque la crainte chez la personne envers laquelle elle est dirigée, qu'elle ou ses proches risquent d'être victime d'une infraction pénale grave, qui pourrait porter atteinte à leur vie, à leur intégrité physique, ou à leurs biens.

---

[38] Art 437-7 loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[39] Voir en ce sens, la Convention internationale de New York de 1965 sur l'élimination de toute forme de discrimination raciale (CERD) élaborée dans le cadre des Nations Unies, la Convention européenne des droits de l'homme (CEDH), la convention africaine des droits de l'homme et des peuples (CADHP), www.admin.ch.

[40] Voir au sujet de cette question l'affaire Yahoo voir TGI de Paris Ordonnance de référé du 20 novembre 2000, Association « Union des Etudiants Juifs de France », la « ligue contre le racisme et l'antisémitisme », le MRAP(intervenant volontaire)Yahoo.inc.Et yahoo France , http :6www.coe. int ;
La société américaine Yahoo était poursuivie par l'association des déportés d'Auschwitz pour le maintien sur son site d'un service de vente aux enchères d'objets nazis réceptionné jusqu'à Paris.

[41] Voir art 431-39 et 431-40 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

L'insulte par contre se réfère à toute expression outrageante, terme de mépris ou invective qui porte atteinte à l'honneur ou à la dignité de la personne[42]. Il devrait clairement résulter de l'expression elle-même que l'insulte est directement liée à l'appartenance à un groupe de la personne insultée. La plupart des cas de crimes contre l'humanité sont motivés par des idées et des théories de nature raciste et xénophobe. C'est pourquoi le législateur sanctionne par la même occasion la négation, l'approbation ou justification d'actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique[43]. Il s'agit d'incriminer toute expression qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international. Cependant le simple fait de commettre une de ces infractions est constitutif de délit cybercriminel et la peine prévue varie entre six (6) mois et sept (7) ans et une amende de 1.000.000 à 10.000.000. FCFA. Les prestataires techniques de services de communication au public par voie électronique ont aussi des infractions qui s'appliquent à eux.

3. Les infractions liées aux activités des prestataires techniques de services de communication au public par voie électronique

La participation des prestataires techniques à la lutte contre les contenus illicites et préjudiciables en ligne dans le cadre d'une démarche de politique criminelle participative (ordre public et bonnes mœurs) est nécessaire. Voilà pourquoi certaines infractions s'appliquent à eux. Les prestataires techniques de services au public utilisant les technologies de l'internet[44] sont définies par la loi sur les transactions électroniques. Ce sont d'abord les Fournisseurs d'accès (FAI) prévus par l'article 3.1 de la loi sur les transactions électroniques qui stipule que « 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 *(...)* ». La fourniture d'accès c'est le rôle technique de connexion des personnes au réseau Internet.

Ensuite les fournisseurs d'hébergement (FH) prévus par l'article 3.2 de la loi précitée dispose que « les personnes physiques ou morales qui assurent, même à titre gratuit, par la mise à disposition au public des biens et services, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ».

Et enfin les fournisseurs de contenus (FC) prévus par l'article 5 de la même loi dispose que « personnes dont l'activité est d'éditer un service de communication au public par le biais des technologies de l'Internet (...) ».Il s'agit de toute personne physique ou morale qui, à titre professionnel ou non édite et met en ligne de l'information (créateur d'un site web, site marchand, d'informations...). L'article 431–43 de la loi sur la cybercriminalité prévoit que « Quiconque aura présenté aux personnes mentionnées au 2° de l'article 3 de la loi sur les

---

[42]Pour une illustration jurisprudentielle, voir Tribunal de 1ère instance de Bruxelles (Corr.), 15 janvier 2002. Ministère public et Infonie : Th. Vanden B

[43] Voir art 431-41 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[44] Art 2.3 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

transactions électroniques, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte...». En effet, la présentation d'informations fausses au fournisseur d'hébergement en vue d'en obtenir le retrait ou la cessation de la diffusion est considérée comme une infraction.

Aux termes de l'article 431 - 44 de la loi précitée le fait pour toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux points 1 et 2 de l'article 3 de la loi sur les transactions électroniques, qui n'aura pas satisfait aux obligations définies au quatrième alinéa du point 5 de l'article 3 de la loi sur les transactions électroniques, n'aura pas conservé les éléments d'information visés à l'article 4 alinéa 1er de la loi susvisée ou n'aura pas déféré à la demande d'une autorité judiciaire d'obtenir communication desdits éléments est considérée comme une infraction. Ainsi, cet article sanctionne le manquement aux obligations incombant aux fournisseurs d'accès et d'hébergement que sont l'obligation de signalement des informations illicites et l'obligation de conservation de données permettant l'identification du créateur d'un contenu ou de l'un des contenus des services, dont elles sont prestataires.

Le manquement à l'obligation spécifique du fournisseur d'accès de mentionner dans les contrats de leurs abonnés l'existence de moyens techniques permettant des restrictions ou la sélection de l'accès à certains services[45] est réprimé. Il convient aussi de préciser que le manquement à l'obligation générale d'identification du fournisseur de contenus est une infraction à la loi[46].

Il ya lieu de distinguer les fournisseurs de contenus professionnels qui ont l'obligation de mettre à la disposition du public des informations permettant son identification (noms, prénoms, domicile, dénomination, siège social...) et les fournisseurs de contenus non professionnels qui ont aussi l'obligation de mettre à la disposition du public des informations permettant l'identification du fournisseur d'hébergement, sous réserve de la communication des éléments d'identification personnelle à ce prestataire. Lorsque l'une des infractions visées est constituée la peine d'emprisonnement varie entre six (6) mois à un (1) an ou une amende de 100.000 à 2.000.000 FCFA. Néanmoins, d'autres infractions sont liées au commerce électronique et à la publicité par voie électronique.

4. Les infractions liées au commerce électronique et à la publicité par voie électronique

Le développement fulgurant des TIC a entrainé des infractions liées au commerce électronique (a) et a la publicité par voie électronique (b).

[45] ART 431-45 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[46] Art 431-46 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

a. Le commerce électronique

Le commerce électronique appelé en anglais e-commerce est l'activité économique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture de biens et la prestation de services[47]. Le commerce électronique ou vente en ligne désigne l'échange de biens et de services entre deux entités sur les réseaux informatiques, notamment Internet. Le commerce électronique s'exerce librement sur le territoire national à l'exclusion des jeux d'argent, même sous forme de paris et de loteries, légalement autorisés, des activités de représentation et d'assistance en justice et du notariat en ligne.

Le champ d'application du commerce électronique concerne les services de fourniture d'informations en ligne, communications commerciales, les outils de recherche, les services d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, même non rémunérées. C'est un marché en pleine expansion. La dématérialisation du processus contractuel, l'internationalité des rapports contractuels et l'anonymat des prestataires ont entrainé une aggravation de la vulnérabilité du consommateur dans le cyberespace.

La loi portant sur la cybercriminalité[48] impose aux fournisseurs d'accès[49] et d'hébergement[50], d'une part l'obligation de signalement aux autorités publiques compétentes les informations illicites en mettant en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type d'informations et de rendre public les moyens qu'ils consacrent à la lutte contre ces activités illicites[51], et d'autre part l'obligation de conservation de données permettant l'identification du créateur d'un contenu ou de l'un des contenus des services dont elles sont prestataires[52].

Cependant, le législateur sénégalais dans le souci de lutter efficacement contre la cybercriminalité sanctionne le manquement de l'obligation d'information[53] du fournisseur de biens et de prestation de services à distance et par voie électronique à l'égard du consommateur[54] par la mise à la disposition des cyberconsommateurs[55] d'informations

---

[47] Art 8 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[48] Art 431-44 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[49] Art 3.1 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[50] Art 3.2 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[51] Art 3.5 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[52] Art 4 alinéa 1 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[53] Art 431-48 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[54] Art 203 de l'acte uniforme sur le droit commercial général

[55] Notion définie par Jean Aloise NDIAYE Magistrat comme « toute personne qui se procure, par voie électronique un produit ou un service pour son usage personnel, familial ou domestique n'entrant pas dans le cadre de son activité professionnelle ».voir « Le cadre juridique des transactions électroniques au Sénégal » : la présentation de la loi n° 2008- 08 du 25 janvier 2008, portant sur les transactions électroniques.

permettant son identification (nom et prénom, raison sociale, adresse complète, siège social, capital social, NINEA…), et indication précise du prix du contrat et les taxes et frais de livraison[56].

Il réprime à cet effet le refus[57] d'un fournisseur électronique de biens ou de services de rembourser des montants reçus d'un consommateur dans l'exercice de son droit de rétraction prévu par l'article 12 du décret n° 2008-718 du 30 juin 2008[58], relatif au commerce électronique pris pour l'application de la loi sur les transactions électroniques qui stipule que «pour tout contrat conclu par voie électronique, le consommateur dispose d'un délai de sept jours ouvrables pour se rétracter, sans indication de motif et sans pénalité». Il s'agit d'une dérogation au principe de la force obligatoire du contrat.

Si le fournisseur électronique de biens ou de services n'a pas satisfait aux obligations d'information à l'égard du consommateur, ce dernier pourra bénéficier d'un délai de rétractation de trois mois (art. 12 du décret précité). La tromperie de l'acheteur sur l'identité, la nature ou l'origine du bien vendu en lui livrant frauduleusement un bien autre que celui commandé et acheté par le consommateur est également considérée comme une infraction[59]. Le tribunal peut prononcer à l'encontre de l'auteur de l'infraction un emprisonnement variant entre un (1) mois et un (1) an et une amende de 200.000 à 10.000.000FCFA ou l'une des deux peines seulement.

Il convient de noter que le décret n° 2008-718 du 30 juin 2008 fixe les conditions d'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques notamment celle relative au commerce électronique. La publicité par voie électronique fera l'objet d'une étude.

b. La publicité par voie électronique

La publicité par voie électronique est prévue par l'article 431 - 51 de la loi sur la cybercriminalité qui dispose que «quiconque aura méconnu les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celles de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie numérique, telles que prévues par l'article 15 de la loi sur les transactions électroniques…».

L'article 431 – 52 de la loi précitée qui prévoit la sanction pénale de la violation de l'obligation d'identification de la publicité dispose que « quiconque aura réalisé des publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique.

---

[56] Art 10 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[57] Art 431-49 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[58] Voir J.O. N° 6440 du Samedi 29 NOVEMBRE 2008

[59] Art 431-50 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

en violation de l'article 14 de la loi sur les transactions électroniques...». A travers ces deux articles cités, les infractions liées à la publicité par voie électronique sont la méconnaissance des conditions pour bénéficier des offres promotionnelles et de la participation à des concours ou à des jeux promotionnels proposés par voie numérique et la réalisation de publicités par courrier électronique non identifiées.

La loi n° 2008 du 25 janvier sur les transactions électroniques en ses articles 13 à 17 pose les conditions de la publicité par voie électronique. En effet, les articles 13 et 14 de cette loi posent l'admission du principe de l'identification de la publicité en ces termes « les publicités, et notamment les offres promotionnelles, adressées par courrier électronique, doivent pouvoir être identifiées de manière claire et non équivoque sur l'objet du courrier dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message ».

Le principe de la transparence des offres, concours ou jeux promotionnels par voie électronique est prévu par l'article 15 de la même loi. L'article 16 du même texte pose l'interdiction de la prospection directe[60] par envoi de message au moyen notamment d'un courrier électronique, en utilisant, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen (art. 16 alinéa 1er) prohibition du spamming (envoi de courriers électroniques non sollicité). La loi susvisée a prévu aussi l'interdiction de la prospection directe en dissimulant l'identité de la personne pour le compte de laquelle la communication est émise (art. 16 alinéa2e).

Le consentement des personnes dont les coordonnées ont été recueillies avant la publication de la loi sur les transactions électroniques, dans les conditions prévues par la loi sur la protection des données à caractère personnel à l'utilisation de celles-ci à fin de prospection directe, peut être sollicité par voie de courrier électronique, pendant les six (6) mois suivants la publication de la présente loi.

A l'expiration de ce délai, ces personnes sont présumées avoir refusé l'utilisation ultérieure de leurs coordonnées personnelles à fin de prospection directe si elles n'ont pas manifesté expressément leur consentement à celle-ci[61]. Le législateur a prévu pour cette infraction une peine d'emprisonnement de six (6) mois à deux (2) ans et une amende de 100.000 à 500.000 FCFA.

Dans la lutte contre la cybercriminalité, le législateur s'est confronté à une inadaptation des sanctions pénales, d'où l'effet de créer de nouvelles sanctions pénales adaptées a la cybercriminalité.

---

[60] Art 2.4 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[61] Art 17 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

B. La création de nouvelles sanctions pénales adaptées à la cybercriminalité

La loi sur la cybercriminalité est à l'origine de nouvelles infractions qui sont spécifiques aux TIC (1) et elle a par la même occasion prévue un régime de responsabilité pénale des acteurs intervenant dans cette lutte (2).

1. Les sanctions spécifiques aux TIC

Le législateur sénégalais a prévu d'une part, l'utilisation d'un système informatique en circonstance aggravante d'infractions contre les biens et des peines complémentaires (a) et d'autre part, le droit de réponse en ligne (b).

a. L'utilisation d'un système informatique en circonstance aggravante d'infraction contre les biens et les peines complémentaires

Il ya d'abord l'utilisation d'un système informatique qui est considérée par le législateur comme une circonstance aggravante d'infractions contre les biens. En effet, l'article 431-54 de la loi sur la cybercriminalité dispose que « lorsque les infractions ont été commises par le biais d'un système informatique, il ne pourra être prononcé le sursis[62] à l'exécution des peines ». Ce qui signifie que quelle que soit l'infraction pour laquelle on est poursuivie, l'auteur ne pourra pas bénéficier du sursis à l'exécution de sa peine. C'est dans cette même lancée que les peines prévues par l'alinéa 1er de l'article 379 du code pénal qui réprime l'escroquerie pourront être portées au double si le délit a été commis par le biais d'un système informatique[63].

Ensuite il ya eu la création de nouvelles peines complémentaires qui accompagnent les sanctions pénales et qui sont prévues pour la juridiction de jugement par la loi sur la cybercriminalité. Il existe des peines complémentaires facultatives[64] que sont l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction, la coupure de l'accès au site ayant servi à commettre l'infraction et l'interdiction de l'hébergement du site ayant servi à commettre l'infraction. Le juge peut par la même occasion faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction ou à toute personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir l'interdiction d'accès, d'hébergement et la coupure de l'accès au site incriminé. Le juge sanctionne la violation des interdictions prononcées.

La peine complémentaire obligatoire est la publication de la décision judiciaire sur un support de communication numérique. En effet, l'article 431-65 de la loi sur la

---

[62] Voir dictionnaire le Robert micro p.1285

[63] Art 431-55 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[64] Art 431-64 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

cybercriminalité dispose qu'« En cas de condamnation à une infraction commise par le biais d'un support de communication numérique, le juge ordonne à titre complémentaire la diffusion aux frais du condamné, par extrait, de la décision sur ce même support. La publication prévue à l'alinéa précédent doit être exécutée dans les 15 jours suivants le jour où la condamnation est devenue définitive. Le condamné qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa précédent sera puni des peines prévues par le code pénal. Si dans le délai de quinze jours (15) jours après que la condamnation soit devenue définitive, le condamné n'a pas diffusé ou fait diffuser cet extrait, les peines prévues au présent article seront portées au double ».

Concernant les infractions se rapportant au contenu, en cas de condamnation aux infractions prévues par les articles 43-8 à 43-41 de la loi sur la cybercriminalité, le Tribunal pourra prononcer à titre complémentaire la confiscation des matériels d'équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi a commettre les infractions. Il existe cependant un droit de réponse en ligne.

b. le droit de réponse en ligne

Enfin au terme de l'article 6 de la loi sur les transactions électroniques « Toute personne nommée ou désignée dans un service de communication au public utilisant les technologies de l'Internet dispose d'un droit de réponse, sans préjudice des demandes de modification ou d'opposition au message qu'elle peut adresser au service. La demande d'exercice du droit de réponse est adressée au directeur de publication ou, lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée au point 2 de l'article 3 de la présente loi qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois (3) mois à compter de la mise à disposition du public du message justifiant cette demande ».

A la lecture de cet article qui prévoit le droit de réponse en ligne, il faut retenir que toute personne nommée ou désignée dans un service de communication au public en ligne[65] dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service. La demande d'exercice du droit de réponse est adressée au directeur de la publication ou, lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée physique ou morale qui assure la mise à disposition au public, qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois mois à compter de la mise à disposition du public du message justifiant cette demande.

Cependant, un décret[66] fixe les modalités d'application du droit de réponse dans un service de communication par voie électronique[67].Il prévoit qu'en application de l'article 6 de

[65] Art 2.5 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

[66] 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.

[67] Art 2 .1 de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques

la loi sur les transactions électroniques, toute personne, physique ou morale, nommée ou désignée dans un service de communication par voie électronique dispose d'un droit de réponse gratuit. Pour les personnes physiques, il est nécessaire d'avoir été mis personnellement en cause pour exercer le droit de réponse. Pour les personnes morales, l'organe qui souhaite exercer le droit de réponse doit être dûment habilité. Il est possible d'exercer le droit de réponse au profit d'un tiers en cas de mandat dûment notifié.

La demande d'exercer du droit de réponse est adressée par lettre recommandée ou par tout autre moyen garantissant l'identité du demandeur et la preuve de la réception de la demande aux destinataires mentionnés à l'article 6 de la loi sur les transactions électroniques. La demande d'exercice du droit de réponse indique toutes les références relatives au message en cause, notamment, s'il est mentionné, le nom de l'auteur, l'emplacement du message, sa nature (écrit, son ou image), les passages contestés et la teneur de la réponse sollicitée. La réponse est mise à la disposition du public par le Directeur de publication dans des conditions similaires à celles du message en cause et présentée explicitement comme résultant de l'exercice du droit de réponse. Elle est soit publiée à la suite du message en cause, soit accessible à partir de celui-ci.

Lorsque le message n'est plus mis à la disposition du public, la réponse est accompagnée d'une référence à celui-ci, d'un rappel de la date et de la durée de sa mise à disposition du public. La réponse demeure accessible durant la même période que celle pendant laquelle le message en cause est mis à disposition du public. La durée pendant laquelle la réponse est accessible ne peut être inférieure à quarante-huit heures. La personne qui adresse une demande d'exercice d'un droit de réponse peut préciser que sa demande deviendra sans objet si les personnes mentionnées à l'article 6 de la loi sur les transactions électroniques acceptent, dans le délai qu'elle indique dans sa requête, de supprimer ou de rectifier tout ou partie du message à l'origine de l'exercice de ce droit. La demande précise les passages du message dont la suppression est sollicitée ou la teneur de la rectification envisagée.

Les personnes susmentionnées au présent article ne sont pas tenues d'insérer la réponse si elles procèdent à la suppression ou à la rectification sollicitée. Le délai mentionné au présent article court dès la réception de la demande d'exercice de droit de réponse. L'absence de désignation d'un directeur de publication n'entrave pas l'exercice du droit de réponse. Pour terminer, cet article a pour effet de sanctionner le manquement à l'obligation du directeur de publication de publier la réponse portant sur l'exercice du droit de réponse en ligne. A défaut ce dernier est passible d'une amende de 200.000 à 20.000.000 FCFA. La loi sur la cybercriminalité a prévu la responsabilité pénale des acteurs.

2. La responsabilité pénale des acteurs

Le caractère punissable d'un acte constitutif d'une infraction ne s'apprécie pas uniquement en considération de l'acte lui-même, mais également en tenant compte de la personne qui en est l'auteur. Anciennement, seules les personnes physiques pouvaient être déclarées responsables. Le code pénal de 1965 institue le principe de la responsabilité pénale des personnes morales. Cependant, la responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits. La responsabilité pénale est

l'aptitude à répondre de ses actes délictueux et à subir la peine qui leur est attachée par la loi. Elle n'est pas un élément de l'infraction, mais en est l'effet et la conséquence juridique. Une personne est punissable si elle est pénalement responsable, si elle a commis une faute (culpabilité) et si son acte n'est pas justifié[68].

La personne morale ne sera pas pénalement responsable des infractions commises dans l'exercice ou à l'occasion de l'exercice de ses fonctions, par un de ses employés, dès lors que celui-ci aura agi de sa propre initiative, ceci, même si la personne morale a pu bénéficier de l'infraction. De même, une personne morale ne sera pas responsable des infractions commises par un dirigeant dans l'exercice ou à l'occasion de l'exercice de ses fonctions, si ce dirigeant avait agi pour son propre compte et dans son seul intérêt. La responsabilité pénale des personnes morales suppose donc que l'infraction ait été commise pour leur compte, par leurs organes ou représentants.

En revanche, la responsabilité pénale d'une personne morale pourra être engagée en l'absence de volonté délibérée de ses organes ou représentants. La personne agissant sous l'autorité de la personne morale c'est-à-dire l'un de ses employés ou agents agissant dans le cadre de leur pouvoir doit remplir certaines conditions pour que la responsabilité soit engagée. Il faut que l'infraction ait été commise par un employé ou agent de la personne morale, qu'elle ait été commise pour le compte de la personne morale ou la commission de l'infraction a été rendue possible par le fait que la personne exerçant un pouvoir de direction n'a pas supervisé l'employé ou l'agent en question. A cet égard, le défaut de supervision devrait être interprété comme incluant le fait de ne pas avoir pris des mesures appropriées et raisonnables pour empêcher les employés ou les agents de se livrer à des activités illégales pour le compte de la personne morale. Celle-ci pourra être condamnée non seulement en tant qu'auteur principal de l'infraction, mais également en qualité de complice.

Traditionnellement, le texte posé par l'article 270 du code pénal sénégalais, intitulé « Des personnes responsables » dispose que : « sont passibles comme auteurs principaux, des peines, qui constituent la répression des infractions prévues : 1)les directeurs de publication, codirecteurs, producteurs, éditeurs ou gérants quelle que soit leur dénomination ;2) à leur défaut, les auteurs ; 3) à défaut des auteurs, les directeurs des entreprises d'impression, d'enregistrement, de reproduction ou de diffusion, de quelque nature qu'elles soient ;4) à défaut de ceux-ci, les vendeurs, afficheurs et distributeurs, quelle que soit leur dénomination. Les importateurs, exportateurs ou transitaires qui auront participé sciemment aux dites infractions pourront être poursuivis directement comme auteurs principaux ». Ce système de responsabilité éditoriale fondé sur une présomption de responsabilité non susceptible de preuve contraire[69] peut-il être transposé au domaine des réseaux informatiques ?

En d'autres termes, ce régime de responsabilité permet-il de démêler l'écheveau de l'identification des personnes responsables dans le cyberespace. Force est de constater que le régime posé par l'article 270 du code pénal qui détermine les personnes responsables en

[68] Voir Fr.jurispedia.org.

[69] RASSAT (M.L.), op-cit, p. 404.

fonction de la qualité des acteurs de la presse audiovisuelle classique ne correspond à aucune des fonctions des intermédiaires techniques du cyberespace.

Pour apporter une réponse à cette question, le législateur sénégalais a prévu à l'article 431-62 de la loi partant sur la cybercriminalité que «les personnes morales autres que l'État, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants ». A la lecture de ce texte, on peut noter que toutes les autres personnes morales peuvent voir leurs responsabilités engagées et être poursuivies à l'exception de l'Etat, les collectivités locales et les établissements publics.

La responsabilité pénale des personnes physiques auteurs ou complices des mêmes faits n'est cependant pas exclue. La condition exigée est la commission de la cyber infraction pour le compte de la personne morale, par ses organes ou représentants. Ce texte pose en effet la consécration du principe de la responsabilité pénale des personnes morales en matière de cybercriminalité.

Cependant, les prestataires techniques également appelés intermédiaires techniques que sont les fournisseurs d'accès, les fournisseurs d'hébergement, les fournisseurs de contenus sont considérés comme des personnes morales. Ces derniers peuvent être tenus responsables en raison des contenus illicites. Ce type de responsabilité est dérogatoire du droit commun de la responsabilité, c'est un système de responsabilité allégée ou limitée des prestataires techniques. Les fournisseurs d'accès et les fournisseurs d'hébergement sont soumis à cette responsabilité.

Concernant les fournisseurs d'accès, aux termes de l'article 6 du décret relatif aux communications électroniques[70] « Les prestataires techniques sont exonérés de leur responsabilité lorsqu'ils se contentent de faire du stockage automatique ou temporaire de l'information ou de jouer un rôle d'intermédiation dans la transmission de celle-ci (...)». A ce titre, les prestataires techniques ont un rôle de simple transporteur d'informations, à l'image de l'opérateur de télécommunication. Ils disposent d'une exonération de principe de la responsabilité. Cette exonération s'applique à condition qu'ils ne sélectionnent pas le destinataire de la transmission ou qu'ils ne sont pas à l'origine de la transmission ou que leurs activités visent exclusivement l'exécution de la transmission ou de la fourniture d'accès ou qu'ils ne modifient pas les informations transmises et ou qu'ils exécutent une décision d'une autorité judiciaire ou administrative de retrait ou l'interdiction d'accès de l'information.

Par contre, les fournisseurs d'hébergement ont une responsabilité limitée. En effet, l'article 3 de la loi précitée ne peut pas voir leur responsabilité civile ou pénale engagée du fait des activités ou des informations stockées que si elles avaient effectivement connaissance de leur caractère illicite, ou si dès le moment où elles en ont eu cette connaissance, elles n'ont pas agi promptement pour retirer ces données ou en rendre l'accès impossible.

[70] 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, JO N°6439du samedi 22 novembre 2008

Le critère fondamental d'engagement de la responsabilité pénale des hébergeurs est la connaissance effective par le prestataire du caractère illicite de l'activité ou de l'information stockée. C'est une consécration d'une présomption de connaissance des faits litigieux lorsque l'hébergeur reçoit notification d'un certain nombre d'informations à savoir : la date de la notification, l'auteur de la notification, le caractère illicite des informations litigieuses, la date de la notification[71]... Les peines encourues sont l'amende, la dissolution, l'interdiction, la fermeture, et la condamnation à une peine d'emprisonnement supérieure à cinq (5) ans. La modernisation des instruments de répression de la cybercriminalité se manifeste par l'adaptation des incriminations traditionnelles aux TIC.

Paragraphe II : L'adaptation des incriminations traditionnelles aux TIC

Le nouveau phénomène criminel dénommé cybercriminalité a brouillé les repères du système pénal dont les réponses traditionnelles conçues et élaborées pour un environnement matérialisé se sont révélées inappropriées pour saisir cette nouvelle ère numérique. Il est apparu la nécessité d'adapter les incriminations traditionnelles aux infractions portant atteintes aux biens (A), celles commises par tous moyens de diffusion publique (B) et celles portant atteintes a la défense nationale (C).

A. Les infractions portant atteintes aux biens

Traditionnellement le droit pénal classique était fortement marqué par la conception matérialiste de l'infraction, mais l'émergence de la révolution numérique a généralisé les atteintes portant sur les biens immatériels tels que l'information devenue un enjeu stratégique de la société de l'information. Le droit pénal sénégalais des atteintes matérielles aux biens exprime bien la tendance à la matérialisation des infractions. En effet, les articles 406 à 422 du code pénal sénégalais et 13 du code des contraventions ont essentiellement pour objet de protéger les biens corporels contre les destructions, dégradations et dommages[72].

Dans le contexte actuel de la révolution numérique, il est évident que la répression des atteintes violentes (incendies, dégradations, destruction...) ayant pour cible les supports matériels des TIC (ordinateurs, disquettes, CD-ROMS, bandes dures ou installations complémentaires) ne soulève aucune difficulté puisqu'en l'état actuel de la législation, ces comportements tombent sous le coup des articles 406 et suivants du code pénal.[73]

En définitive, il résulte clairement de l'audit du cadre juridique de la législation pénale sénégalaise relative aux atteintes matérielles aux biens, une absence totale de protection des biens informationnels, nécessitant l'élaboration d'une stratégie méthodique d'adaptation de ses qualifications pénales à l'immatérialité inhérente à ces biens se transmettant

---

[71] Art 7 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

[72] Voir sur ce point (M.L.) RASSAT, op-cit. p. 199, également VITU (A.), destruction dégradations et dommages. Rép. Pen. 1968.

[73] (R.) GASSIN. Le droit pénal de l'informatique. D.S 1986. chron. P. 37.

indépendamment de leur support. Ainsi, l'assimilation de l'information au bien présentera le mérite de permettre une adaptation du droit pénal des atteintes juridiques aux biens à l'évolution technologique. Aussi le nouveau montage juridique des délits portent une atteinte juridique aux biens devra s'effectuer par l'inclusion des biens informationnels dans l'énumération des choses : objets de vol, de recel, d'escroquerie, l'abus de confiance, etc..., ce qui garantira sa protection pénale contre lesdites atteintes.

Le vol est traditionnellement défini comme la soustraction frauduleuse de la chose d'autrui[74]. La soustraction est ici considérée comme le déplacement de la chose des mains de son possesseur légitime à celle de l'auteur du délit. Soustraire c'est donc un acte matériel qui suppose l'appréhension, l'enlèvement d'une chose qui se trouvait hors de la détention du coupable. Le terme chose vise tous les biens qui existent, quels qu'ils soient. Il peut s'agir de biens mobiliers corporels ou incorporels[75].

Le juge sénégalais a procédé à une dématérialisation du droit pénal des atteintes aux biens avant même l'adoption de la loi sur la cybercriminalité dans un jugement du 06 mai 2006 dans l'affaire dite « Clinique du Cap[76] », en admettant le vol de données informatiques et la décision a été confirmée par l'arrêt de la Cour d'Appel de Dakar du 16 avril 2007.le législateur a consacré la théorie du vol informatique en son article 431-53 de la loi sur la cybercriminalité qui stipule que « la soustraction frauduleuse d'information au préjudice d'autrui est assimilable au vol ».

Cette nouvelle forme d'appropriation frauduleuse facilite le vol de données informatiques. Le terme générique de vol de données recouvre plusieurs situations distinctes faisant référence à l'appropriation frauduleuse de données. C'est notamment le cas de la copie sans autorisation de fichiers ou données. Le terme couvre aussi la lecture sans autorisation du fichier, le transfert frauduleux de fonds ou le téléchargement non autorisé, etc...

L'escroquerie est une forme d'appropriation frauduleuse originale. C'est un délit dont la réalisation suppose le consentement de la victime, son adhésion ou tout au mois sa crédulité. C'est un délit multiforme, dynamique qui s'adapte aux conditions sociales et techniques de l'époque.

Archétype de la délinquance astucieuse, l'escroquerie est certainement l'infraction qui prospère le plus grâce à l'utilisation des technologies de l'information et de la communication.

L'escroquerie est définie comme "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

[74] Art 364 du code penal sénégalais.

[75] M. L.) RASSAT, Droit pénal spécial, 2ème édition, Dalloz 1999

[76] Inédit

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[77].

L'article 431-56 de la loi sur la cybercriminalité punit quiconque aura reçu des informations personnelles, confidentielles ou celles qui sont protégées par le secret professionnel, usant de manœuvres frauduleuses quelconques, soit en faisant usage de faux noms ou de fausses qualités. Cet article instaure l'admission de l'escroquerie portant sur une information comme le social engineering ou l'usage de fausse qualité en ligne. Le terme d'«ingénierie sociale»(en anglais «*social engineering*») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur. A titre d'exemple, on peut citer : Le *Scam* ou 419. («Ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. Cette arnaque est issue du Nigeria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds. En répondant à ce type de message, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euros s'il mord à l'hameçon et même la vie dans certains cas. *Le* phishing (contraction des mots anglais «fishing», en français pêche, et «phreaking», désignant le piratage de lignes téléphoniques) est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

Le mail envoyé par ces pirates[78] usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien et de mettre à jour des informations les concernant dans un formulaire d'une page web factice aux couleurs du site original en prétextant par exemple une mise à jour du service, une

[77] Art 379 du code penal

[78] Mohamed N Salam « le piratage informatique: définition et problèmes juridiques », www.lb.refer .org

intervention du support technique, etc. Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés, il arrive que le destinataire soit effectivement client de la banque. Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.). Grâce à ces données, les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

Pour la loterie internationale, il s'agit d'une vielle consistant à exploiter la cupidité de la victime. La victime reçoit un courrier électronique indiquant qu'elle est l'heureuse gagnante du premier prix d'une grande loterie d'une valeur de plusieurs centaines de milliers d'euro. Pour empocher le pactole, il suffit de répondre à ce courrier.

Après une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant qu'elle est bien le vainqueur, son interlocuteur lui expliquera que pour pouvoir toucher ladite somme, il lui faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées, etc. C'est de cette façon que ces cyber truands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

Cependant, les escrocs agissent à partir de pays de l'Afrique de l'Ouest tels la Côte d'Ivoire, le Ghana, le Bénin, le Togo, le Sénégal, le Nigeria[79] et le Burkina Faso et leur principal outil de commission est l'internet, grâce aux courriers électroniques. Tout récemment la police Sénégalaise a affirmé avoir arrêté un groupe de 23 Nigérians accusés de s'adonner à ces pratiques frauduleuses, consistant à soutirer d'énormes sommes d'argent contre la promesse de contrats d'affaires mirobolants, ou de transferts de gros montants que l'on veut sortir illégalement d'un pays, ou encore de gains substantiels à des loteries étrangères...

Dans le courant de l'année 2000, la police a arrêté le premier Sénégalais qui faisait de la cybercriminalité. Il était propriétaire d'un cybercafé dans le quartier de Dakar. Il a réussi à proposer une affaire concernant de grosses quantités d'or à un homme des Émirats Arabes Unis. A titre d'illustration, un individu a contacté la police leur disant qu'un Américain avait été victime d'une arnaque et leur a donné son e-mail. La police a contacté l'ambassade des États unis ici qui a un agent spécialisé. Il a contacté la victime aux États-Unis, qui a confirmé les dires de la personne qui les a informés. Elle a envoyé tous les documents relatifs à cette affaire, après analyse la police a pu localiser le cerveau, puis ses complices. Six Nigérians et deux Sénégalaises ont été arrêtés par la brigade sénégalaise de lutte contre la criminalité (BLC). C'est la première fois que la police arrête des femmes. Elles étaient en fait les complices des Nigérians. Elles avaient réalisé toutes les démarches pour ouvrir des comptes à leur nom, les hommes s'étant dit que, s'ils le faisaient eux-mêmes, cela éveillerait des

[79] Quotidien le soleil – Sénégal escroquerie sur Internet : les ravages de la «fraude nigériane» - (dossier publié le jeudi 31 juillet 2003)

soupçons parce qu'ils ne sont pas nationaux. Elles se sont fait passer pour des commerçantes ce qui constituait une couverture béton.

Cependant, les escrocs cybercriminels agissent à partir de pays de l'Afrique de l'Ouest tels la Côte d'Ivoire, le Ghana, le Bénin, le Togo, le Sénégal et le Burkina Faso et leur principal outil de commission de l'infraction est l'internet, grâce aux courriers électroniques. Tout récemment la police Sénégalaise a affirmé avoir arrêté un groupe de 23 Nigérians accusés de s'adonner à ces pratiques frauduleuses, consistant à soutirer d'énormes sommes d'argent contre la promesse de contrats d'affaires mirobolants, ou de transferts de gros montants que l'on veut sortir illégalement d'un pays, ou encore de gains substantiels à des loteries étrangères[80].

Le recel d'information est aussi réprimé par la loi sur la cybercriminalité en son article 431-57 qui punit ceux qui auront recélé des informations enlevées, détenues ou obtenues a l'aide d'un crime ou d'un délit. L'article 430 du code pénal[81] a prévu le recel, mais cette incrimination ne s'applique qu'aux biens matériels quels qu'il soit.

Traditionnellement, l'association de malfaiteurs[82] s'appliquait aux crimes ou délits commis contre les personnes ou les propriétés. Mais avec la loi sur la cybercriminalité celui qui aura participé a une association formée ou a une entente établie en de préparer ou de commettre une ou plusieurs infractions prévues par la présente loi sera poursuivie pour association de malfaiteurs[83].

Ce mouvement de politique criminelle procède en réalité d'une stratégie de « modernisation de la politique criminelle» mise à l'épreuve de l'apparition de nouveaux comportements d'écart aux normes suscitées par l'essor des technologies de l'information et de la communication, pour mieux protéger la société contre de tels agissements répréhensibles[84]. L'exemple le plus illustratif d'association de malfaiteurs est celui des actes de piratage organisés aux États-Unis, à l'encontre de nombreux sites Internet gouvernementaux. Les données du site du département de la Justice ont été remplacées par un portrait d'Adolf Hitler et par des photographies pornographiques. Puis, ce fut le tour de la CIA et enfin de l'armée américaine.

Par ailleurs devant la recrudescence des agissements ayant pour cible les éléments immatériels des TIC (système informatique, données informatiques, réseau numérique…), le système pénal sénégalais exigeait un mouvement d'adaptation des qualifications classiques du

---

[80] Voir « Séminaire » Informatique et libertés, quel cadre juridique pour le Sénégal ? 29 et 30 aout 2005 p.143 à 146

[81] «ceux qui, sciemment, auront recélé, en tout ou partie, des choses enlevées, détournées ou obtenues a l'aide d'un crime ou d'un délit seront punit des peines prévues a l'article 370 du code pénal etc. »

[82] Art 238 du code penal

[83] Art 431-33 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[84] DELMAS-MARTY, (M.), op-cit. p. 307.

droit pénal aux TIC.[85] Cependant, les infractions commises par tous moyens de diffusion publique ont été réadaptées.

B. Les infractions commises par tous moyens de diffusion publique

Aux termes de l'article 248 du code pénal sénégalais sont considères comme moyen de diffusion publique, la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces préférés dans les lieux ou réunions publiques et généralement tous procédé technique destiné à atteindre le public. Cependant, L'émergence du cyberespace amène à poser la question suivante : Internet, véhicule des messages contraires à l'ordre public peut-il être considéré comme un moyen de diffusion publique, au sens des dispositions de l'article 248 du code pénal.

La jurisprudence sénégalaise a eu à se prononcer sur cette question dans le jugement n° 2 rendu par le tribunal régional de Ziguinchor le 06 janvier 2004. Dans cette affaire, Christian Costaux a été prévenu d'avoir diffusé sur son site dénommé « sénégalaisement com » des propos diffamatoires contre Robert Sagna maire de Ziguinchor et propriétaire de l'hôtel « Kadiandoumogne », propos aux termes desquels, le maire se livrait à une concurrence déloyale dans l'irrespect des Casamançais.

Le juge du tribunal régional de Ziguinchor, statuant en matière correctionnelle, a estimé que « l'outil Internet en cause qui constitue un réseau international permettant à des personnes habitant divers endroits du monde et disposant d'ordinateurs de communiquer entre elles» constitue un « procédé technique destiné à atteindre le public», c'est-à-dire un moyen de diffusion publique au sens de l'article 248 du code pénal. Christian Costeaux fut ainsi déclaré coupable du chef de diffamation condamné à un an d'emprisonnement ferme et un mandat d'arrêt international fut décerné contre lui.

La qualification de « procédé technique destiné à atteindre le public» donné au réseau Internet par le juge correctionnel traduit la réalité de l'inadaptation au droit pénal sénégalais mis à l'épreuve des TIC, n'ayant pas pris en compte dans ses prévisions répressives, le nouveau moyen de diffusion publique qu'est l'internet. En réalité plus qu'un simple «procédé» Internet constitue un véritable moyen de communication électronique qui n'a pas une vocation exclusive à atteindre le public, mais offre plutôt plusieurs services à ses utilisateurs (courrier électronique, discussion en ligne, recherche d'informations…)[86].

Une modification du texte de l'article 248 du code pénal est donc nécessaire pour atteindre plus efficacement les agissements contraires à l'ordre public commis via Internet, en incluant ainsi dans son énumération limitative les moyens de communication électronique (comme Internet). A cet effet, la loi sur la cybercriminalité en son article 431-58 à procéder à

---

[85] Voir sur ce point (J.) FRANVILLON, l'adaptation du droit pénal à certaines formes de délinquance informatique et audiovisuelle. Mélanges A. VITU, ed. CUJAS. 1989, p. 211.

[86] TORTELLO (N.) : LOINTIER (P), Internet pour les juristes, Dalloz, 1996, p.1.

l'extension du droit pénal des infractions de presse en y incluant l'expression « tout moyen de communication numérique par voie électronique». En effet, cet article dispose que « Sont considérés comme moyens de diffusion publique : la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique ».

Il ressort également de l'article 431-59 de la loi précité que quiconque aura : 1) fabriqué ou détenu en vue d'en faire commerce, distribution, location affichage ou exposition ; 2) importé ou fait importer, exporté ou fait exporter, transporté ou 3) fait transporter sciemment aux mêmes fins ; 4) affiché, exposé ou projeté aux regards du public ; 5) vendu, loué, mis en vente ou en location, même non publiquement ; offert, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ; 6) distribué ou remis en vue de leur distribution par un moyen quelconque. Ce texte susvisé réprime tous les imprimés, écrits, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images qui sont contraires aux bonnes mœurs. Le maximum de la peine pourra être prononcé lorsque ces faits ont un caractère pornographique.

Cependant le condamné se verra, pour une durée ne dépassant pas six (6) mois, interdit d'exercer les fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publications périodique. Néanmoins certaines infractions peuvent porter atteintes à la défense nationale.

C. Les infractions portant atteintes à la défense nationale

Le secret de défense nationale doit pour des raisons stratégiques garder sa confidentialité car sa livraison à une puissance ou à une organisation étrangère est de nature à porter atteinte aux intérêts politiques de l'Etat. Avec l'essor des TIC, le secret de la défense nationale peine à préserver sa confidentialité et est souvent l'objet d'atteinte de toutes sortes consécutives à des intrusions frauduleuses dans les systèmes et réseaux gouvernementaux aux détriments des intérêts fondamentaux de l'Etat. Les articles 60 et 61 du code pénal ne protègent que les supports matériels à savoir les renseignements, documents ou procédé qui doivent être tenues secret dans l'intérêt de la défense nationale à l'exclusion des supports immatériels que sont les fichiers et données informatisés nationale susceptible d'être livrés par voie électronique à une puissance ou à une organisation étrangère. Il importera alors pour le législateur d'intégrer dans l'objet des atteintes à l'intégrité du secret de défense nationale, les éléments immatériels, que sont les données informatiques et les fichiers informatiques renfermant des secrets de défense nationale. A titre illustratif, en mai 1998 un groupe de jeune « hackers[87] » ont forcé le dispositif de sécurité du réseau du centre de recherche atomique indien et s'est assuré la possession des travaux sur les derniers essais nucléaires du gouvernement indien.

[87] Ce sont des pirates informatiques

Dans le but de lutter contre les atteintes notoires contre la défense nationale, l'adaptation normative des textes de loi était nécessaire. De ce fait La loi sur la cybercriminalité a modernisé le droit penal des atteintes a la défense nationale en prévoyant en son article 431-60 de la loi sur la cybercriminalité que sera coupable de trahison et punit de la perpétuité tout sénégalais qui : 1) livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que se soit un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ; 2) s'assure, par quelque moyen que se soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisé ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ; 3) détruit ou laisse détruire tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère. L'auteur de l'infraction sera condamné à perpétuité.

Cependant l'article 431-61 de la loi susvisée punit tout sénégalais ou tout étranger qui, dans l'intention de les livrer à tout pays tiers, rassemblera des renseignements, objets, documents, procédés, données ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense nationale. Cette même article réprime tout gardien, tout dépositaire par fonction ou par qualité d'un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de défense nationale, qui sans intention de trahison ou d'espionnage, l'aura : 1) détruit, soustrait, laissé détruire ou soustraire, reproduit ou fait reproduire ; 2) porté ou laissé porter à la connaissance d'une personne non qualifiée ou du public. La peine sera celle de la détention criminelle de cinq à dix ans si le gardien ou le dépositaire a agi par maladresse, imprudence, inattention, négligence ou inobservation des règlements.

Il est cependant courant aujourd'hui d'observer qu'avec l'essor des TIC, le secret de défense nationale peine à préserver sa confidentialité et est souvent l'objet d'atteintes de toutes sortes consécutives à des intrusions frauduleuses dans les systèmes et réseaux gouvernementaux par des groupes organisés. Ces textes pénal inclut de son domaine les supports immatériels de conservation du secret de défense nationale (donnée, fichiers) susceptible d'être livrés par voie électronique à une puissance ou à une organisation étrangère.

La modernisation du droit pénal des atteintes à la défense nationale a facilité l'intégration des valeurs intangibles du cyberespace « données numérisées ou fichiers informatisés » dans l'énumération légale des objets des atteintes au secret de défense nationale. La modernisation des instruments de répression dans le cadre de la lutte contre cybercriminalité ne pourra se faire sans l'amélioration de la procédure de répression.

SECTION II : L'AMELIORATION DE LA PROCEDURE DE REPRESSION DE LA CYBERCRIMINALITE

L'adaptation de la législation sénégalaise au cyberespace consistera à prendre en compte les TIC (Internet) utilisées par les cybercriminels pour la commission de leurs actes répréhensibles, seule gage de leur répression efficace par les autorités judiciaires.

Cette amélioration a été mise en œuvre par l'aménagement de la procédure pénale actuelle (paragraphe I) et par la consécration de nouvelles procédures spécifiques aux TIC (paragraphe II).

Paragraphe I : L'aménagement de la procédure pénale actuelle

Dans la conduite des investigations judiciaires tendant a la manifestation de la vérité en matière d'infractions cybercriminelles, les enquêteurs sont confrontés à de sérieuses difficultés en raison de la dématérialisation des agissements liées aux TIC .l'adaptation de la procédure pénale traditionnelle se manifeste tant dans les règles de perquisition et de saisie informatique (A) que dans la recherche de la preuve informatique (B).

A. La perquisition et la saisie informatique.

La consécration du pouvoir de perquisition dans un système informatique (1) permettrait à l'autorité judiciaire d'accéder aux données stockées dans le système et de faire la saisie des informations utiles à la manifestation de la vérité (2).

1. La perquisition informatique.

En procédure pénale classique, la juridiction d'instruction peut effectuer des perquisitions[88], c'est-à-dire une fouille dans tous les lieux où peuvent se trouver des objets dont la découverte serait utile à la manifestation de la vérité (article 85 du code de procédure pénale).[89]

Il ne fait pas de doute que l'analyse de ce texte permet de dire que le législateur sénégalais n'a entendu conférer au juge d'instruction qu'un pouvoir de perquisition dans un endroit réel « où il est possible de se rendre physiquement »[90].

Aussi, en l'état actuel de la législation, le pouvoir judiciaire de perquisition du juge dans le cyberespace sur le fondement de l'article 85 du code de procédure pénale se heurte aux conditions de régulation de la perquisition posées par l'article 86 et 87 du code de procédure pénale. En effet, la perquisition faite au domicile de l'inculpé ne peut avoir lieu de

---

[88] Voir Lexique des termes juridiques Dalloz 16 e me édition p.486

[89] Voir STEFANI (G.) : LEVASSEUR (G.) ; BOULOC (B.) Procédure pénale, Dalloz, 14ème édition, 1990, p.663.

[90] MALONGA (Y.), op-cit, p. 295.

nuit et doit s'accomplir en présence de l'inculpé et de la personne au domicile de laquelle elle a lieu. Aussi, lorsqu'elle est faite au domicile d'un tiers, elle doit être accomplie en présence de la personne chez laquelle elle doit s'effectuer.

Il est évident que le respect de ces conditions de régularité en matière d'infractions informatiques, est impossible, en raison de l'immatérialité du lieu de perquisition (cyberespace). Ainsi un aménagement du droit de la perquisition paraît nécessaire par l'extension du pouvoir judiciaire de perquisition dans le cyberespace.

L'Article 677 – 36 de la loi sur la cybercriminalité dispose que « Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire sénégalais, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial. 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 le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur».

Cependant la perquisition exige une utilité des données informatisées pour la manifestation de la vérité. Elle s'opère par un accès à un système informatique ou à une partie de celui-ci ou dans un autre système informatique.

Le système informatique peut englober à l'heure de la numérisation un nombre important de dispositifs, allant d'un ordinateur ou de ses composantes (unité centrale, disque dur) à tous les réseaux d'ordinateurs interconnectés, comme l'Internet par exemple, ou simplement designer une carte de paiement ou de crédit.

Ces données informatiques désignent en pratique toute donnée relative au texte, au son à l'image et à la vidéo susceptible d'être traitée ou conservée, par des systèmes et moyens informatiques. Il est fait obligation à l'État-Partie de prendre des mesures spécifiques pour permettre la perquisition lorsque les autorités compétentes dans la pratique les officiers police judiciaire, le Procureur de la République ou le juge d'instruction estiment nécessaire de procéder en accédant à un système informatique précis et de pouvoir étendre rapidement ladite perquisition à un autre système informatique lorsqu'elles ont des raisons de penser que les données recherchées sont stockées dans ce système ou dans une partie de celui-ci, sis sur le territoire de l'État ou en un autre lieu relevant de sa souveraineté, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système .

Il faut noter que les limites classiques en matière de perquisition prévues par les articles 86 et 87 du code penal ne sont pas prises en compte dans le cadre de la loi sur la cybercriminalité. Ces règles de forme pourraient être envisagées dans le but d'assurer, aussi complètement que possible, la protection des droits individuels et la contradiction lors des opérations de perquisitions d'un système informatique ou de simples données informatiques. Ce sont la présence nécessaire de la personne suspectée ou inculpée ou d'un représentant de son choix, à défaut, des témoins présentant des garanties de neutralité choisis par le juge

d'instruction, le procureur de la République ou l'officier de police judiciaire chargé des opérations, l'assentiment exprès et préalable de la personne chez qui la perquisition est opérée et l'établissement d'un procès verbal des opérations portant la signature de toutes les personnes qui ont assisté aux opérations. L'aménagement du droit de la saisie procède aussi du souci d'étendre les pouvoirs d'investigation des autorités judiciaires.

2. La saisie informatique.

Traditionnellement, la saisie est le résultat logique de la perquisition effectuée et qui révèle l'existence d'objets susceptibles de servir à la manifestation de la vérité. En effet, lorsque la perquisition effectuée révèle l'existence d'objets susceptibles de servir à la manifestation de la vérité, il peut être procédé à leur saisie, c'est-à-dire à la mise sous main de justice des éléments de preuve[91]. C'est ce qui résulte de l'article 88 alinéas 2 du code de procédure pénale selon lequel « tous objets et documents saisis sont immédiatement placés sous scellés ».

En outre, les scellés ne peuvent être ouverts et les documents dépouillés qu'en présence de l'inculpé assisté de son conseil, et le tiers chez lequel la saisie est opérée doit être invité à assister à l'opération[92]. Il résulte alors de ce dispositif que la saisie ne s'applique qu'aux choses corporelles à l'exclusion des choses immatérielles, telles que l'information stockée dans un système informatique. Le droit pénal sénégalais a intégré dans ses prévisions répressives l'immatérialité de certains biens dans la réglementation de la saisie.

L'Article 677 – 37 de la loi sur la cybercriminalité dispose 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 scellées.

Le juge d'instruction désigne toute personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article précédent dans le système informatique ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le juge d'instruction ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles. Lorsque la mesure prévue à l'alinéa 2 de l'article 677-37 de la présente loi n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge

---

[91] PRADEL (J.), Procédure pénale, CUJAS, 5ème Edition, 1985, n° 263.

[92] Voir article 88 alinéa 3.

d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité. Le juge d'instruction informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

A la lecture de ce texte il apparait que si le juge d'instruction découvre dans le système informatique des données stockées qui sont utiles pour la manifestation de la vérité et que la saisie du support ne paraît pas souhaitable , ce dernier procède a la Saisie par copiage sur des supports de stockage informatique pouvant être saisis et placés sous scellés , ainsi que celles qui sont nécessaires pour leur compréhension (hypothèse des données cryptées). Les données informatiques auxquelles l'accès a été autorisé par la perquisition sont saisies en vue de leur utilisation éventuelle dans des enquêtes et procédures pénales.

Le juge d'instruction désigne une personne ayant une connaissance sur les TIC pour procéder à des saisies sur un système informatique ou une partie de celui-ci ou un support permettant de stocker des données informatiques ,de réaliser et conserver une copie de ces données informatiques , de préserver l'intégrité des données informatiques stockées pertinentes et enfin de rendre inaccessibles ou enlever ces données du système informatique consulté. La preuve électronique est aussi admise par la loi dans le souci d'élargir les pouvoirs d'investigations des autorités judiciaires.

B. La preuve électronique.

L'évolution technologique a rendu nécessaire l'adaptation du système classique de preuve des infractions aussi bien au niveau de la charge de la preuve qu'au niveau des modes de preuve admissibles.

En matière répressive du fait du principe de la présomption d'innocence posé par l'article 9 de la Déclaration des Droits de l'Homme de 1789, [93] la charge de la preuve appartient à la partie poursuivante qu'est le Ministère Public, à qui il incombe de prouver l'existence de l'infraction et non à la partie poursuivie, de rapporter la preuve de son innocence[94].

Par ailleurs, la présomption d'innocence entraîne une dispense de preuve pour celui au profit de qui, elle existe et lorsqu'un doute plane sur sa culpabilité, il doit être acquitté ou relaxé. Le doute dit-on profite à l'accusé mais ce système traditionnel de preuve est difficilement transposable à la recherche de la preuve des infractions informatiques. En effet, l'évolution numérique a engendré une sophistication des technologies de l'information et de la communication, derrière laquelle se réfugient souvent les cybercriminels et la technicité

[93] « Tout homme est présumé innocent jusqu'à ce qu'il ait été déclaré coupable ».

[94] Cass. Crim. 22 mars 1966. Bull. crim. n° 106.

inhérente à la science du traitement de l'information (informatique) expose de plus en plus des données informatiques à des manipulations de toutes sortes.

L'on a pu écrire ainsi qu'à l'ère de la société de l'information « les informations traitées et les données de traitement se créent, s'effacent et se manipulent »[95]. La théorie générale des modes de preuve en matière pénale est dominée par le principe de la liberté de preuve et celui de l'intime conviction. En effet selon l'article 414 du code de procédure pénale « hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout moyen et le juge décide d'après son intime conviction ». Ainsi, tous les moyens de preuves sont admis (écrits, témoignage, aveu, perquisition, saisies ...), pourvus qu'ils aient été rapportés « au cours des débats et discutés devant le juge » (article 414 alinéa 2).

Cependant, le passage de l'analogique au numérique a précipité l'immatérialité et la volatilité des données traitées qui par essence sont propices à la manipulation des délinquants et à l'effacement des mémoires. D'où la difficulté à reconstituer le modus operandi de l'acte infractionnel par le recours aux modes traditionnels de preuve.

Le principe de l'intime conviction dispense le juge de rendre compte du chemin intellectuel par lequel il est parvenu à la certitude, il est permis au juge sénégalais de fonder sa conviction sur des preuves obtenues au moyen des TIC dès lors, qu'elles ont été régulièrement discutées devant le juge[96].

L'article 27 de la loi sur les transactions électroniques redéfinie la notion d'écrit. L'écrit, dispose ce texte, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

L'article 677-40 de la loi sur la cybercriminalité pose l'admission expresse de la preuve électronique en matière pénale. Ce texte dispos que « l'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier conformément aux dispositions de l'article 40 de la loi sur les transactions électroniques ». En effet la copie ou toute autre reproduction d'actes passés par voie électronique à la même force probante que l'acte lui-même lorsqu'elle est certifiée conforme par des organismes agréés par l'Agence de l'Informatique de l'Etat (ADIE) selon des règles définies par décret. La certification donne lieu, le cas échéant, à la délivrance d'un certificat de conformité[97].

Cependant les mécanismes de sécurisation des transactions électroniques sont posés par les articles 36 à 42 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques. Ces articles posent le principe de l'équivalence entre l'écrit traditionnel et l'écrit électronique et admet l'écrit sous forme électronique en facturation au même titre que l'écrit sur support

---

[95] CASILE (J-F). Plaidoyer en faveur d'aménagements de la preuve de l'infraction informatique. RSC. janvier-mars 2004. P. 65

[96] Voir DIOUF (Nd.). op-cit. p. 31.

[97] Art 40 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques

papier. Certaines conditions sont nécessaires pour l'admission de la preuve électronique, il s'agit de l'identifiée la personne dont il émane et l'établissement et la conservation de la preuve dans des conditions de nature à en garantir l'intégrité. La conservation des documents sous forme électronique doit se faire pendant une période de dix (10) ans. La copie de toute reproduction d'acte électronique a la même force probante que l'acte lui-même lorsqu'elle est certifiée conforme par les organismes agrées par l'ADIE.

On est obligé cependant d'admettre que le juge ne peut utiliser comme fondement de sa décision que les preuves régulièrement obtenues, car « si la preuve est libre, son administration ne l'est pas »[98]. C'est ce qui explique que parfois, les juges ont tendance à rejeter les preuves obtenues au moyen de procédés qui portent atteinte aux droits fondamentaux de la personne humaine effet, même si le recours aux procédés électronique est admis, c'est sous réserve que les preuves soient légalement obtenues. Dans ces conditions une preuve obtenue au moyen d'une intrusion dans un système informatique en violation des règles qui sont en vigueur doit être purement et simplement rejetées des débats. En effet, le principe de loyauté qui, comme le principe de l'égalité encadre la recherche et l'administration de la preuve, interdit la production de preuves obtenues par la ruse et le stratagème qui sont considères comme des procédés contraires a la dignité de la Justice[99].

Il faut préciser que le droit des systèmes de paiement des Etats Membres de l'UEMOA a consacré dans les articles 17 à 20 du Règlement n° 15 du 19 septembre 2002, l'admission de la preuve électronique, mais ce nouveau dispositif a une portée limitée, puisque ne s'appliquant qu'à « toute information, de quelque nature qu'elle soit, prenant la forme d'un message de données utilisées dans les transactions bancaires et financières et dans tous les systèmes de paiement »[100].

En définitive, l'admission de la preuve électronique est un moyen efficient pour une lutte efficace contre la cybercriminalité. Néanmoins pour lutter contre cette nouvelle forme de délinquance, il faut instaurer de nouvelles procédures qui sont spécifiques aux TIC.

Paragraphe II : La consécration de nouvelles procédures spécifiques aux TIC

Dans le cadre de la lutte contre la cybercriminalité, le législateur sénégalais a perçu la nécessité de concevoir de nouvelles procédures spécifiques aux TIC par la conservation rapide des données informatiques archivées et l'interception de données informatisées (A) et la procédure spécifique aux infractions liées aux données à caractère personnel (B).

A. La conservation rapide des données informatiques archivées et

[98] V. Blondet, ruses et Artifices, dans l'enquête de police – JCP 1958. I - n° 14719

[99] Ndiaw DIOUF, Procédure Pénale et TIC.

[100] Voir article 17 du Règlement n°15 CM/UEMOA/ du 19 septembre 2002 relatif aux systèmes de paiement dans les Etats membres de l'UEMOA.

l'interception de données informatisées.

La loi sur la cybercriminalité permet d'étudier ces nouvelles procédures à savoir la conservation rapide des données informatiques archivées (1) et l'interception de données informatisées (2).

1. La conservation rapide des données informatiques archivées.

Il importe d'établir une distinction entre la « conservation des données » et l'« archivage des données ». Les deux expressions ont des sens voisins dans le langage courant, mais différents en informatique. Conserver des données, c'est garder des données qui existent déjà sous une forme stockée et en les protégeant contre tout ce qui pourrait en altérer ou en dégrader la qualité ou l'état actuel. Archiver des données, c'est garder en sa possession pour l'avenir des données qui sont en cours de production. L'archivage des données implique l'accumulation des données dans le présent et la garde ou la possession de ces données en prévision d'une période future. L'archivage des données est le processus de stockage des données. En revanche, la conservation des données est l'activité qui garantit leur sécurité et leur sûreté[101].

La conservation rapide des données informatiques archivées est prévues par l' article 677 – 35 de la loi portant sur la cybercriminalité qui prévoit que « si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées[102] 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 une 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 ».

En effet lorsqu'il ya risques de perte ou de modification des données informatisées archivées dans un système informatique, il est fait Injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pour la bonne marche des investigations judiciaires et d'en garder le secret. Le délai de conservation des données est de deux (2) ans au maximum. Mais toutefois la conservation doit se faire si les nécessités de l'information l'exigent.

La conservation des données constitue un pouvoir ou une procédure juridique entièrement nouvelle en droit interne. Il s'agit d'un nouvel instrument d'enquête important dans la lutte contre la criminalité informatique et en relation avec l'ordinateur, en particulier contre les infractions commises par le biais de l'Internet.

---

[101] Conseil de l'Europe - Rapport explicatif sur la Convention sur la cybercriminalité (STE No. 185)

[102] Art 431-7 de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

Premièrement, en raison de leur volatilité, les données informatiques sont faciles à manipuler et à modifier. Ainsi, il est facile de perdre des éléments prouvant une infraction si les pratiques de traitement et de stockage manquent de rigueur, si les données sont intentionnellement manipulées ou effacées pour détruire tout élément de preuve ou si elles sont effacées dans le cadre d'opérations normales d'effacement de données qui n'ont plus à être conservées. L'un des moyens de préserver l'intégrité des données consiste pour les autorités compétentes à opérer des perquisitions ou à accéder d'une autre manière aux données et à saisir les données ou à se les procurer d'une autre manière. Toutefois, lorsque le gardien des données est digne de confiance, l'intégrité des données peut être garantie plus rapidement au moyen d'une injonction de conserver les données. Une injonction d'avoir à conserver les données peut être moins perturbatrice pour les activités et moins préjudiciable à la réputation d'une entreprise honnête qu'une opération de perquisition de ses locaux aux fins de saisie.

Deuxièmement, les infractions informatiques et en relation avec l'ordinateur sont très souvent commises au moyen de la transmission de communications par le biais du système informatique. Ces communications peuvent contenir un contenu illicite, tel que la pornographie enfantine, des virus informatiques ou d'autres instructions qui portent atteinte aux données ou entravent le bon fonctionnement du système informatique, ou des éléments tendant à prouver que d'autres infractions ont été commises, par exemple des cas de trafic de stupéfiants ou d'escroquerie. L'identification de la source ou de la destination de ces communications antérieures peut aider à établir l'identité des auteurs de ces infractions. Pour déterminer la source ou la destination de ces communications, il faut disposer de données relatives au trafic concernant ces communications antérieures.

Troisièmement, lorsque ces communications présentent un contenu illicite ou la preuve d'agissements criminels et que des copies de ces communications sont archivées par les fournisseurs de services (de courrier électronique, par exemple), la conservation de ces communications est importante afin de ne pas perdre des éléments de preuve essentiels. L'obtention de copies de ces communications antérieures (par exemple de courriers stockés qui ont été envoyés ou reçus) peut révéler que des infractions ont été commises.

Le pouvoir de conservation rapide des données informatiques doit permettre de faire face à ces problèmes. Les problèmes peuvent aussi être résolus grâce à l'interception des données informatisées.

2. l'interception des données informatiques

L'interception peut être définie comme « le fait d'écouter ou d'enregistrer des communications privées, fonctions ou données d'un ordinateur dans le but d'en prendre connaissance pour en appréhender le sens, l'objet ou la substance »[103]. Ainsi, l'interception peut s'appliquer à des communications de nature privée comme cela est bien souvent le cas par exemple pour les écoutes téléphoniques ou les interceptions de correspondance postales

[103] Pour une définition de l'interception, voir Pierre Trudel, Droit du cyberespace, op. cit., note 1, p. 10-8.

effectuées par les autorités policières ou, encore, le fait par ces mêmes autorités de prendre connaissance des fonctions d'un ordinateur, par exemple du courrier électronique qu'il dessert, afin d'en appréhender le contenu[104].

Aux termes de l'article 677 – 38 de la loi sur la cybercriminalité « 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 ». Cet article habilite le juge d'instruction soit à utiliser les moyens techniques appropriés en vue de la collecte ou de l'enregistrement en temps réel des données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique.

Il peut aussi 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 les données informatisées. Il est fait obligation pour le fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

Il faut noter que l'interception de données informatisées concerne seulement les données relatives au contenu de communications spécifiques (par opposition aux données de connexion ou de trafic), transmises au moyen d'un système informatique. Néanmoins l'officier de police judiciaire peut par délégation judiciaire[105] procéder aux actes de conservation rapide des données informatiques archivées, à la perquisition et la saisie informatique et a l'interception des données informatisées, ceux en vertu de l'article 677-39 de la loi précitée. Cependant une procédure spécifique aux infractions liées aux données à caractère personnel est mise en place.

B. La procédure spécifique aux infractions liées aux données caractère personnel

La numérisation du réseau a crée de nouveaux risque pour les données à caractère personnel qui sont de plus en plus l'objet de manipulation, de collecte, de détournement et de traitements illicites, violant l'intimité de la vie privée garantie par l'article 13 de la Constitution du 22 janvier 2001.

---

[104] Sur l'interception de communications privées, voir Pierre Trudel, *op. cit.*, note 1, p.10-8 / 10-9 / 10-10.

[105] Art 142 et suivants du Code de Procédure pénale sénégalaise, p. 91 et suivants

Ainsi le législateur sénégalais , dans le soucis d'assurer la protection générale des droits et libertés fondamentaux de la personne humaine, a crée la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données a caractère personnel .Cette loi en son article 4 .6 définie les données à caractère personnel comme « toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique » Ainsi cette notion renvoie à toute information concernant une personne physique identifiée ou identifiable par un procédé technique quelconque[106].

Aux termes de l'article 677 - 41 de la loi sur la cybercriminalité « dans les cas prévus aux articles 431-17 à 431-30 de la présente loi, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission des Données Personnelles (CDP) sont habilités à constater l'effacement de ces données ».

Les articles 431-17 à 431-30 cités sont relatives aux atteintes spécifiques aux droits de la personne au regard du traitement des données a caractère personnel.

Cette nouvelle procédure spécifique aux infractions liées aux données à caractère personnel permet d'ordonner l'effacement des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction. Cette mesure est ordonnée par l'autorité judicaire, en cas d'infractions aux données à caractère personnel. Cet article donne une habilitation légale aux membres et aux agents de la Commission des Données Personnelles [107](CDP) pour constater l'effacement des données personnelles.

L'article 677-42 de la loi sur la cybercriminalité « Le procureur de la République avise le président de la Commission des Données Personnelles de toutes les poursuites relatives aux infractions aux présentes dispositions et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'audience de jugement. La juridiction d'instruction ou de jugement peut appeler le président de la Commission des Données Personnelles ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Le juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie ». A la lecture de cet article le Ministère Public à l'obligation d'informer le Président de la Commission des Données Personnelles[108] des poursuites liées aux infractions relatives aux données à caractère personnel et le cas échéant, des suites a leurs données. Le Ministère Public l'informe de la date de l'audience de jugement des infractions relatives aux données à caractère personnel.

---

[106] Sur la distinction entre données créatrices et données nominatives, voir NICOLEAU (J.), la protection des données sur les autoroutes de l'information. D.S 1986 , chron. p.111.

[107] Voir la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel

[108] La loi n°2008-12 du 25 janvier 2008 portant sur la protection des données a caractère personnel, chap.II.

Le Président de la Commission des Données Personnelles ou son représentant ont la faculté de déposer ses observations ou à les développer oralement à l'audience. Cependant la main levée de la saisie peut être ordonnée d'office par le juge ou a la demande de la personne intéressée à tout moment de la procédure.

En définitive, la stratégie d'adaptation du droit pénal sénégalais à l'évolution numérique procède sans nul doute du souci de garantir la répression devant le juge des agissements facilités par les TIC.

L'élaboration d'une stratégie méthodique de modernisation de l'arsenal répressif sénégalais constitue un instrument sûr, assurant des réponses pénales adaptées au phénomène cybercriminel. Mais cette modernisation du cadre juridique nécessite la mise en œuvre pratique de la lutte contre la cybercriminalité.

CHAPITREII : LA MISE EN ŒUVRE PRATIQUE DE LA LUTTE CONTRE LA CYBERCRIMINALITE

L'essor des nouvelles technologies de l'information et de la Communication (NTIC) a engendré un changement d'espace qui s'est traduit par le dépassement de l'espace physique matérialisé par les frontières des nations souveraines et l'avènement de l'environnement cyber spatial. Cependant, la mise en œuvre pratique de la lutte contre la cybercriminalité est incontournable pour mener à bien ce combat.

Mais concrètement, la lutte contre la cybercriminalité se heurte à un certain nombre de difficultés (section I), mais ces dernières ne sont pas insurmontables. En effet, des solutions peuvent être adoptées pour y remédier (section II).

SECTION I : LES DIFFICULTES RENCONTREES DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

Les obstacles à la lutte contre la cybercriminalité résident dans le fait que certaines difficultés sont liées au caractère transfrontalier des infractions cybercriminelles (paragraphe 1) et d'autres sont liées à la spécialisation et à l'équipement technologique (paragraphe 2).

Paragraphe I : Les difficultés liées au caractère transfrontalier des infractions cybercriminelles

Dans la conduite des investigations, les autorités judiciaires sénégalaises saisies du contentieux cybercriminel se heurtent à l'immatérialité des comportements liés aux TIC qui se déploient dans un environnement transnational, se jouant des frontières étatiques. Le caractère transfrontalier de la cybercriminalité est à l'origine de nombreux problèmes qui sont liés à la compétence des autorités policières et judiciaires (A) et à la souveraineté des Etats (B).

A. Les problèmes liés à la compétence des autorités policières et judiciaires

La cybercriminalité est une infraction transfrontalière étant donné qu'il n'y a pas de frontières dans le monde immatériel. L'espace internet ignore la répartition territoriale des compétences entre les autorités judiciaires tant sur le plan national qu'international.

Sur le plan national, les autorités chargées des enquêtes et qui seront amenées à agir dans le cadre d'infractions cybercriminelles vont rencontrer d'énormes difficultés surtout sur le plan de la compétence territoriale telle que définie par les textes.

La compétence territoriale est l'aptitude d'une juridiction pénale à connaitre d'une infraction en fonction d'une circonstance de lieu. En effet aux termes de l'article 17 du Code de procédure pénale (CPP) : « les officiers de police judiciaire ont compétence dans les limites territoriales où ils exercent leurs fonctions habituelles. En cas de nécessité, ils peuvent poursuivre leurs investigations hors de ces limites à charge d'en rendre compte au Procureur de la république territorialement compétent ».

A la lecture de cet article, il ressort que les officiers de police judiciaire (OPJ) chargées de l'enquête ne peuvent agir en dehors de leur ressort territorial qu'en cas de nécessité et après en avoir informé le Procureur de la République. Mais, il faut dire que cette extension est limitée au cas où les OPJ exécutent une commission rogatoire[109], ou dans le cadre des délits flagrants[110].

Les OPJ sont, le plus souvent, les premiers sur le terrain dès qu'une infraction a été dénoncée. Dans l'hypothèse de faits répréhensibles de cybercriminalité, il est nécessaire que les premiers actes d'enquête soient rapides et que l'OPJ, qui va poser ces actes, puisse suivre les traces de ces faits où qu'ils se trouvent, donc même au delà des limites du ressort territorial de l'OPJ. En effet, les délinquants peuvent facilement se servir d'un logiciel serveur ou du courrier électronique afin d'enregistrer dans un ordinateur éloigné, éventuellement hors du ressort territorial de l'autorité en charge de l'enquête, il faut prendre en considération la célérité avec laquelle une donnée informatique peut être déplacée. L'article 17 susvisé ne permet cette extension qu'en cas de nécessité alors que, vu le caractère transfrontalier de la cybercriminalité, il est nécessaire de permettre aux OPJ de faire leur enquête sur toute l'étendue du territoire.

L'article 40 du CPP sénégalais prévoit que la compétence territoriale du juge d'instruction coïncide avec celle du tribunal dans lequel il a été nommé. L'implication de cette disposition est que le juge d'instruction ne peut instruire que dans le ressort territorial du tribunal dont il relève. Des exceptions sont prévues par l'article 84 du CPP, mais seulement dans le ressort des tribunaux limitrophes et après avis au Procureur de la République. Le juge d'instruction peut aussi procéder à des actes d'instruction dans tout le ressort de la Cour d'appel dont relève le tribunal dans lequel il exerce ses fonctions, à condition d'obtenir une autorisation du président de la chambre d'accusation de ladite cour.

Il faut cependant déplorer le fait que les textes n'aient pas étendu cette possibilité du juge d'instruction sur toute l'étendue du territoire national. En pratique, toutes les mesures nécessaires à la manifestation de la vérité comme les perquisitions et les saisies sont posées par la police judiciaire, la justification étant que c'est cette dernière qui se transporte généralement, et sans désemparer, sur le terrain avec le souci de rassembler et préserver tous les indices susceptibles d'aider à la manifestation de la vérité. La volatilité, l'immatérialité et l'anonymat de la cybercriminalité font que les autorités judiciaires doivent effectuer tous les actes nécessaires à la manifestation de la vérité sans aucune contrainte sur toute l'étendue du territoire national.

La répartition territoriale des compétences entre les autorités de police ou du pouvoir judiciaire prévue par le CPP constitue un frein aux investigations et notamment à cette lutte contre la cybercriminalité.

---

[109] Art 142 à 148 du Code de Procédure Pénale.

[110] Art 45 et suivants du Code de Procédure Pénale.

Sur le plan international, les possibilités de transmission de données d'un lieu à un autre ou de diffusion de ces données dans le monde entier pose problème lorsqu'il faut suivre les traces des infractions qui empruntent l'internationalité de ces transmissions. Les frontières physiques des Etats nationaux ne constituent pas un obstacle.

En effet, l'obstacle existe pour les services qui sont chargés de lutter contre la criminalité dont les compétences s'arrêtent aux frontières du pays. Dans le cas de systèmes informatiques liés entre eux, il arrive que l'enquête soit étendue à d'autres systèmes situés dans d'autres pays que ceux où la recherche a physiquement lieu, entravant ainsi les mesures d'enquête. Il ne s'agira pas seulement de pouvoir procéder aux dites mesures hors des frontières nationales mais il faudra encore accomplir ces actes aussi rapidement que possible.

Des procédures classiques de coopération judiciaire bilatérale ou multilatérale instaurent des procédures d'entraide comme les commissions rogatoires internationales dont la pratique a révélé une lenteur incompatible avec les investigations à mener sur le réseau Internet et sur les autres modes de commission des infractions cybercriminelles.

Par commission rogatoire internationale, il faut entendre une mission donnée par un juge à toute autorité judiciaire relevant d'un autre Etat de procéder en son nom à des mesures d'instruction ou à d'autres actes judiciaires[111]. La commission rogatoire est donc la procédure classique usitée lorsqu'un Etat requiert d'un autre, sur le territoire de ce dernier des actes nécessaires à la manifestation de la vérité. Cependant il faut souligner que l'exécution des commissions rogatoires internationales prend beaucoup de temps, au regard des voies qu'elles doivent emprunter, à l'aller comme au retour. En effet, il est très souvent prescrit que la transmission de ces procédures se fasse par la voie diplomatique.

Ainsi l'usage des commissions rogatoires laisse aux personnes concernées par la mesure (ou même automatiquement à leurs systèmes informatiques) suffisamment de temps pour faire disparaître instantanément les données via les canaux de télécommunication et ce a cause du caractère transfrontalier de la cybercriminalité.

A côté des problèmes tirés de la limitation textuelle de la compétence des autorités judiciaires et de la barrière frontalière des Etats ainsi que de la lenteur de certaines procédures nationales et internationales, subsistent d'autres entraves à la manifestation de la vérité liées à la souveraineté des Etats.

B. Les problèmes liés à la souveraineté des Etats

Le caractère transnational des comportements liés aux TIC a désorganisé les repères des règles de compétence internationale des juridictions répressives, aussi bien pour les agissements commis au Sénégal que pour ceux réalisés à l'étranger, entrainant ainsi des conflits de juridiction[112].

---

[111] Voir Lexique des termes juridiques. Dalloz. 16e édition. p 138.

[112] Ibid . p 156.

Internet offre l'occasion à des personnes d'émettre à partir d'un serveur localisé au Sénégal des informations ou affirmations contraires à l'ordre public, susceptibles de causer un préjudice à des personnes établies à l'étranger.

Ainsi de tels procédés relèvent bien de la compétence législative de la loi sénégalaise en raison du principe de la territorialité de la loi pénale qui s'applique à toutes les infractions commises au Sénégal.

Concernant les infractions commises au Sénégal, l'article 668 du CPP assimile à une infraction commise au Sénégal, « toute infraction dont un acte caractérisant un des éléments constitutifs a été accompli au Sénégal ». De même, l'article 665 du CPP prévoit que relève de la compétence des juridictions sénégalaises, l'acte de complicité accompli au Sénégal par un sénégalais ou un étranger à condition que le crime ou délit « ait été constaté par une décision définitive de la juridiction étrangère ».

Mais, la mise en œuvre de ce système de compétence internationale des juridictions sénégalaises entraine des difficultés en matière de cybercriminalité.

En effet, il peut arriver que la compétence juridictionnelle soit revendiquée par plusieurs Etats en même temps. Par exemple, lorsque des messages illicites disponibles sur Internet sont émis au Sénégal alors qu'un acte de complicité de cette infraction est accompli en France, les juridictions tant françaises que sénégalaises peuvent en connaître. Et cette situation risque de se compliquer dans l'hypothèse où un autre Etat dispose des mêmes règles de compétence internationale.

La transnationalité des agissements cybercriminels entraine des conflits positifs[113] de compétence juridictionnelle qui ne facilite pas le jugement de la cybercriminalité.

Un aménagement des règles de compétence dans le cadre de la coopération internationale s'avère nécessaire en vue de régler les conflits de compétence.

En ce qui concerne les infractions commises à l'étranger, l'article 664 alinéa 1er du CPP dispose que les juridictions sénégalaises sont compétentes pour les juger si elles n'ont pas été définitivement jugée à l'étranger.

Mais, l'internationalisation des infractions suscitée par le développement des réseaux numériques a chamboulé les systèmes de compétence, en les rendant inappropriés lorsque l'Etat dans lequel les infractions cybercriminelles sont commises applique le même système de compétence. Et ceci sera à l'origine d'un nouveau conflit positif de compétence nécessitant un aménagement législatif puisque la juridiction étrangère peut légitimement retenir sa compétence. C'est dans ce sens que les Etats membres du Conseil de l'Europe, conscients des problèmes de compétence que cela entraine, se sont engagés à redéfinir les règles de compétence internationale.

---

[113] Ibid, p156.

Ils ont adopté les mesures se révélant nécessaires pour établir leur compétence juridictionnelle à l'égard de toute infraction pénale lorsqu'elle est commise sur leur territoire ou par un de leurs ressortissants si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence d'aucun Etat ; il en est de même lorsque l'auteur présumé de l'infraction est présent sur leur territoire et ne peut être extradé vers un autre pays.

Dans le souci d'éviter les conflits positifs de compétence, devenus fréquents en raison de la transnationalité des agissements liés aux TIC, le législateur européen a prévu que « lorsque plusieurs parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la convention, les parties concernées se concertent lorsque cela est opportun, afin de décider quelle est celle qui est mieux à même d'exercer les poursuites ».[114]

La convention sur la cybercriminalité donne de simples recommandations aux États membres devant permettre à ces derniers d'édicter des règles législatives nécessaires pour établir leur compétence juridictionnelle, de la même manière qu'il a procédé par ailleurs pour le contenu matériel en ses dispositions afférentes aux délits informatiques.

En effet, Il résulte de l'article 22 de la Convention de Budapest que chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente convention, lorsque l'infraction est commise sur son territoire, à bord d'un navire battant pavillon de cette partie, à bord d'un aéronef immatriculé selon les lois de cette partie ou par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

Il ressort de ces indications au moins deux critères de détermination de la compétence juridictionnelle que sont la règle de compétence territoriale qui dépend du seul lien avec le territoire et la règle de compétence personnelle active qui résulte du lien de nationalité[115].

Néanmoins, certaines difficultés sont liées à la faiblesse des moyens déployés pour la lutte contre la cybercriminalité.

Paragraphe II : Les difficultés liées au manque de moyens des autorités chargées de la lutte contre la cybercriminalité

Les intervenants dans la lutte contre la cybercriminalité sont confrontés à des problèmes de spécialisation (A) et d'équipement technologique (B).

---

[114] Sur cette question, voir Elhadji Mame GNING, Cybercriminalité et poursuites pénales : l'expérience européenne, Africajuris, n° 12 du 18 au 24 avril 2002, p.4.

[115] Elhadj Mame GNING « L'organisation des poursuites internes , le Projet de convention européenne sur la criminalité dans le cyberespace », www.lex-electronica.org.

A. Le manque de spécialisation des acteurs de la lutte contre la cybercriminalité

Internet de par sa nature et sa conception favorise la commission de crimes et de délits. Or, les mesures de sécurité mises en place tendent à protéger un environnement donné dans un contexte particulier, mais ne peuvent aucunement empêcher la réalisation d'activités criminelles.

A l'heure actuelle, la cybercriminalité est mal maîtrisée, les raisons de cette situation sont notamment liées aux caractéristiques du cyber crime (capacité à être automatisé, savoir-faire embarqué dans le logiciel, réalisation à distance), à la possibilité offerte au cybercriminel d'usurper facilement et sans risque excessif l'identité d'utilisateurs légitimes, ruinant par la même la capacité de la justice à identifier les auteurs réels d'une infraction, à la détermination des compétences pour réaliser une enquête, à la pénurie de ressources humaines et matérielles au sein des services chargés de la répression des crimes et délits informatiques, au caractère transnational de la cybercriminalité qui nécessite des recours fréquents à la coopération et à l'entraide judiciaire internationale. Cette dernière implique des contraintes de temps non compatibles avec la rapidité d'exécution des agressions et les besoins de reprise immédiate des systèmes informatiques concernés par les cybers attaques, à la difficulté à qualifier les faits au regard de certaines législations pénales, à la nature mal définie et à la volatilité de la plupart des preuves informatiques.

Pour toutes ces causes, le système judiciaire dans le contexte de l'Internet, n'est pas efficace et ne peut effectuer pleinement sa mission de régulation sociale. En effet, les comportements antisociaux comme l'espionnage économique par exemple, qu'autorise l'Internet, comme d'ailleurs toutes les infractions non réprimées, apportent un gain immédiat et sans contrepartie à leurs auteurs. Cela contribue à déstabiliser le marché et perturbe ainsi le bon fonctionnement de l'économie.

La cybercriminalité, en rendant non-équitables les rapports entre les différents acteurs, introduit ainsi un facteur déséquilibrant majeur, qui rend toute idée d'autorégulation utopique. Par ailleurs, ce n'est pas nécessairement par absence de loi que le crime informatique est peu ou mal réprimé. Un certain nombre de crimes et de délits informatiques sont déjà qualifiés par le biais des législations pénales existantes.

Renforcer la législation n'est donc pas forcément une mesure adaptée voire suffisante, dans la mesure où, d'une part, les moyens de l'appliquer manquent, et d'autre part, les caractéristiques mêmes du crime empêchent la justice d'opérer. En effet, quelle peut être l'utilité d'une loi extrêmement restrictive si la justice n'est pas en mesure de traiter les preuves qui permettent de mener un procès à son terme et de sanctionner les auteurs de comportements criminels ? La législation n'est plus efficace lorsque les malveillants ont le sentiment d'agir en toute impunité. Face à un tel dysfonctionnement, les Etats doivent prendre des mesures efficaces pour sauvegarder leur légitimité.

Le manque de compétences spécialisées est un problème pesant chez la police judiciaire qui a vocation à mener des enquêtes, à perquisitionner et à procéder à des saisies en ligne, au cours des investigations qu'elle sera amenée à faire sur la commission d'infractions

cybercriminelles. Elle doit, dans ce genre de situation, agir vite et même très vite, les indices et autres éléments de preuve à recueillir sur le réseau sont très volatiles en raison même de la nature de celle-ci.

La formation tant initiale que continue dont elle bénéficie ne prend que sporadiquement et sommairement en compte les données de la cybercriminalité. On pourrait penser que les autorités politiques des Etats ignorent la réalité cybercriminelle ou la minimisent. En réalité, le problème est que le coût financier de la formation et de l'acquisition du matériel nécessaire à cette fin est exorbitant, or les Etats sont pauvres et sont dans une logique ou tout est prioritaire.

Il reste à savoir si la police judiciaire dispose d'officiers ou d'agents de police judiciaire spécialisés pour la conduite des investigations cybercriminelles. La réponse est sensiblement négative, il n'y a pas jusque-là de cas de cyber perquisition et de saisie en ligne ayant donné lieu de preuve au juge, alors que la cybercriminalité est malheureusement une réalité quotidienne au Sénégal.

La police sénégalaise organise à cet effet des formations régulières dans le domaine de la cybercriminalité. Des stages sont organisés fréquemment pendant lesquels des experts forment ou perfectionnent les savoirs des OPJ. L'objectif est de donner une connaissance solide de cette forme de criminalité qui est en évolution constante, et de familiariser les officiers avec les modus operandi des réseaux locaux et internationaux. Toutefois, les infractions de ce type, qui sont le plus souvent commises en langue anglaise, nécessitent la formation des enquêteurs pour la maîtrise de ce moyen de communication. Néanmoins, certains policiers ont suivi des formations dans le domaine de la cybercriminalité pour pouvoir être à la hauteur de la progression du phénomène.

Ceux qui sont formés transmettront ensuite leur savoir à d'autres policiers qui viendront à tour de rôle faire des stages pratiques d'information. La direction générale de la sûreté nationale organise par ailleurs régulièrement des stages de formation. De même, la direction de l'automatisation du fichier, rattachée au ministère de l'intérieur et composée d'ingénieurs et d'informaticiens, familiarise le policier de base à l'outil informatique.

Mais, avec ces formations la police sénégalaise n'est pas à même d'endiguer totalement la cybercriminalité. Elle n'est pas opérationnelle à 100% et connaît d'ailleurs des problèmes de logistique car les connections Internet ne sont pas toujours très bonnes. Il y a aussi la barrière de la langue parce que la plupart des cybercriminels sont originaires de pays anglophones, or les policiers sénégalais ne parlent pas tous anglais. Un problème que les autorités essayent de résorber. Mais, globalement, les policiers, surtout les cadres de Dakar, sont bien formés. Les petits commissariats d'arrondissement qui n'ont pas d'expertise se rabattent sur la Brigade de lutte contre la criminalité (BLC) lorsqu'ils ont une affaire de cybercriminalité et cette dernière leur apporte l'aide nécessaire pour qu'ils puissent poursuivre leur enquête.

On pourrait, certes, penser pallier ces carences de la police judiciaire par la possibilité de recourir à des tiers intervenants techniquement qualifiés et outillés. En effet, en enquête flagrante comme en enquête préliminaire, les pouvoirs coercitifs dont sont investis les

services répressifs leur permettent de requérir toutes personnes qualifiées s'il y a lieu, afin de procéder à des constatations ou à des examens techniques.

Concrètement, la plupart des juges et des juristes manquent de compétences juridiques et techniques en matière de droit applicable aux nouvelles technologies. L'Internet est un phénomène innovant, comprenant des problèmes spécifiques, qu'il semble parfois difficile d'appréhender sans connaissance préalable de la spécificité du Réseau. Les moyens juridiques classiques de règlement des litiges sont souvent insatisfaisants. En effet, les solutions positives applicables et efficaces semblent être à définir aussi bien par la jurisprudence que par la doctrine. Mais, il n'en demeure pas moins que les moyens et ressources mis à la disposition des juridictions classiques pour venir à bout de ces problèmes font souvent cruellement défaut.

La question de l'inadéquation de la formation des acteurs par rapport à la spécificité et à la technicité de la cybercriminalité interpelle sur la nécessité d'améliorer la formation des acteurs mais aussi la spécialisation de ceux-ci en vue de leur permettre de lutter efficacement contre ce nouveau phénomène qu'est la délinquance numérique.

C'est dans ce sens que l'Agence de l'Informatique de l'ETAT (ADIE) a organisé de nombreux séminaires de formation des acteurs intervenant dans cette lutte contre la cybercriminalité.

En effet, les policiers, les gendarmes et les magistrats doivent bénéficier dès leur formation initiale et tout au long de leur parcours professionnel, d'une sensibilisation à la cybercriminalité. La lutte contre la cybercriminalité ne doit pas être un champ d'action réservé à des spécialistes. Elle concerne l'ensemble des acteurs impliqués dans cette lutte.

Il convient de développer les connaissances techniques et juridiques des enquêteurs sur les aspects législatifs récents et sur l'évolution des technologies en particulier, d'introduire dans la formation des modules de techniques élémentaires pour traiter les infractions classiques et de préciser les conduites à tenir, de la réception des plaintes aux premières investigations jusqu'au jugement pour les infractions plus spécifiques liées à la criminalité informatique.

Il s'agit donc de renforcer le savoir-faire technique des services d'investigation dans le domaine des technologies de pointe et de faciliter ainsi leurs recherches, notamment grâce à une coopération entre les services opérationnels de la police et de la gendarmerie. Néanmoins, des problèmes d'équipement technologique constituent une entrave à l'efficacité de cette lutte contre la cybercriminalité.

B. Les problèmes d'équipement technologique

Les technologies de l'information occupent une position duale au sein de la criminalité, à la fois en tant qu'objectif et moyen, constituant une cible pour les délinquants ou leur fournissant un outil efficace pour l'accomplissement de leurs méfaits.

Les progrès constants que connaissent ces technologies sont autant d'occasions pour la cybercriminalité d'échapper aux forces de l'ordre. En effet, la vitesse d'exécution des crimes et délits a augmenté avec une dissimulation des traces.

Agir sur le réseau suppose que les services de police disposent d'une connexion à Internet. Sur le plan de la couverture, on pourrait même dire que certaines parties du territoire ne sont même pas électrifiées[116]. A cela s'ajoute le fait que bon nombre de services de police ne sont pas encore, en cette ère d'Internet, dotés d'outils informatiques[117].

De ce fait, l'immatérialité du réseau rend délicate l'application des règles positives de perquisitions et de saisies relatives aux infractions du cyber crime. Intangibles, les preuves ne se prêtent pas à une collecte facile, volatile et éphémère, leur collecte judicieuse commande de se passer des règles limitatives du temps des investigations.

Cependant, la police judiciaire doit aussi savoir collecter ces informations à la mesure de l'immatérialité d'Internet. Certes, pour un CD-ROM ou un ordinateur tout entier à saisir, la technique sera sensiblement similaire à la saisie d'un couteau ou d'un lingot d'or, moyennant des mesures très précautionneuses à utiliser pour ne pas abîmer le contenu. Il en va différemment lorsqu'il s'agit de perquisitionner dans l'espace même du réseau. Ce qui était simple dans l'espace physique, sera compliqué dans le monde immatériel.

En effet, la police judiciaire renferme tout un ensemble lourd et cosmopolite d'intervenants, laissant supposer que tous ne pourraient avoir les compétences techniques et les outils nécessaires aux investigations et plus particulièrement aux perquisitions et saisies sur le réseau.

Les services de police et de gendarmerie ne doivent pas se laisser distancer dans la course aux technologies de plus en plus performantes et sophistiquées. Ils doivent au moins s'adapter aux évolutions de la cybercriminalité, au mieux devancer les éventuels détournements ou usages déviants de ces technologies.

A cet effet, deux principes doivent être respectés : disponibilité et primeur de l'information. La somme des connaissances requises pour résoudre certains problèmes techniques ne peut être maîtrisée en permanence par tous les enquêteurs, ce qui implique un nécessaire partage de l'information technique.

Par ailleurs, les services de police et de gendarmerie doivent être informés de l'état de l'art, à la fois pour bénéficier des dernières avancées et pour devancer d'éventuelles menaces à venir. . Toutefois, les difficultés décelées dans la lutte contre la cybercriminalité peuvent trouver des remèdes.

---

[116] www .osiris.sn

[117] Pour le cas africain. M. JENSEN, « L'Internet Africain : un état des lieux », <http://www3.sn.apc.org/africa/afstat.htm>

SECTION II : LES SOLUTIONS AUX DIFFICULTES ENTRAVANT LA LUTTE CONTRE LA CYBERCRIMINALITE

En raison du caractère transfrontalier de la cybercriminalité, l'harmonisation des législations nationales s'avère nécessaire pour que la lutte contre cette nouvelle forme de criminalité ne soit pas un vœu pieux.

La question de la réaction contre ce phénomène cybercriminel est abordée par plusieurs instances communautaires et internationales constituées en vue de l'adoption d'instruments juridiques assurant une répression méthodique. La réussite de cette lutte passe nécessairement par la nécessité d'harmonisation des législations nationales (paragraphe I) et le renforcement des capacités et le recours à la régulation (paragraphe II).

Paragraphe I : La nécessité d'harmonisation des législations nationales

Pour assurer une lutte efficace contre cette forme de délinquance numérique, la nécessité s'impose aux Etats de créer un instrument régional de lutte contre la cybercriminalité (A) et d'inviter les Etats à une coopération juridique et institutionnelle internationale (B).

A. Un instrument régional de lutte contre la cybercriminalité

Le cadre juridique et politique de la société de l'information en Afrique de l'Ouest a fait l'objet de nombreuses discussions. Le caractère international du réseau, joint au caractère immatériel des infractions, exigent que la lutte contre la cybercriminalité se traduise par des réactions spécifiques, surtout communautaires.

En effet, un atelier sur le cadre légal harmonisé des Technologies de l'Information et de la Communication (TIC) en Afrique de l'Ouest s'est tenu dans les locaux de la Banque d'Investissement et de Développement (BIDC) de la CEDEAO[118] à Lomé[119].

L'objectif de cet atelier est d'examiner et valider les projets de textes communautaires élaborés sous les auspices de la Commission Economique des Nations Unies pour l'Afrique (CEA) pour doter la sous région Ouest Africaine d'un cadre légal harmonisé en matière des Technologies de l'Information et de la Communication (TIC).

Le comité des experts des Etats membres et des institutions spécialisées des Nations Unies ont insisté sur la nécessité de disposer d'un cadre légal harmonisé sur les Technologies de l'Information et de la Communication (TIC) dans l'espace Ouest Africain CEDEAO-UEMOA[120]. C'est une condition sine qua non du développement de ces technologies dans la sous région et à l'intérieur de chaque pays.

---

[118] Communauté Économique des États de l'Afrique de l'Ouest.

[119] Rapport de l'atelier sur le cadre légal harmonisé sur les TIC en Afrique de l'Ouest , Lomé (Togo, 10-11 décembre 2007.

[120] Union Economique et Monétaire Ouest Africain.

Cette institution joue un rôle fondamental dans le développement des TIC en Afrique en général, et en particulier en Afrique de l'Ouest. Les pays de la CEDEAO et de l'UEMOA reconnaissent les TIC comme un vecteur important de développement et de compétitivité régionale.

Le rapport sur le cadre légal pour le e-commerce en Afrique de l'Ouest s'est fixé comme objectif l'intégration sous régionale, l'harmonisation des actions, la création de synergies et la coopération avec les autres organes africains. L'harmonisation des politiques gouvernant le marché des TIC dans l'espace africain est une présentation des principaux axes du projet de marché commun ouest africain.

L'adoption des lignes directrices et la réunion des conditions de mise en œuvre (juridique, financier, ressources humaines), la participation aux efforts d'harmonisation au plan africain, le suivi des travaux au plan international, l'implication dans le processus des organisations représentatives du secteur privé, de la société civile, les institutions de régulation, les médias et les universités, la conception et l'adoption des principes directeurs de sanction pénale en matière de lutte contre la cybercriminalité , l'harmonisation de la terminologie utilisée dans le droit des TIC en tenant compte des cultures juridiques en cours dans l'espace UEMOA-CEDEAO, l'élaboration des supports de communication (site web, ouvrages didactiques etc.) sur l'harmonisation des législations TIC et la poursuite de réformes au plan national dans le secteur des TIC sont les principes issus de cet atelier régional.

A l'initiative de l'Union Internationale des Télécommunications (UIT) l'OHADA des télécoms a organisé une réunion des régulateurs africains à Dakar en juin 2008, en présence des autorités sénégalaises et des nombreux acteurs du secteur privé (opérateurs, fournisseurs de services, associations...).

Au cours de cette réunion, les Chefs d'Etats africains avaient fixé cinq objectifs essentiels afin d'atteindre les objectifs du millénaire pour le développement : connecter toutes les capitales et les principales villes africaines par une infrastructure large bande en 2012, connecter les villages africains aux services large bande en 2015, adopter les mesures réglementaires essentielles, permettant l'accès aux services large bande et une connectivité IP à l'International, développer les compétences (centres d'excellence dans les NTIC dans chaque sous-région et mise en place de centres de formation dans chaque pays) et adopter des e-stratégies permettant le développement d'applications e-gouvernement, e-éducation, e-commerce, e-médecine,...

Mais, ces orientations ont été confirmées à la Conférence du Caire en mai 2008 par, notamment l'adoption d'un cadre de référence pour l'harmonisation des politiques dans les télécommunications et les NTIC et l'harmonisation des cadres réglementaires en Afrique.

Les pays africains conscients de l'importance de la société de l'information dans leur développement économique et social, ont entrepris plusieurs actions pour répondre à la problématique de la cybercriminalité qui crée un risque sécuritaire dans la société numérique. C'est dans cette optique que l'Agence des Télécommunications de Côte d'Ivoire (ATCI).

l'Organisation Internationale de la Francophonie (OIF) et l'Union Africaine (UA) ont organisé la conférence régionale africaine sur la cybersécurité en novembre 2008 en Côte d'Ivoire. Cette conférence avait pour thème: « bâtir un espace numérique de confiance en Afrique » avec pour objectif général la proposition d'un plan d'actions de cybersécurité et de lutte contre la cybercriminalité. La présente conférence a consisté en s, des conférences, des échanges débats et le partage d'expérience de certains pays.

La Conférence régionale africaine sur la cybersécurité recommande à la Commission de l'Union africaine (CUA) de rédiger la charte africaine sur le Cybersécurité, également de créer une unité dans le département des Ressources Humaines, la Science et la tenue annuelle de façon tournante dans une des différentes régions de l'Afrique. Il y a une prise de conscience générale en Afrique de la nécessité d'harmoniser sans délai les réglementations des communications électroniques et de mettre en œuvre les objectifs visés dans cette lutte contre la cybercriminalité.

L'Afrique de l'Ouest semble aborder correctement le processus de transposition en législations nationales des Actes additionnels de la CEDEAO. Il y a urgence à adopter un cadre réglementaire harmonisé pour éviter d'accroître la fracture numérique. Les pays de la sous région devraient également lancer un large plan d'éducation et de formation dans le domaine des TIC.

La mise en place d'un cadre juridique des TIC requiert une coopération au niveau régional voire international. En effet, les technologies évoluent trop rapidement, la circulation des données est mondiale et les défis juridictionnels sont déroutants. Sur le plan de la coopération régional, le travail a commencé récemment à l'occasion de la septième réunion des Ministres de la CEDEAO chargés des télécommunications et des TIC, en 2008. Lors de cette rencontre, il a été examiné et adopté un projet de Directive sur la protection des données à caractère personnel et un projet d'Acte Additionnel relatif à la cybercriminalité dans l'espace CEDEAO. Ces deux projets devront être soumis au Conseil des Ministres de la CEDEAO et à la Conférence des Chefs d'Etat et de Gouvernement. Une fois en vigueur, ces textes permettront aux autorités policières et judiciaires de disposer d'autres moyens de coopération pour faire face notamment à la cybercriminalité venue d'ailleurs[121].

En sommes, les Etats doivent instaurer des autorités de régulations compétentes et autonomes, mettre en place des outils de régulation performants, doter les autorités de régulation de ressources humaines compétentes, réviser les lois des télécommunications en prenant en compte la convergence des technologies, harmoniser les politiques réglementaires dans chaque sous région, développer de bonnes stratégies pour l'accès universel et faciliter la connectivité, favoriser la neutralité technologique dans l'attribution des licences, réduire les barrières fiscales pour encourager les investissements des opérateurs, encourager les investissements sur la fibre optique, développer les points d'échange IXP pour réduire les tarifs d'accès à l'Internet, amener tous les acteurs du secteur à contribuer au Fonds du Service Universel, instaurer le dégroupage de la boucle locale, réaménager les bandes de fréquences

[121] Mouhamadou Lo. La réglementation de la société sénégalaise de l'information

audiovisuelles, favoriser l'investissement dans les technologies sans fil, réduire les taxes douanières pour favoriser les investissements dans les nouvelles générations.

L'harmonisation du cadre juridique des TIC dans les Etats d'Afrique de l'Ouest (UEMOA-CEDEAO) et la nécessité d'une étroite coopération entre les autorités de la chaîne judiciaire et les autorités judiciaires des différents pays aura le mérite de favoriser la naissance d'un véritable cyber droit pénal, régulateur du cyberespace.

Cependant, au regard de tous ces textes, on peut dire que les pays de la sous région ne disposent en ce moment d'aucun texte communautaire répressif pouvant constituer une source commune de régulation du cyberespace et de répression de l'activité délictuelle qui se déroule dans cette espace. Outre l'adoption d'un instrument régional, lutter efficacement contre le phénomène du cyber crime suppose également de mettre en branle une coopération juridique et institutionnelle entre les différents Etats.

B. Une coopération juridique et institutionnelle internationale

L'internationalisation criminelle et la diffusion des messages illicites sur Internet peuvent avoir des effets qui peuvent s'entendre dans plusieurs pays en même temps. Ainsi, cette nouvelle forme de délinquance transnationale se heurtant au principe classique de la territorialité de la loi pénale, demande un concours concerté, un renforcement de la coopération juridique et institutionnelle internationale[122].

D'abord, la coopération juridique internationale vise à favoriser la collaboration entre Etats en matière pénale par l'adoption d'instruments collectifs de traitement de la cybercriminalité. Dans le cadre de la lutte contre cette forme de criminalité, des Etats sont parvenu à adopter un instrument juridique international de lutte contre la criminalité numérique ouverte à la signature des Etats du monde.

En effet, la Convention européenne de Budapest du 23 novembre 2001 sur la cybercriminalité constitue le premier traité international visant à apporter des réponses aux problèmes soulevés par l'interconnexion des réseaux informatiques[123].

Il résulte en effet des dispositions de l'article 37 de la Convention qu'« après l'entrée en vigueur de la présente convention, le comité des ministres du conseil de l'Europe peut après avoir consulté les Etats contractants à la convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre et n'ayant pas participé à son élaboration à adhérer à la présente convention... ». En conséquence, la Convention de Budapest peut légalement servir d'instrument de répression de la cybercriminalité aux Etats africains y nt adhéré. Mais, force

---

[122] R. ZIMMERMANN, La coopération judiciaire internationale en matière pénale, Stqempfli SA Berne, 2004, 2è éd., n°346. Il faut relever que cette règle est subtilement posée à l'art. 1er al. 11 suivant lequel le terme « infraction » désigne « le fait ou les faits constituant une infraction pénale ou des infractions pénales selon la législation des Etats membres »

[123] Xavier Le CERF, Lutter contre la cybercriminalité : le projet de Convention du Conseil de l'Europe sur la cybercriminalité. http://www.juriscom.com.

est de constater que le Sénégal qui n'a pas adhéré à la Convention de Budapest ne dispose pas d'instrument juridique international de répression de la criminalité.

Cette convention s'applique aux crimes commis sur et à travers les réseaux informatiques. Elle a pour but d'harmoniser les législations des Etats signataires en matière de cybercriminalité et à cette fin, la convention établit des définitions communes de certaines infractions pénales commises par le biais des réseaux informatiques.

Elle sert à compléter les législations, notamment en matière procédurale afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter des preuves sur le territoire national avant qu'elles ne disparaissent et en même temps améliorer la coopération internationale.

Le protocole additionnel à la Convention sur la cybercriminalité ouvert à la signature en janvier 2003 demande aux Etats de criminaliser la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques. Ce protocole élargit donc le champ d'application de la convention afin de couvrir également les infractions de propagande raciste ou xénophobe commises via les réseaux informatiques. Il prévoit, par ailleurs, de faciliter l'extradition des contrevenants à l'intérieur de l'espace européen, ainsi que de favoriser l'entraide judiciaire pour la répression de ces agissements. Ce Protocole poursuit deux objectifs : premièrement, harmoniser le droit pénal matériel dans la lutte contre le racisme et la xénophobie sur l'Internet et deuxièmement, améliorer la coopération internationale dans ce domaine.

Les instruments de la coopération internationale que sont les traités, recommandations et directives mettant souvent à la charge des Etats membres une obligation de transposition des normes internationales en droit interne et constituent un levier sûr de l'harmonisation de la répression de la cybercriminalité.

Le renforcement de la coopération juridique entre les Etats dans le cadre de la lutte contre la cybercriminalité engendre en droit l'harmonisation des normes pénales qui n'est qu'un aspect de la mondialisation du droit[124]. En effet, le droit conventionnel issu de la coopération internationale tend à jeter les bases des principes communs organisant la répression des cybercriminels, faute d'une intégration globale.

En matière de cybercriminalité, l'harmonisation concerne les incriminations de la cybercriminalité dont les contours sont cernés par le droit conventionnel. Par exemple, la convention de Budapest du 23 novembre 2001 dans ses articles 2 et suivants relatifs au droit pénal matériel invite les Etats membres à adopter « les normes législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales », les agissements liés à l'utilisation des TIC. Les articles 19 et suivants tendent à fixer les principes communs relatifs aux perquisitions et saisies informatiques, à la compétence juridictionnelle, à la valeur probatoire des preuves informatiques et à la coopération judiciaire internationale.

Il faut relever que l'harmonisation des législations nationales ne peut se faire au mépris de la souveraineté des Etats, illustrée en droit pénal par le pouvoir de la sanction pénale

[124] M.DELMAS-MARTY ;La mondialisation du droit : Chances et Risques, D. 1999, Chron. 43, p 3.

considéré comme le droit pour l'Etat d'infliger un châtiment au délinquant en rétribution du trouble causé à la société.[125]

Ainsi, le droit conventionnel issu de la coopération internationale renvoie, s'agissant de la sanction pénale applicable, aux comportements cybercriminels aux législations des Etats membres. En effet, il résulte des dispositions de l'article 13 de la Convention de Budapest du 21 novembre 2001 sur la cybercriminalité que « chaque partie adopte les mesures législatives et autre qui se révèlent nécessaires pour faire en sorte que les infractions pénales (...) soient passibles de sanctions pénales effectives proportionnées et dissuasives comprenant des peines privatives de liberté ».

Cependant, l'internationalisation de la procédure de répression de la cybercriminalité devant le juge sénégalais est largement tributaire de l'amélioration de la coopération au plan institutionnel.

La coopération institutionnelle internationale s'exerce entre les polices nationales grâce à diverses techniques juridiques mises à la disposition des Etats par les instances policières. Cette coopération apparaît insuffisante à l'heure actuelle car dans la conduite des investigations et enquêtes liées à la cybercriminalité, les organes qui sont chargés de poursuivre leur mission hors des territoires de leurs Etats se heurtent souvent à des obstacles.

La consolidation de la coopération entre autorités policières et judiciaires chargés de la recherche, de la constatation et du jugement des infractions informatique est donc une nécessité pour une lutte efficace contre la cybercriminalité.

En matière de coopération policière, l'Office Européen de Police dit Europol siégeant à la Hayes aux Pays-Bas est un organe policier chargé du traitement des renseignements reçus des Etats membre relatifs à la commission d'actions criminelles. Il a essentiellement pour objectif d'améliorer l'efficience des services de police compétents dans les Etats membres et d'accroître la coopération dans le cadre de la prévention et de la lutte contre les formes de criminalité transnationale organisée comme la cybercriminalité. En Europe, dans le cadre des accords de Schengen, il a été créé un système d'information entre les Etats signataires leur permettant une consultation automatisée des données dans le domaine de la criminalité informatique.

Mais, la plus prestigieuse est sans nul doute l'Organisation Internationale de Police Criminelle (OIPC) créé en 1929 dite Interpol. Cette organisation à laquelle le Sénégal est membre depuis 1961 vise à améliorer la coopération policière dans le monde et à faciliter la lutte contre le terrorisme, le trafic de stupéfiants et la cybercriminalité entre autres.

Dans le cadre de la coopération internationale, Interpol a mis en place un système d'analyse, de collecte, de documentation et de formation du personnel en matière de pédopornographie. Et les informations susceptibles d'être collectées sont vérifiées par les analystes d'Interpol avant d'être intégrées dans un fichier d'analyse identifiable.

---

[125] R. MERLE et A. VITU, Traité de droit criminel, Edition CUJAS, 1973, p 646.

Interpol dispose également d'un système d'assistance technique, d'expertise pour les enquêtes et opérations menées par les polices nationales et de programmes spécifiques de formation du personnel des services de police chargés des enquêtes relatives à la criminalité numérique. Le système de communication commun à tous les pays membres de l'Interpol basé sur des données criminelles internationales est relayé depuis 1999 par un site web accessible aux Etats, afin de permettre une plus large diffusion des informations collectées.

Une nouvelle démarche a permis à Interpol de réaliser des opérations de police judiciaire de grande envergure telles que l'opération « Cathédrale » lancée en 1998 qui a été à l'origine du démantèlement d'un réseau diffusant 750 000 clichés de pornographie enfantine et qui s'est soldée par l'arrestation de 107 personnes dans 12 pays.

Il faut dire que le renforcement de la coopération policière garantit un traitement beaucoup plus effectif de la cybercriminalité surtout dans les pays africains qui, en raison de la modicité de leurs moyens techniques, sont souvent impuissants face aux agissements liés aux TIC. Mais la même observation vaut également pour la coopération entre les autorités judiciaires.

La révolution numérique justifie la mise en œuvre d'une stratégie de rationalisation de l'entraide judiciaire et l'élaboration d'une seconde stratégie de renforcement du droit de l'extradition judiciaire.

L'entraide judiciaire résultant d'accords bilatéraux (Accord de coopération en matière de Justice entre le Sénégal et la France du 14 juin 1962) et multilatéraux (accords conclus par le Sénégal sous les auspices d'organisations régionales ou internationales)[126] est marquée par sa lourdeur et son inadaptation aux investigations judiciaires liées aux TIC.

La convention de coopération entre le Sénégal et la France du 14 juin 1962 stipule que la « transmission des actes juridiques, ou extrajudiciaires destinés à des personnes résidant sur le territoire de l'une des parties contractantes ainsi que la transmission des commissions rogatoires, s'effectuent entre ministres de la justice des deux Etats » ; mais la convention précise que les Etats ont toujours la faculté de faire remettre par leurs représentants ou délégués, les actes judiciaires ou extrajudiciaires destinés à leur ressortissants.

Par ailleurs, l'article 27 de la convention donne aux autorités judiciaires de la partie requérante, en cas d'urgence, le pouvoir d'adresser directement à leurs homologues de la partie requise les demandes d'entraide ou les communications s'y rapportant.

Les investigations judiciaires impliquant des infractions informatiques requièrent une coopération judiciaire rapide et pragmatique en raison de la fugacité des comportements cybercriminels.

En Europe, la convention de Budapest du 23 novembre 2001 fixant dans son Titre III, les principes généraux de l'entraide judiciaire, précise que « chaque partie peut en cas d'urgence formuler une demande d'entraide ou les communications s'y rapportant par des

[126] Dans le cadre de l'Union Africaine et Malgache (UAM) : Convention du 12 septembre 1961, JOS 1967, p 900.

moyens rapides de communication tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification... ». L'Etat requis qui accepte la demande y répond par n'importe lequel de ces moyens rapides de communication[127].

L'extradition judiciaire par contre représente la manifestation la plus importante de la coopération judiciaire que les Etats se prêtent en vue de la répression des infractions. Elle est définie comme la procédure par laquelle un Etat appelé « Etat requis » ou « Etat de refuge » livre un individu à un autre Etat appelé « Etat requérant », qui le lui demande, en vue de le juger ou de lui faire subir sa peine[128]. Elle constitue selon la jurisprudence un acte de souveraineté en ce que « le gouvernement qui fait arrêter sur son territoire le prévenu d'un crime commis sur un autre territoire et le livre à la puissance qui le réclame, pour le juger et le punir, use d'un droit qu'il puise de sa propre souveraineté »[129].

Au Sénégal, le droit de l'extradition résulte des traités d'extradition signés par le Sénégal avec d'autres pays et de façon dérogatoire de la loi n° 71-77 du 28 décembre 1971. Il en résulte alors que la possibilité pour le gouvernement d'un Etat d'obtenir l'extradition auprès d'un autre Etat suppose que ces deux Etats soient liés par un accord bilatéral ou multilatéral de coopération judiciaire d'extradition, ce qui à notre sens limite sensiblement la portée du droit de l'extradition et ne manque pas d'achopper sur la transnationalité de la cybercriminalité.

Une extension du champ de l'extradition judiciaire devrait être envisagée par l'adoption d'une convention internationale contre la cybercriminalité prévoyant des dispositions relatives à l'extradition judiciaire. C'est dans ce sens que la convention de Budapest en Europe précise en son article 24 que les dispositions relatives à l'extradition judiciaire prévues au titre II (« les principes relatifs à l'extradition ») s'appliquent à l'extradition entre les parties pour les infractions liées aux TIC « à condition qu'elles soient passibles dans la législation des deux parties concernés par une peine privative de liberté pour une période d'au moins 1 an ou par une peine plus sévère ».

Cette disposition sur l'extradition est pour les juges traitant des procédures impliquant la cybercriminalité la meilleure solution puisqu'elle permet une extradition auprès d'un Etat membre de la Convention de Budapest, dès l'instant que l'incrimination en cause est prévue par la dite convention, même auprès d'un Etat avec lequel il n'a conclu aucun accord bilatéral de coopération judiciaire d'extradition.

En somme, la convention sur la cybercriminalité vise d'abord à harmoniser les législations nationales en matière d'incrimination et de sanctions pénales pour une liste de comportements soumis à répression. Doivent, entre autres, être réprimés l'accès illégal à un système informatique ou la diffusion de matériel pédophile par le biais d'un système informatique. En second lieu, elle tend à compléter l'arsenal juridique des Etats en matière procédurale, afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à rassembler des preuves sur le territoire national avant qu'elles ne

[127] Voir Convention de Budapest.
[128] Voir Pape Assane TOURE, « Le traitement de la cybercriminalité devant le Juge sénégalais », Mémoire de Diplôme d'études approfondies.
[129] Cass. 4 mai 1895, S. 1866 I. 36.

disparaissent. Enfin, elle adapte les règles classiques des conventions du Conseil de l'Europe en matière d'extradition et d'entraide répressive.

En définitive, le traitement efficace de la cybercriminalité passe nécessairement par l'harmonisation des normes juridiques et par une coopération institutionnelle conjuguée avec un renforcement des capacités et le recours à la régulation.

Paragraphe II : Le renforcement des capacités et le recours à la régulation

La lutte contre la cybercriminalité doit passer nécessairement par le renforcement des moyens humains et technologiques (A) et par la participation des acteurs dans la régulation du cyberespace (B).

A. Le renforcement des moyens humains et technologiques

Le dispositif de renforcement des moyens humains et technologiques s'appuie sur la mise en place d'un réseau mixte public et privé d'experts et sur l'identification d'axes de recherche correspondant aux priorités des services opérationnels. Le réseau d'experts devrait rassembler des spécialistes de la police, de la gendarmerie, reliés par des outils de travail coopératifs.

La sécurité des réseaux, la téléphonie et les accès à Internet doivent être les principaux domaines explorés. Un forum de discussion devrait être créé au sein de la police et de la gendarmerie et qui de ce fait prolongera les échanges du réseau d'experts au sein des services concernés des deux forces.

Les logiciels développés par la police et la gendarmerie doivent faire l'objet d'une mise à disposition mutuelle sans formalité administrative. C'est également ensemble que la police et la gendarmerie nationale devront rechercher les matériels les mieux adaptés à leurs missions de veille et d'investigation.

En France, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé au sein la Direction Centrale de la Police judiciaire au ministère de l'intérieur afin de mieux lutter contre cette criminalité. La Direction de la surveillance du territoire, compétente pour diligenter des enquêtes judiciaires relatives à des actes de piratage sur les systèmes informatiques des établissements à régime restrictif ou des données classifiées de défense, intervient de manière complémentaire à l'action de l'OCLCTIC. La Division nationale de répression des atteintes aux personnes et aux biens (DNRAPB) a pris en charge le traitement des atteintes aux mineurs victimes et des infractions à la loi sur la presse liées au cyberespace.

Le Sénégal doit suivre l'exemple de la France par la création d'organe de lutte comme l'OCLCTIC pour mieux assurer cette lutte contre la cybercriminalité. Il doit également concevoir et mettre en œuvre une posture plus offensive en organisant des alliances entre la police, la gendarmerie et les autres composantes de la sécurité intérieure, mais aussi développer des coopérations techniques, juridiques avec toutes les institutions, les entreprises, les organismes publics ou privés qui agissent chacun dans son domaine contre la cybercriminalité.

A cela s'ajoute, bien évidemment, la coopération internationale, car les technologies numériques ne connaissent pas de frontière. Des dispositions doivent être prises dans le sens de mieux faire connaître les infractions relatives au cyberespace. Les capacités opérationnelles des services de police et de gendarmerie doivent être accrues avec un développement en amont d'actions de formation communes. Cette formation devrait s'adresser aux enquêteurs spécialisés de la police et de la gendarmerie. Elle bénéficierait à l'ensemble des policiers et gendarmes dès leur formation initiale et tout au long de leur carrière.

Le développement d'une politique de prévention est nécessaire. Cette politique doit consister en des opérations de communication en direction du grand public et des professionnels, avec des campagnes de sensibilisation sur les dangers et risques liés à Internet et sur les règles qui doivent s'y appliquer.

Parallèlement aux efforts et mesures à entreprendre par les pouvoirs publics, un sursaut doit provenir des acteurs mêmes de la société de l'information en termes d'autorégulation.

B. La nécessité d'une participation des acteurs dans la régulation du cyberespace

La cybercriminalité constitue un phénomène déviant, c'est-à-dire un comportement d'écart à la norme qui, par sa nature, peut être perçu comme une infraction, terme pris au sens non spécifiquement pénal d'écart à la normativité juridique[130]. Il s'agit d'un acte de transgression d'une interdiction susceptible de recevoir en politique criminelle deux réponses, l'une de nature étatique, c'est la répression, l'autre d'origine sociétale appelée autorégulation.

La participation aux activités dans le cyberespace met en scène une diversité d'acteurs qui n'ont de point commun que l'utilisation des NTIC. Le cyberespace est par excellence le lieu d'une nouvelle socialisation d'architecture cybernétique. De ce fait, le niveau de connectivité entre les structures étatiques et sociétales détermine dans une large mesure l'identité et la qualité des acteurs intervenant dans le cyberespace. Espace transfrontier, le cyberespace met en relation des acteurs issus de cultures différentes et soumis à une législation distincte. L'acceptation paradigmatique du vocable cybernaute ou celui d'acteur pour désigner un usager du cyberespace traduit la reconstitution d'un ensemble de structures ou d'individus mettant en relation des Etats, des organisations intergouvernementales ou non gouvernementales, le secteur privé, la société civile ou simplement le citoyen[131].

Les acteurs publics internationaux intervenant dans le cyberespace et les organisations politiques semblent occuper une place importante. En effet, l'Organisation des Nations Unies (NU) se positionne dans le management de la société de l'information. Les déclarations et

---

[130] (M.) DELMAS-MARTY, Les grands systèmes de politique criminelle, Paris, PUF 1992, p. 11.

[131] CISSE Abdoullah, Les acteurs du droit du Cyberespace,saintlouis.ustrasbg.fr.

plan d'actions adoptés sous l'égide des NU servent de principes directeurs aux législations nationales destinées à être directement applicables au cyberespace.

L'Afrique, représentée par l'UA, la CEA et par le NEPAD, a un volet important sur le renforcement de l'utilisation des TIC par les pays en développement. L'OHADA, l'UEMOA et la CEDEAO ont chacun pour leur part une politique régionale sur l'environnement juridique des TIC. En effet, avec des projets d'harmonisation des législations nationales sur les TIC, ces instances communautaires participent à la construction d'un cyberdroit africain plus conforme avec les réalités continentales. Sous le couvert de la coopération internationale, les instances africaines élaborent des cadres de concertation et des politiques communes avec d'autres organisations internationales. Les initiatives issues de ces rencontres forment un ensemble pertinent de documents et d'institutions en mesure d'accroître la participation africaine au processus de décision internationale. Une autre dimension majeure du volet international concerne les ONG.

Les acteurs publics nationaux notamment l'Etat restent la principale constante dans la hiérarchie des organismes intervenant dans le cyberespace au niveau national. Ainsi, les organes centraux de l'Etat regroupés autour des ministères chargés des télécommunications ou des TIC dans les pays africains coordonnent la politique gouvernementale en la matière. Au Sénégal par exemple, le ministère des télécommunications s'appuie sur des régulateurs (ARTP[132], HCA[133]) et des services spécialisés (ADIE, APIX[134]) pour promouvoir les orientations de la société sénégalaise de l'information et contrôler les activités des acteurs intervenant dans le cyberespace.

L'admission du secteur privé comme entité autonome en compagnie des Etats et de la société civile a un soubassement idéologique lié au triomphe de l'économie de marché sur les autres systèmes à vocation organisationnelle. Confrontés au cyberespace, les mécanismes de l'économie de marché se sont adaptés au point de se situer en concurrence directe avec les autorités publiques dans la régulation des relations qui s'établissent autour de l'accès et de l'utilisation des ressources du monde virtuel.

Les acteurs privés transnationaux sont considérés comme des partenaires privilégiés des acteurs publics dans le processus de régulation juridique et sociale du cyberespace. En Afrique, l'engagement du secteur privé national est perceptible à travers la densité des indices de participation relevés dans le cyberespace. Ainsi, à défaut de parler d'une véritable cristallisation des acteurs locaux dans le cyberespace, il est possible de percevoir les prémisses d'une participation accrues des entreprises privées en Afrique, surtout celles s'investissant dans le secteur des TIC.

La société civile est une réalité composite regroupant aussi bien des associations transnationales, régionales, nationales et locales, que des individus qui militent pour une cause déterminée ou revendique un droit précis. Les négociations de l'OMC sur le commerce internationale ont mis en évidence la variabilité et l'intensité des revendications collectives

[132] Agence de Régulation des Télécommunications et des Postes.
[133] Haut Conseil de l'Audiovisuel.
[134] Agence pour la Promotion des Grands Travaux.

sur plusieurs thématiques différentes. L'Internet non plus n'a pas échappé à ce nouveau phénomène soucieux d'une plus grande équité dans l'accès et la régulation du cyberespace. Les enjeux cruciaux pour le continent africain révèlent une synergie régionale structurée autours de revendications communes et dont le point culminant est sans aucun doute le concept de fracture numérique que tente de juguler la solidarité numérique, autre création africaine.

En relation avec les spécificités africaines, une société civile internationale tisse sa toile dans le cyberespace grâce aux forums sur Internet. Elle œuvre pour la reconnaissance de la liberté d'expression, la liberté de navigation, liberté d'accès entre autres besoins. En effet, il est assez symptomatique de constater l'absence permanente des membres de la société civile dans les instances de prise de décision internationale. En Afrique surtout, cette absence est renforcée par le gap numérique qui prolonge ses avatars dans le monde physique.

La typologie des organisations nationales vouées à la régulation du cyberespace concerne souvent les autorités administratives indépendantes chargées de veiller au bon fonctionnement des mécanismes induits par la privatisation et la libéralisation du secteur des télécommunications. Dans l'espace CEDEAO par exemple, il s'agit des organismes membres de l'ARTAO, tels que l'ARTP (Sénégal), DPPT (Bénin), ARTEL (Burkina Faso), ATCI (C.I). etc ... Toutes ces organisations œuvrent au plan national à maintenir un niveau approprié d'intégration des TIC dans le processus de développement des pays. En outre, les prérogatives réglementaires attribuées à ces entités contribuent à asseoir un contrôle plus pragmatique des activités des acteurs privés dans les domaines de l'interconnexion, la tarification et l'Internet haut-débit.

Il faut enfin préciser que l'alternative de l'autorégulation[135] correspondant soit à une réponse corporative du milieu professionnel (autodiscipline) ou à une réponse individuelle de la victime (autodéfense), se traduit dans le cyberespace notamment par l'élaboration de codes de conduite et de déontologie fixant les règles de transparence et de responsabilité . La sensibilisation du grand public sur les risques de Internet (autodiscipline) et la mise en place de procédés techniques de contrôle tels que la diffusion de logiciels de contrôle (parental notamment), le recours au cryptage, la conception des mots de passe sécurisés ou inviolables etc... (autodéfense) sont autant de possibilités à mettre en œuvre dans le cadre d'une lutte efficient et efficace contre le phénomène de la cybercriminalité[136].

[135] Voir Pape Assane TOURE. « Le traitement de la cybercriminalité devant le Juge sénégalais », Mémoire de Diplôme d'études approfondies.

[136] Ibid ,Pape Assane TOURE.

CONCLUSION

L'avènement de la révolution numérique du XXI^{ème} siècle a suscité l'apparition de nouveaux comportements dématérialisés se mouvant dans l'environnement cyber spatial, rendant ainsi impertinentes les notions d'espace matériel de temps et de territoire, qui étaient jusque-là des repères fondamentaux de la création et de l'application de la norme pénale.

Le phénomène de la cybercriminalité n'est pas une réalité spontanée, mais le fruit d'une longue évolution économique conduite par le développement accru des nouvelles technologies de l'information et de la communication. Cette nouvelle forme de criminalité connaît une ampleur exponentielle difficile à évaluer, laissant apparaître comme une évidence incontournable l'inadaptation du système judiciaire. La difficulté d'appréhender cette criminalité sur les technologies de l'information et de la communication tient en partie au fait que ce réseau est un moyen de communication mondial permettant de véhiculer tous types de données.

Le traitement efficace de la cybercriminalité devant le juge sénégalais passe d'une part, par un mouvement d'expansion du champ de la politique criminelle s'adossant sur l'existence d'un cadre juridique normalisé matérialisé par l'élaboration d'une stratégie de modernisation des incriminations de droit pénal ainsi qu'une démarche d'amélioration de la procédure de répression de la criminalité numérique ; et d'autre part, par un renforcement des capacités humaines et matérielles au niveau des services policières et judiciaires à travers l'organisation de formations et la mise à disposition d'équipements et de technologies de pointe adaptées à la lutte contre cette nouvelle forme de délinquance. Enfin, le recours à la régulation constitue une voie salutaire pour venir à bout de ce phénomène.

L'avènement de la cybercriminalité a le mérite de favoriser la naissance d'un véritable cyber droit pénal, régulateur du cyberespace qui était jusque là une zone affranchie du droit fonctionnant selon le principe libertaire.

Mais, force est de constater qu'une répression adéquate du phénomène cybercriminel ne saurait se réaliser sans une dynamique tendant à l'internationalisation la politique criminelle.

En effet, avec la mondialisation de l'économie qui s'accompagne de la mondialisation de la criminalité surtout via l'outil informatique, les Etats se doivent, ne serait ce que pour sauvegarder les valeurs communes fondamentales (paix, sécurité, bien être social...), d'impulser l'élaboration d'un minimum de règles de droit pénal et de procédure pénale communes de sorte à assurer la répression des comportements cyber déviants quel que soit le lieu de leur commission ou d'établissement de leurs auteurs ou bénéficiaires.

La perspective de la mise en place d'un arsenal juridique mondial, une adhésion du Sénégal et des Etats africains à la Convention de Budapest du 21 décembre 2001 pourrait constituer un tremplin. Pareil choix semble être plus rationnel en ce qu'il dispensera les

adhérents d'une suite de problèmes : conférences diplomatiques coûteuses et, parfois, lieu de contradictions peu fructueuses. Cela répondrait, par ailleurs, mieux au caractère mondial que doit revêtir la réponse au phénomène de la cybercriminalité.

En tout état de cause, il semblerait que la réalité de la criminalité cybernétique n'a pas encore été suffisamment pris en compte par les autorités politiques africaines et tarde à être inscrite parmi les priorités des services de répression. Il semble également que la question n'a pas encore été suffisamment prise en charge du côté de la doctrine africaine qui a pourtant une large vocation avant-gardiste.

BIBLIOGRAPHIE

DIOUF (Nd.), Infractions pénales et NTIC, http://saintlouis.ustrasbg.fr.

DELMAS MARTY (M.), Droit pénal des affaires, PUF, Coll Thémis, Paris 1973,Tome I et II.
MERLE (R.) et VITU (A.), Traité de droit criminel, Editions Cujas, 2ème éd.1973.
PRADEL (J.), Droit pénal général, Cujas, 10ème édition, 1995.
PRADEL (J.), Procédure pénale, Cujas, 5ème édition, 1990.
RASSAT (M-L), Droit pénal spécial, Infractions du et contre les particuliers, Précis Dalloz, 2ème édition 1999.
STEFANI (B.), LEVASSEUR (G.) BOULOC (B.), Droit pénal
MARTIN (D.), La criminalité informatique, PUF, Coll. Criminalité internationale, 1997.
NDIAYE (J.A), « La protection des mineurs dans l'internet », mémoire de DEA Economique et des Affaires, UGB St LOUIS.
AMMAR (D.), La preuve électronique, RTD, Civ, 1993, p. 499.
CHABOT (G.), La cyberjustice : Réalité ou fiction ? D. 2003, n° 34.
DEVEZE (J.), La fraude informatique : Aspects Juridiques, JCP, 1987, Doct. n° 3289.
DEVEZE, (J.), Le vol des biens informatiques, JCP. Ed. G. 1986 II, p.337 n° 14712.
DIOUF (Nd.), La procédure pénale à l'épreuve des nouvelles technologies de l'information, Revue de l'Association sénégalaise de Droit pénal, n° 5, 6, 7 et 8, 1997-1998, p. 27.
KORMANN, Le délit de diffusion d'idées racistes ; JCP 1989, Doct. n° 3404.
PADOIN (D.), Lutter contre la criminalité sur les systèmes d'information : La police judiciaire, RFC, 281, 1996, p. 66.
PRADEL (J.) et FEUILLARD (Ch.), Les infractions commises au moyen de l'ordinateur, Rev. Dr. pén et crim, 1985, p. 307 et s.
SCHULTZ (H.), Compétence des juridictions pénales pour les infractions commises à l'étranger, RSC 1967. P 335.
VIVANT (M.), La responsabilité des intermédiaires de l'Internet, JCP, Ed. G. I, 180, 1999/11/10, p. 2021.
CHAMPY (G.), La fraude informatique, Etudes phénoménologique et typologique appliquées au contexte français, thèse, Paris, 1985.
CISSE (A.), La transaction pénale administrative, thèse Tunis II, 1993.
Le CERF (X.), Lutter contre la cybercriminalité : le projet de Convention du Conseil de l'Europe sur la cybercriminalité.
JOUGLEUX (Ph.), La criminalité dans le cyberespace, Mémoire de DEA, Aix Marseille, 1999.
MALONGA YOUNAS (J-P), La répression des agissements liés aux nouvelles technologies de l'information : l'exemple du Congo, Thèse, Dakar 2003.
TOURE (P.A), Le traitement de la cybercriminalité devant le Juge sénégalais, mémoire DEA Université Gaston BERGER de ST LOUIS.
Mohamed N. Salam, Mémoire de DEA « Le piratage informatique: Définition et problème juridique ».

TOURE (P.A), « La cyberstratégie de répression de la cybercriminalité au Sénégal : la présentation de la loi n° 2008- 11 du 25 janvier 2008, portant sur la cybercriminalité »

Agence de l'Informatique de l'Etat (ADIE), Recueil du droit sénégalais dans la société de l'information « décret et loi d'application »

NDIAYE (J.A), Le cadre juridique des transactions électroniques au Sénégal : la présentation de la loi n° 2008- 08 du 25 janvier 2008, portant sur les transactions électroniques.

Séminaire ADIE-Coopération française «Informatique et libertés, quel cadre juridique pour le Sénégal ? ».

LO (M), La réglementation de la société sénégalaise de l'information.

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.

MENGA (L.K), Droit pénal et TIC .

CISSE Abdoullah, « Les sources du droit du cyberespace ».

Séminaire « Informatique et libertés, quel cadre juridique pour le Sénégal ? ».

BRETON (T.), chantier de lutte contre la cybercriminalité.

NGOM (Mb.), Docteur en droit UFR SJP – UGB Saint-Louis, « Le cadre juridique des transactions électroniques au Sénégal »

CISSE (A), Cyberaudit stratégique.

Le Sénégal à l'heure de l'Information, Technologies et Société, sous la Dir. de Momar Coumba DIOP, Edition Karthala, Paris 2002.

CISSE (A), Les acteurs du droit du cyberespace.

LEMOINE (v), La cybercriminalité : « les acteurs, les infractions ».

VAGENA (E), « La responsabilité des intermédiaires dans la société de l'information » ou « Quand un clic pourrait ouvrir une nouvelle boîte de Pandore » mémoire de D.E.A Informatique et Droit.

Convention de Budapest du 21 novembre 2001 sur la cybercriminalité, http://conventions.coe.int.

AMEGEE (M), La protection des mineurs sur Internet : la problématique de la pornographie.

SITES CONSULTES

www.juriFrance.com

www.dalloz.fr

www.lexisnexis.com

www.legalis.net

www.osiris.sn

www.adie.sn

www.memoireonline.com

www.forum internet.org

www.gouv.sn

www.lb.refer.org

www.telecom.gouv.sn

www.jo.gouv.sn

www.cybercrimes.net

TABLEDES MATIERES