CONSEIL DE L'EUROPE-PROGRAMME OCTOPUS INTERFACE 2010
Conférence sur la coopération contre la cybercriminalité,
Strasbourg, France, 23-25 mars 2010.

La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 200 8, portant sur la cybercriminalité.

Depuis sa première connexion officielle au réseau Internet en 1996, le Sénégal contemporain n'a cessé d'accomplir des avancées considérables dans le secteur des TIC. La vision du e-Sénégal a vite placé notre pays au cœur de la société de l'information et lui a valu de se voir confier le volet TIC dans le cadre du NEPAD[1].

Cependant, comme l'enseignait déjà le Doyen Jean CARBONNIER « *l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance* »[2] En effet, comme pour la plupart des grandes découvertes contemporaines, la révolution numérique a engendré des retombées négatives parmi lesquelles figure en bonne place la criminalité[3]. Ainsi, le développement des TIC a généré une nouvelle forme de criminalité dénommée cybercriminalité, charriée par les premières lueurs de la société sénégalaise de l'information. L'attaque dont a été victime le site officiel du Gouvernement du Sénégal[4] en mai 2001 de la part d'un pirate informatique se disant membre de la « *Hack Army* »[5] ainsi les actes sabotage informatiques par cheval de Troie envoyé depuis le forum de discussion dirigés contre le site d'informations en ligne nettali.com en janvier 2008[6], ont fini de convaincre sur l'expansion de la cybercriminalité au Sénégal.

Face aux enjeux suscités par l'avènement de la cybercriminalité, les pouvoirs publics sénégalais ont, dès janvier 2005, entrepris, un vaste chantier juridique de mise en place des textes législatifs et réglementaires favorables au développement des TIC au Sénégal, en vue de protéger les biens, les personnes et les institutions publiques contre le phénomène cybercriminel[7].

Cette réforme de grande ampleur de l'arsenal pénal a donné naissance à la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité[8]. Ce texte de loi qui a apporté de grandes innovations dans le droit criminel sénégalais, a trouvé une source d'inspiration notamment dans la convention de Budapest sur la

---

1 V. M. C. DIOP (dir.), Le Sénégal à l'heure de l'information, technologies et société, Ed. Karthala, Paris 2002, p. 63 ; également, O. SAGNA, Les technologies de l'information et de la communication et le développement social au Sénégal : un état des lieux, Dakar, UNRIDS, Janvier 2001, p. 61.

2 V. J. CARBONNIER, Sociologie Juridique, PUF, 1978, p.401

3 A. LEPAGE, Internet : un nouvel espace de délinquance, Act. Jur.Pén. , n° 6, juin 2005, Dossier, p. 217 ; M.QUEMENER, Cybercriminalité : aspects stratégiques et juridiques, in « *De la cybercriminalité à la cyberguerre* », Rev. Défense nationale et sécurité collective, mai 2008, p. 23

4 http://www.gouv.sn

5 V. Le site Web du Gouvernement attaqué par un « hacker », in Batik, Osiris, n° 22, mai 2001, p. 4

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

7 V. A CISSE, La réflexion sur les éléments constitutifs et avant projets de lois sur la société de l'information, Rapport Général, Séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal* ?», Dakar, 29 et 30 août 2005, p. 205.

8 J.O.R.S, n° 6406, du 3 mai 2008, p. 419.

cybercriminalité du 23 novembre 2001, dans la décision cadre du conseil de l'Union européenne du 24 février 2005 relative aux attaques visant les systèmes d'information, et dans certaines législations européennes[9].

A la différence de la législation antérieure[10], cette loi procède d'une appréhension globale du phénomène cybercriminel. Les rédacteurs de la loi sur la cybercriminalité, ont en effet élaboré une véritable cyberstratégie de répression du phénomène de la cybercriminalité[11] articulée d'une part autour de la modernisation des instruments de répression de la cybercriminalité (I) et d'autre part autour de l'amélioration de la procédure pénale contre la cybercriminalité (II)

Paragraphe I : La modernisation des instruments de répression de la cybercriminalité

En vue de garantir l'effectivité de la politique de modernisation du droit pénal classique, le législateur l'a étendu à tous mécanismes du droit substantiel. Les dispositions de droit pénal substantiel de la loi ont été intégrées au Code pénal[12].La reconstruction du droit pénal envisagé a concerné pour l'essentiel, les technqiues de l'incrimination pénale (I) et de la responsabilité pénale (II)

I. La modernisation des incriminations pénales

La stratégie de modernisation des qualifications du droit pénal traditionnel a eu pour objectif principal de remédier aux situations de vide juridique et d'inadaptation juridique qui caractérisait l'édifice pénal classique[13]. Aussi, a-t-il été envisagé d'une part de créer de nouvelles infractions spécifiques aux TIC (A) et d'autre part d'adapter les infractions classiques aux TIC (B)

A. L'adoption d'incriminations nouvelles spécifiques aux TIC

La loi du 25 janvier 2008 a élaboré une stratégie de comblement des vides législatifs pour conjurer le développement des paradis numériques au Sénégal[14]. Les grands axes de cette option législative se sont articulés autour de la protection pénale des

---

9 V. la loi française dite loi Godfrain n° 88-19 du 5 janvier 1988 du 5 janvier 1988 relative à la fraude informatique (J.O.R.S du 6 janvier 1988, p. 231), modifiée par la loi n° 2004-575 du 21 juin 2004, pou r la confiance dans l'économie numérique (LCEN) (J.O.R.S du 22 juin 2004, p. 11568), et la loi belge du 28 novembre 2000, relative à la criminalité informatique, modifiée par la loi du 15 mai 2006.

10 G. RIVES, Le droit criminel sénégalais, R.S.D, Juin 1974, n° 15, 7e année, p. 45 ; ND. FALL, Le droit pénal africain à travers le système sénégalais, EDJA, 2003, p. 13.

11 Sur les soubassements théoriques de la réforme, M. DELMAS-MARTY, Les grands systèmes de politique criminelle, Paris, PUF 1992, p. 305-306 ; du même auteur, Modèles et mouvements de politique criminelle, Paris, Economica, 1983, p.159 et s. ; A. CISSE, Les déterminants juridiques à la promotion des technologies de l'information et de la communication (TIC) au Sénégal : enjeux, perspectives et méthodologie, Revue trimestrielle d'informations sur les télécommunications, la régulation et la recherche de l'ARTP, Octobre, novembre, décembre 2006, p.20 et s.

12 V. art. 1e de la loi du 25 janvier 2008, portant sur la cybercriminalité.

13 P.A TOURE, L'audit des normes applicables à la cybercriminalité, Actes, Séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal* », Dakar, 29 et 30 août 2005, p. 109.

14 Sur le spectre des paradis informatiques, V. M. THIOBANE, Le paradis pénal du cyberspace : www.osiris.sn/article2085.html

systèmes informatiques et des données informatiques, de la répression des abus de dispositifs et des infractions informatiques.

1. La protection pénale des systèmes informatiques

Le législateur a proposé de donner une définition à la notion de « *système informatique* » avant de décliner les différentes atteintes aux systèmes informatiques.

a. La notion de système informatique

Selon l'article 431-7 CP issu de la loi sur la cybercriminalité, on entend par « système informatique » : « *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* ». Cette approche du système est conforme aux définitions données à cette notion par la convention de Budapest sur la cybercriminalité du 23 novembre 2001 et par la décision cadre du conseil de l'Union européenne du 24 février 2005 relative aux attaques visant les systèmes d'information. Récemment, un jugement du Tribunal des Flagrants Délits de Dakar du 18 septembre 2009[15] a déjà assimilé un ordinateur pris isolément à un système informatique au sens de la loi. Il a été également jugé qu'un terminal de paiement électronique constitue un système informatique[16].

b. Les atteintes aux systèmes informatiques

La loi de 2008 a érigé en valeurs pénalement protégées, la confidentialité et l'intégrité des systèmes informatiques.

. Les atteintes à la confidentialité des systèmes informatiques

La confidentialité des systèmes informatiques est garantie par deux infractions :

- L'accès frauduleux à un système informatique « *hacking* ». L'article 431-8 CP érige en infraction le piratage informatique. Ce texte dispose que: « *quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique…* ». D'après un jugement du Tribunal des Flagrants délits de Dakar du 18 septembre 2009[17] : « *l'accès frauduleux à un système consiste à une intrusion, une pénétration par une personne dans le système sans y être autorisé, à l'aide de manipulations ou de manœuvres quelconques, c'est-à-dire à l'établissement d'une communication avec le système* »
- Le maintien frauduleux dans un système : L'article 431-9 CP sanctionne « *quiconque se sera maintenu ou aura tenté de se maintenir frauduleusement dans tout ou partie d'un système informatique (…*)». Il s'agit d'un délit continu.

. Les atteintes à l'intégrité des systèmes informatiques

Cette infraction informatique est prévue par l'article 431-9 CP. En vertu de ce texte : « *quiconque aura entravé ou faussé ou aura tenté d'entraver ou de fausser le*

---

15 V. T.R.H.C Dakar, n°4241/ 09 du 18 septembre 2009 , jugement inédit.

16 TRHC Dakar, 2e Ch. Corr., 21 janvier 2010, Affaire Fulgence BAHI, jugement inédit.

17 V. T.R.H.C Dakar, n°4241/ 09 du 18 septembre 2009, jugement précité.

fonctionnement d'un système informatique sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs »
Ce délit protège les systèmes contre les infections informatiques qui sont programmes destinés à perturber le fonctionnement ou à détruire les éléments indispensables leur fonctionnement normal (virus, informatique, chevaux de Troie…)

. Les atteintes à la disponibilité des systèmes informatisées
Ces atteintes ont pour siège l'article 431-9 CP qui incrimine « *quiconque aura accédé ou tenté d'accéder frauduleusement, introduit ou tenté d'introduire frauduleusement des données dans un système informatique* ». Ce délit protège les systèmes contre des changements frauduleux d'état.

2. La protection pénale des données informatisées
Le législateur a au préalable envisagé de définir la notion de « *données informatisées* » avant de décliner les différentes atteintes à ces données.

a. Le concept de donnée informatisée
Selon l'article 431-7 CP l'expression «*données informatisées*» désigne : « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique* ». Il s'agit de la représentation numérisée de l'information. Cette définition reprend presque fidèlement celle de l'article 1e de la convention de Budapest.

b. Les atteintes aux données informatisées.
Les infractions relatives aux données informatisées se déclinent autour des atteintes à la confidentialité et des atteintes à leur intégrité.

- **Les atteintes à l'intégrité des données informatisées.**

L'intégrité des données est garantie par le délit d'interception frauduleuse de données informatisées prévu par l'article 431-12 CP. Ce texte réprime le fait d'intercepter ou de tenter 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. Cette infraction garantit le secret des données informatisées, lors de leur transmission, conformément à l'article 13 de la constitution sénégalaise du 7 janvier 2001, consacrant le principe du secret des correspondances électroniques.

- **Les atteintes à la disponibilité des données informatisées.**

L'article 431-13 CP sanctionne l'endommagement, l'altération, la modification la détérioration, l'effacement frauduleux de données informatisées.
Ces atteintes à l'intégrité des données assurent une protection aux données similaires à celle dont bénéficient les biens matériels classiques contre les destructions dégradations et dommages[18].

3. Les infractions informatiques.
Les infractions informatiques visent la falsification informatique et la fraude informatique.

18 V. art. 406 et s. du Code pénal.

a. La falsification de données informatiques.

L'article 431-14 CP sanctionne sous la qualification de falsification informatique, le fait de produire ou de 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.

Cette infraction protège l'authenticité des données informatisées, à l'image du faux du droit commun. Avant l'adoption de la loi sur la cybercriminalité, la 1e Chambre Correctionnelle du Tribunal Régional de Dakar dans l'affaire de la Direction du Traitement Automatique de l'Information (DTAI) rendue le 5 septembre 2008[19], avait admis, de façon assez surprenante, la possibilité d'un faux portant sur des données informatiques.

L'article 431-14 CP érige en infraction l'usage de faux informatique, consistant à faire usage en connaissance de cause des données contrefaites.

b. La fraude informatique

L'article 431-1 CP sanctionne « q*uiconque aura obtenu frauduleusement, pour soi-même ou pour autrui, 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* ». Cette infraction tend à renforcer la protection des biens (argent) contre les manipulations informatiques réalisées en vue de porter atteintes aux biens d'autrui.

Mais, le droit pénal sénégalais présente à ce niveau une particularité par rapport à la Convention de Budapest. En effet, l'article 431-8 alinéa 2 CP sanctionne une forme particulière de fraude informatique constituée lorsque le fraudeur « *se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique* ». Dans l'affaire Fulgence BAHI[20], la 2e chambre Correctionnelle du Tribunal Régional Hors Classe de Dakar a jugé que le fait pour une personne d'utiliser une carte de paiement falsifiée, en accédant aux terminaux de paiement électronique (TPE) d'une banque, installés dans une bijouterie en se faisant remettre des bijoux d'un montant de 07 millions de francs CFA, constitue le délit prévu par l'article 431-8 alinéa 2 du CP.

4. La répression des autres abus.

Ces infractions particulières ayant pour objet de prévenir la commission des infractions informatiques. Il s'agit des abus de dispositifs, de l'association de malfaiteurs informatiques et de la tentative de certains délits informatiques.

a. Les abus de dispositifs

Les abus de dispositifs consiste selon l'article 431-32 CP à produire, à vendre, importer, détenir, diffuser, offrir, céder ou mettre à disposition un équipement, un programme informatique, tout dispositif un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système

19 V. T.R.H.C.Dakar, n° 499/ 2008 du 5 septembre 2008 , affaire de la Direction du Traitement Automatique de l'Information (DTAI), jugement inédit.

20 TRHC Dakar, 2e Ch. Corr., 21 janvier 2010, Affaire Fulgence BAHI, jugement inédit.

informatique ou donnée conçue ou spécialement adaptée pour commettre des infractions contre les systèmes ou les données.

b. L'association de malfaiteurs informatiques

L'association de malfaiteur informatique prévue par l'article 431-33 CP, réprime le fait de participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la loi sur la cybercriminalité.

Inspirée du droit commun de l'association de malfaiteurs des articles 238 et s. CP, cette nouvelle infraction traduit le souci du législateur de frapper pénalement certains comportements cybercriminels placés au début de l'iter criminis, qui ne peuvent être qualifiés ni de tentative, ni de complicité.

Elle présente en outre, le mérite d'assurer une défense de la société contre le fléau que représentent les organisations et groupements de cybercriminels comme les « *cyberfraudeurs* » qui, de plus en plus forment des bandes organisés, surtout en matière d'escroquerie en ligne[21].

c. La répression de la tentative des délits informatiques

Les articles 431-8 à 431-16 du CP incriminent la tentative des infractions informatiques prévues par la loi, à l'exception du faux et de la fraude informatique. Cette omission constitue une lacune qu'il importe de corriger.

4. Les infractions se rapportant au contenu

Ces infractions concernent la pornographie infantile et les actes de nature raciste et xénophobe commis par le biais d'un système informatique

a. La pornographie infantile

L'ampleur du phénomène de la pédopornographie qui a fini par prendre les propositions d'un véritable fléau, a incité le législateur à proposer de conceptualiser la notion de « pornographie *infantile* » avant de prévoir des infractions spécifiques à ce phénomène.

. La notion de « pornographie infantile »

Selon l'article 431-7 CP la « *pornographie infantile* » vise : « *toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite* » .

Cette approche très extensive de la pornographie infantile, reprend en substance celle proposée par la convention européenne sur la cybercriminalité.

. Les infractions prévues

Le législateur a adopté des infractions nouvelles qui tendent à protéger les mineurs d'une part contre le risque d'exploitation sexuelle et d'autre part contre le risque d'exposition des mineurs à des contenus pédopornographiques.

- Le risque d'exploitation sexuelle des mineurs

21 Ch. CORNEVIN, L'arnaque à la nigériane, in « *la délinquance électronique* », Problèmes politiques et sociaux, n° 953, octobre 2008, p. 59

L'article 431-34 CP incrimine la production, l'enregistrement, l'offre, la mise à disposition, la diffusion, la transmission d'une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique. Ce texte a pour objet de lutter contre les producteurs de pornographie infantile, à savoir les réseaux pédopornographes et éditeurs de sites de pornographie infantile.
Au titre des comportements des consommateurs de pornographie infantile, l'article 431-35 du CP frappe pénalement l'action de se procurer à soi même ou à autrui, l'importation ou l'exportation d'une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.
En outre, l'article 431-36 alinéa 1e CP pénalise la seule possession d'une image ou d'une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.

- Le risque d'exposition des mineurs à des contenus pédopornographiques

La protection des mineurs contre le risque d'exposition à des contenus à caractère pédopornographique est assurée par le délit de facilitation de l'accès à des images, documents ou représentation présentant un caractère de pornographie infantile à un mineur (article 431-36 al. 2 CP)

b. Les actes de nature raciste et xénophobe commis par le biais d'un système informatique

Ces infractions sont inspirées du Protocole additionnel à la Convention sur la cybercriminalité sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques du 7 novembre 2002. Mais, au préalable le législateur a entrepris de définir la notion de raciste et xénophobe en matière en matière des technologies de l'information et de la communication.

. La notion de raciste et xénophobe en matière en matière des technologies de l'information et de la communication

L'article 431-7 CP définit cette notion comme « *tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure ou cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes* ». Cette notion se rapproche du concept de « *matériel raciste et xénophobe* » auquel fait référence le Protocole additionnel à la convention sur la cybercriminalité sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

. Les actes prohibés

La loi sanctionne plusieurs comportements :

- La création, le téléchargement, la diffusion ou mise à disposition d' écrits, de messages, photos, dessins ou de toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique (article 431-38 CP)
- La menace et l'insulte commises par le biais d'un système informatique, de commettre une infraction pénale, 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 dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques (article 431-39 et 431-40 CP)

- La négation, l'approbation ou la justification d'actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique (article 431-41 CP)

B. L'adaptation des incriminations classiques aux TIC

La stratégie d'adaptation des actes infractionnels au particularisme de la cybercriminalité s'est manifestée par une extension de l'objet des infractions contre les biens (1) et par un élargissement des moyens de publication dans les infractions de presse (2).

1. L'élargissement de l'objet des infractions contre les biens

Devant les lacunes de la législation classique essentiellement orientée vers la protection des biens matériels, le législateur a envisagé d'intégrer l'information dans l'assiette de certaines atteintes aux biens[22].

. Le vol d'information. L'article 431-53 CP disposant que: « *La soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol* », consacre la théorie du vol d'information, en tranchant le débat sur le statut pénal de l'information[23]. Avant l'entrée en vigueur de la loi sur la cybercriminalité, le jugement du 9 mai 2006 du Tribunal Régional Hors Classe de Dakar, dans l'affaire dite de la Clinique du Cap[24] confirmé par l'arrêt de la Cour d'Appel du 16 avril 2007[25] avait déjà admis la possibilité d'un vol portant sur des données électroniques contenues dans serveur, par simple copiage.

. L'escroquerie d'information. L'article 431-56 CP prévoit l'escroquerie d'information, en intégrant les « *informations personnelles, confidentielles ou celles qui sont protégées par le secret professionnel* » dans l'objet de ce délit ; ce qui se traduit par une dématérialisation de l'infraction d'escroquerie.

. Le recel d'information. L'article 431-57 CP pose la possibilité d'un recel portant sur une information[26]. La nouvelle législation a le mérite de dissiper l'ambiguïté qui caractérisait la jurisprudence de la 1e chambre correctionnelle du Tribunal Régional Hors Classe de Dakar. En

---

22 Sur cette question, S. JACOPIN, Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse, RDP, Avril 2001, p. 6

23 Sur le débat du vol d'information, M.P LUCAS de LEYSSAC, Une information seule est-elle seule susceptible de vol ou d'une autre atteinte juridique aux biens, D. 1985.Chron. p. 51 ; M. CHAWKRI, Le vol d'informations : quel cadre juridique aujourd'hui ?, p. 18, disponible à l'adresse suivante : http://www.droit-tic.com/pdf/vol_information.pdf; J.DEVEZE, Le vol des « biens informatiques », JCP. 1985, I, 3210, n° 13 ; D. CIOLINO-BERG, Vol d'information sur Internet, Comm. Com. électro. nov. 2003, p. 22.

24 T.R Hors Classe Dakar n°1981 du 9 mai 2006, affaire de la Clinique du Cap, jugement inédit.

25 V. C A Dakar, n°680 du 16 avril 2007, arrêt inédit .

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

effet, après avoir rejeté la possibilité d'un recel portant sur une information provenant de la violation du secret de l'instruction dans l'affaire Madiambal DIAGNE rendue le 21 novembre 2006[27], les juges ont admis la possibilité d'un recel d'une information provenant d'un délit d'initié dans le jugement rendu 1e avril 2008[28]. Cette dernière décision a d'ailleurs été confirmée en toutes ses dispositions par un arrêt de la Cour d'Appel de Dakar du 24 juillet 2009[29].

2. L'extension des moyens de publication des infractions de presse

Devant la recrudescence des infractions de presse[30] réalisées sur les réseaux numériques (sur le web, les forums de discussion, ou dans les services de presse en ligne…), les rédacteurs de la loi de 2008, ont proposé d'intégrer expressément les « *moyens de communication numérique par voie électronique* », notamment les réseaux numériques comme l'Internet dans les moyens de diffusion publique, énumérés par l'article 248 CP (article 431-58 CP)

Dans l'affaire Robert Sagna, rendue par le Tribunal régional de Ziguinchor le 06 janvier 2004[31], les juges avaient déjà admis 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.

II. La consécration de la responsabilité pénale des personnes morales.

L'article 431-62 CP a consacré le principe de la responsabilité pénale des personnes morales pour les infractions prévues par la dite loi, commises pour leur compte par leurs organes ou représentants. Il s'est surtout agit de prendre en compte la diversité des acteurs du cyberespace susceptibles de voir leur responsabilité engagée en raison d'actes répréhensibles.

Les peines encourues sont l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques , l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique, la fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés, ou même la dissolution de la personne morale.

Paragraphe II : L'amélioration de la procédure pénale contre la cybercriminalité

Devant le constat de l'inadéquation des mécanismes procéduraux traditionnels à la conduite des investigations dans l'environnement électronique[32], les auteurs de la loi

---

27 V. TRHC Dakar, n°5310 du 21 novembre 2006, affair e Madiambal DIAGNE, jugement inédit.

28 TRHC Dakar, 1e avril 2008, jugement inédit.

29 V. CA Dakar, n°555 du 24 juillet 2009, jugement in édit.

30 V. D. NDOYE, La liberté d'opinion et d'expression au Sénégal. La doctrine politique et les textes, éditions du CAFORD, 2003 ; O SEYE, La procédure en matière de délits de presse, Nouvelles Annales Africaines, n°2, 2008, p. 349.

31 TR Ziguinchor, 06 janvier 2004, Affaire Robert SAGNA, jugement inédit

32 V. Nd. DIOUF, 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 ; J-P MALONGA YOUNAS, La répression des agissements liés aux nouvelles technologies de l'information : l'exemple

sur la cybercriminalité, intégrant les nouvelles dispositions procédurales au Code de procédure pénale[33], ont procéder d'une part à l'aménagement des techniques procédurales traditionnelles (A) et d'autre part à l'institution de nouvelles procédures pénales (B)

A. L'aménagement des instruments probatoires classiques

L'adaptation des outils de procédure classiques a permis de consacrer la perquisition et la saisie électronique (1) et d'admettre la preuve électronique en matière pénale (2)

1. La consécration de la perquisition et de la saisie informatique

L'article 677-36 CPP a étendu les prérogatives du juge d'instruction, en l'habilitant à opérer une perquisition dans un système informatique ou à une partie de celui-ci, lorsque des données stockées dans un système informatique sont utiles à la manifestation de la vérité.

Mais, si les données sont stockées dans un autre serveur 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.

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, l'article 677-37 CPP habilite le magistrat instructeur à copier ces données, ainsi que celles qui sont nécessaires pour les comprendre, sur des supports de stockage informatique pouvant être saisis et placés sous scellés[34].

Ce nouveau dispositif de perquisition et de saisie électronique ture principalement sa source d'inspiration de la convention de Budapest et de la loi belge sur la criminalité informatique.

2. L'admission de la preuve électronique en matière pénale

Malgré, l'admission du principe de la liberté de preuve applicable en droit pénal commun[35], l'article 677-40 CPP a posé le principe de l'admission de la preuve électronique an matière pénale « *sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ». Les enjeux liés au recours judiciaire à la preuve électronique (caractère manipulable et volatilité du numérique) ont largement justifié un encadrement juridique de la preuve électronique en matière pénale.

B.L'institution de nouvelles procédures spécifiques aux TIC

Ces nouvelles procédures renvoient à la conservation rapide de données archivées (1) et de l'interception de données informatisées (2)

1. La conservation rapide de données archivées informatisées

---

du Congo, Thèse, Dakar 2003, p. 295; Ph. BELLOIR, L'application des règles de procédure pénale aux infractions commises sur Internet, (1e partie), Expertises, juillet 2002, p. 257.

33 V. art. 2 de la loi du 25 janvier 2008, portant sur la cybercriminalité.

34 Th. VERBIEST et E. WERY, Le droit de l'Internet et de la société de l'information. Droits européen, belge et français, Larcier, 2001, p. 34-35

35 V. art. 414 alinéa 1e du Code de Procédure Pénale, « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* »

Compte tenu de l'évanescence des données informatiques qui sont souvent nécessaires à l'enquête, l'article 677-35 CPP a habilité le juge d'instruction à 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, lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification. Le gardien des données est par ailleurs tenu au secret professionnel et peut encourir les peines de la violation du secret professionnel.

2. L'interception de données informatisées

L'article 677-38 CPP permet enfin aux magistrats, si les nécessités de l'information l'exigent d'utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications sur son territoire, 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 ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est en outre tenu de garder le secret.

Conclusion

En définitive, la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité a apporté de grandes innovations dans l'arsenal pénal sénégalais. Ce texte de droit interne a fini par secréter un véritable cyberdroit pénal au Sénégal, régulateur de la société sénégalaise de l'information à dimension humaine inclusive ouverte, dérogatoire à bien des égards des principes du droit pénal commun.

Mais, la nature planétaire de la cybercriminalité exige une mobilisation de la communauté internationale contre ce phénomène international.

Au Sénégal, les experts réunis lors du Séminaire « *informatique et libertés : quel cadre juridique pour le Sénégal ?* » organisé en août 2005[36] , après avoir rejeté la proposition de l'adoption d'un instrument juridique africain de traitement et de répression de la cybercriminalité[37], ont conclu que l'internationalisation du traitement de la cybercriminalité gage de l'harmonisation de la cyberépression, devrait passer par l'adhésion du Sénégal à la Convention de Budapest sur la cybercriminalité du 23 novembre 2001[38] ; ce traité étant ouvert à l'adhésion des Etats non Membres du Conseil de l'Europe et n'ayant pas participé à son élaboration[39].

---

36 Les conclusions du séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal* ? », organisé les 29 et 30 août 2005 par l'ADIE, A.CISSE, Quel cadre juridique pour le Sénégal ? Éléments de synthèse, séminaire *Informatique et libertés, quel cadre juridique pour le Sénégal ?* A.D.I.E, Dakar 29 et 30 août 2005 ; également plus récemment, A. CISSE, La cybersécurité : les moyens juridiques de protection, in « *Bâtir un espace numérique de confiance en Afrique* », Conférence régionale africaine sur la cybersécurité, Youmoussoukro, du 17 au 20 novembre 2008.

37 L. KALINA, Cybercriminalité : quels outils pour l'Afrique, 21 janvier 2006, disponible à l'adresse suivante : http://www.blogg.org/blog-35519-themes-seminaire_afrique_et_cybercriminalite-64801.html

38 J. COSTE, La convention du Conseil de l'Europe du 8 novembre 2001 : premier traité international contre la « cybercriminalité », Lamy droit de l'informatique et des réseaux, n° 142, décembre 2001 , p .

Le Gouvernement de la République du Sénégal conscient des enjeux liés au renforcement de la lutte internationale contre la cybercriminalité, a manifesté une volonté d'adhérer à cet instrument juridique international. Aussi, la mise en œuvre effective de cette volonté politique et sa traduction législative devraient contribuer à inscrire le Sénégal dans la coopération internationale contre la criminalité du cyberespace, qui constitue une sérieuse menace pour la sécurité des réseaux et développement d'une société de l'information.

Papa Assane TOURE
Magistrat
Juge au Tribunal Régional Hors Classe de DAKAR (Sénégal)
Doctorant en Droit Privé et Sciences Criminelles
email : papaassanetoure@yahoo.fr

1 ; G. DE VEL, La convention sur la cybercriminalité, in G. CHATILLON (Dir), « l*e Droit International de l'Internet »*, Bruxelles, Bruyant, 2002, p. 237 et s

39 V. article 37 de la Convention de Budapest