Organisation pour l'Harmonisation en Afrique du Droit des Affaires
Organization for the Harmonization of Business Law in Africa
Organizacion parala Armonizacion en Africa de la Legislacion Empresarial
Organização para a Harmonização em Africa do Direiton dos Negocios

ECOLE REGIONALE SUPERIEURE
DE LA MAGISTRATURE (ERSUMA)

FORMATION DES MAGISTRATS, AVOCATS ET OFFICIERS DE POLICE JUDICIAIRE DES SERVICES D'INTERPOL

Thème *La législation communautaire intégrée en matière de criminalité d'affaires*

- *Criminalité transfrontalière*
- *Cibercriminalité*
- *Propriété intellectuelle*

du 02 au 05 septembre 2013

« LA CYBERCRIMINALITE DANS LES LEGISLATIONS COMMUNAUTAIRES INTEGREES EN AFRIQUE »

Papa Assane TOURE
Magistrat
Conseiller Technique au Ministère de la Justice
Docteur en Droit Privé et Sciences Criminelles
Expert en Cyberdroit et Formateur à l'ERSUMA.
papaassanetoure@yahoo.fr

ORGANISATION POUR L'HAMONISATION EN AFRIQUE DU DROIT DES AFFAIRES (OHADA).

ECOLE REGIONALE SUPERIEURE DE LA MAGISTRATURE (ERSUMA)

Formation des Magistrats, Avocats, et Responsables des Officiers de Police Judiciaire des services d'Interpol.

« La cybercriminalité dans les législations communautaires intégrées en Afrique »

Papa Assane TOURE
Magistrat
Conseiller Technique au Ministère de la Justice
Docteur en Droit Privé et Sciences Criminelles
Expert en Cyberdroit et Formateur à l'ERSUMA.
papaassanetoure@yahoo.fr

INTRODUCTION

Le développement contemporain des technologies de l'information et de la communication (TIC) constitue un tournant majeur de la civilisation humaine. L'illustration la plus parfaite de l'essor des technologies numériques est sans nul doute l'avènement du réseau Internet[1].

Malgré le faible taux d'accès aux TIC en Afrique[2], le passage de l'analogique au numérique a changé profondément la physionomie de la société traditionnelle qui s'est très vite transformée en une société de l'information[3].

Mais, l'essor des réseaux numériques a entrainé l'apparition d'une nouvelle forme de criminalité charriée par les premières lueurs de la société africaine de l'information, appelée « *cybercriminalité* ». Le cyberespace est devenu criminogène. En effet, l'espace dématérialisé qu'offrent les TIC, notamment Internet, est de plus en plus le lieu virtuel de commission de divers agissements répréhensibles[4]. Le surgissement en Afrique de la cybercriminalité est symbolisé par le phénomène de l'escroquerie en ligne devenue une véritable menace pour le développement dans certains pays[5].

Malgré les difficultés de conceptualisation du cybercrime[6], il est possible de retenir un modèle conceptuel du phénomène cybercriminel résultant des travaux du onzième congrès des Nations Unies pour la prévention du crime et la justice pénale du 18 au 25 avril 2005. Selon les conclusions du congrès, l'infraction informatique recouvre : « *tout comportement interdit par la législation et/ou par la jurisprudence qui: a) est dirigé contre les technologies de calcul électronique et de communication elles-mêmes; b) fait intervenir l'utilisation de technologies numériques pour la commission de l'infraction; et c) suppose l'utilisation incidente d'ordinateurs pour la commission d'autres infractions* »[7].

---

1. A. DUFOUR, *Internet*, « *Que sais-je* ? », 8e édition, Paris, 2000 ; J. BOYER, « La révolution d'Internet », *P.A*, 10 novembre 1999, n° 224, p. 11.

2 P.DANDJINOU, *Les nouvelles technologies de l'information et de la communication (TIC) et les objectifs du Millénaire pour le développement en Afrique*, p. 5590 ; A. BA, *Internet, cyberespace et usages en Afrique*, *L'Harmattan*, 2003, p. 11.

3. L.COSTES, « Vers une nouvelle société de l'information », *Lamy droit de l'informatique et des réseaux*, Bull. actualité, J. février 1996, n° 78 p.1.

4 W. CAPELLER, « Un net pas très net », in « *l'immatériel et le droit* », *Arch. phil. dr*, n° 143, p. 167 ; M. QUEMENER et J. FERRY, *Cybercriminalité. Défi mondial*, 2e édition, *Economica*, 2009, p. 1 ; M.QUEMENER, « Cybercriminalité : aspects stratégiques et juridiques », in « *De la cybercriminalité à la cyberguerre* », *Rev.Déf.nat.séc.coll*, mai 2008, p. 23

5 Ch. CORNEVIN, « L'arnaque à la nigériane », in « *la délinquance électronique* », *Problèmes politiques et sociaux*, n° 953, octobre 2008, p. 59 ; S. ROUJA, « De quelques faux clics et vrais escrocs », *R.L.D.I*, novembre 2008, p. 85 et s. ; J. J. BOGUI, « La cybercriminalité, menace pour le développement. Les escroqueries Internet en Côte d'Ivoire », *Afrique contemporaine*, 2010/2 n° 234, p. 155-170.

6 En ce sens, M. QUEMENER et Y. CHARPENEL, *Cybercriminalité ; Droit pénal appliqué*, *Economica*, Paris, 2010, p. 7, n° 27.

7 Onzième Congrès des Nations-Unies pour la prévention du crime et le traitement des délinquants, Bangkok, 18-25 avril2005, disponible sur http : //www. un.org/ events /11thcongress /docs /bkkcp15f.pdf

Il s'agit ainsi des comportements infractionnels qui supposent l'implication des technologies numériques (systèmes, logiciels, données informatiques, cartes bancaires, Internet etc.) dans le processus criminel soit objet soit comme moyen de commission d'infractions.

La cybercriminalité présente des particularités criminologiques certaines. En effet, il est devenu classique de la présenter sous les traits d'une délinquance marquée essentiellement par l'immatérialité de son objet[8], l'internationalité de ses implications, la fugacité de ses contenus et par l'anonymat de ses acteurs.

Mais, la cybercriminalité revêt souvent la nature d'une criminalité d'affaires et se mue en une cybercriminalité d'affaires[9]. Les agissements cybercriminels sont souvent le fait d'acteurs hyper adaptés du cyberespace qui anticipent avec une grande rapidité les évolutions technologiques à la recherche de « *l'argent des autres* »[10]. Les hackers ne se limitent plus à pénétrer dans un système informatique depuis leurs chambres pour le simple plaisir ou par défi ; ils en profitent pour modifier, introduire ou supprimer des données en vue de détourner des fonds appartenant à autrui par simple clic d'ordinateur « *sans se salir les mains* ».

Ces spécificités de la cybercriminalité ont vite favorisé un brouillage des repères des mécanismes traditionnels d'appréhension de la criminalité. Les réponses traditionnelles du système pénal, conçues et élaborées pour un environnement matérialisé et national, se sont vite révélées inadaptées pour saisir la délinquance de l'âge du numérique[11]. Ces difficultés d'appréhension juridique de la cybercriminalité dans l'ordre pénal ont été aggravées par la rigueur des méthodes d'interprétation pénale postulant une interprétation stricte de la loi pénale[12].

Pourtant, à l'image de l'espace terrestre maritime ou aérien, le cyberespace n'est pas une zone de non droit et ne saurait être rebelle à toute activité régulatrice de ses contenus[13].

---

[8] M.VIVANT, « L'immatériel, nouvelle frontière pour un nouveau millénaire », *J.C.P*, éd.G, 2000, I. 193 ; P. SIRINELLI et M. VIVANT, « De l'irrésistible ascension de l'immatériel », *R.L.D.I*, n°1, janvier 2005, p. 3

[9] D.SZABO, *La criminalité d'affaires : aspects criminologiques, l'année sociologique*, *P.U.F*, 1981, p. 290. Ce criminologue définit le crime d'affaires comme étant « *un acte illégal perpétré sans le recours à la contrainte physique, usant de la dissimulation et ayant une intention frauduleuse, en vue de l'obtention de propriétés ou d'avantages monétaires ou pour éviter des pertes d'argent ou de propriétés par le truchement d'avantages obtenus dans les affaires ou à titre personnel* ».

[10] Depuis l'aube du XIX[e] siècle, les affaires sont « *l'argent des autres* » selon l'aphorisme dont la paternité est attribuée à Alexandre DUMAS fils, V. sur ce point, F.-J PANSIER, *Le droit pénal des affaires*, « *Que sais-je ?* », *P.U.F*, 2[e] édition 1992, p. 3.

[11] En ce sens, 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 ; ND. DIOUF, « La procédure pénale à l'épreuve des nouvelles technologies de l'information », *Rev. Ass. sén. dr. pén*, n° 5, 6,7 et 8, 1997-1998, p.13 ; P.A TOURE, « L'audit des normes applicables à la cybercriminalité », Communication, Séminaire, « *Informatique et libertés, quel cadre juridique pour le Sénégal ?* », ADIE, Dakar, 29 et 30 août 2005.

[12] V. P. A. TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*, Thèse Doctorat, Saint-Louis, 2010, n° 25

[13] Ph. AMBLARD, *Régulation de l'Internet, l'élaboration des règles de conduite par le dialogue internormatif*, Facultés Universitaires Notre Dame de la Paix de Namur, *Bruyant*, Bruxelles, 2004, p. 1

En Afrique, les instances des certaines organisations communautaires ont pris conscience des défis posés par la cybercriminalité dans le vie des affaires, en apportant des réponses de politique criminelle à ce fléau. Dans le cadre de l'Union Economique et Monétaire Ouest Africaine (UEMOA), on peut citer la loi uniforme n° 2008-48 du 3 septembre 2008, relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement[14].

La Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) a adopté un Acte Additionnel A/SA.2/01/10 du 16 février 2010 portant transactions électroniques dans l'espace de la CEDEAO et un Acte Additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel.

Lors de sa 66e session tenue à Abuja (Nigéria) les 17 à 19 août 2011, le Conseil des Ministres de la CEDEAO a adopté la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

Dans l'espace de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) et de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC), certains instruments juridiques abordent certains enjeux liés au phénomène cybercriminel. Il s'agit de la Directive n°07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communications électroniques au sein de la CEMAC et du Règlement n° 02/03-CEMAC-CM du 4 avril 2003 relatif aux systèmes, moyens et incidents de paiement qui incrimine les atteintes aux systèmes de paiement.

Dans l'espace de l'Afrique Centrale, la deuxième réunion des Ministres en charge des télécommunications et TIC des Etats membres de la CEEAC tenue à Ndjamena le 22 avril 2010 a chargé le Secrétaire Général de la CEEAC de préparer un texte sur la cybercriminalité. A cet égard, un Projet de loi-type CEMAC/ CEEAC sur la lutte contre la cybercriminalité a été élaboré.

A l'échelle continentale, lors de la conférence de l'Union Africaine tenue à Khartoum (Soudan) en septembre 2012, le projet de Convention de l'Union Africaine sur la confiance et la sécurité dans le cyberespace a été validé par les Ministres en charge de la communication et des TIC qui l'ont soumis à la Commission de l'UA pour adoption. Ce texte constituera le premier juridique africain de lutte contre la cybercriminalité.

Ces textes sont inspirés des standards internationaux, à l'image de la Convention européenne de Budapest sur la cybercriminalité du 23 novembre 2001 et du Guide de la cybersécurité pour les pays en développement de l'Union Internationale des Télécommunications (UIT) (2007). Certains Etats africains ont également entrepris des

[14] J.O.R.S, n° 6453, du 7 février 2009, p. 120

chantiers de réforme de leur cadre juridique. Il s'agit du Sénégal (loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité) et du Cameroun (loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité) et de la Côte d'Ivoire a récemment entrepris un chantier d'élaboration d'une loi sur la cybercriminalité.

En Afrique, ces cyberdroits pénaux communautaires ont envisagé d'apporter de grandes innovations dans les systèmes pénaux des Etats Membres. En effet, en vue de lutter efficacement contre la cybercriminalité d'affaires, les instruments communautaires africains ont d'une part adopté de nouvelles cyberinfractions d'affaires (I) et ont d'autre part prévu des techniques d'investigations contre de telles infractions (II)

I. L'ADOPTION DE NOUVELLES CYBERINFRACTIONS D'AFFAIRES.

En Afrique, les principales infractions pénales à la disposition des magistrats et des officiers de police judiciaire sont pour l'essentiel héritées du système colonial. Ces incriminations pénales conçues pour la répression de formes traditionnelles de criminalité se sont révélées inappropriées au traitement de la cybercriminalité d'affaires.

Quoi qu'il en soit, la stratégie de modernisation des infractions envisagée est largement tributaire des schémas d'implication des TIC dans le processus criminel. En effet, les TIC peuvent être un objet de commission des délits d'affaires (**A**) ou un simple instrument de réalisation de ces actes infractionnels (**B**).

A. LES TIC : UN OBJET DE COMMISSION D'INFRACTIONS D'AFFAIRES.

En Afrique, l'apparition de la cybercriminalité d'affaires ayant pour objet les TIC a confronté les autorités judiciaires à deux situations juridiques.

Les organes répressifs se sont heurtés à une situation de vide juridique, lorsque les comportements cybercriminels avaient pour cible des valeurs nouvelles, réalisés au moyen de procédés frauduleux également nouveaux (intrusion, diffusion de virus informatiques etc.)

Par ailleurs, ils ont achoppé sur une situation d'inadaptation juridique lorsque ces mêmes agissements visant des valeurs nouvelles du cyberespace, sont commis à l'aide de procédés traditionnels connus de la législation (vol, faux, détournement etc.).

Les instruments juridiques communautaires africains ont envisagé de dissiper le malaise des magistrats et des enquêteurs, d'une part par la création d'incriminations nouvelles spécifiques aux TIC en vue de combler les vides juridiques constatés en législation (**1**) et d'autre part par l'adaptation des incriminations classiques auxdites technologies (**2**)

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

L'essor contemporain de l'informatique et des technologies numériques modernes a généré l'apparition de nouveaux « *biens* » caractérisés par leur immatérialité qualifiés par la doctrine

de « *biens informationnels* »[15] ou de « *biens informatiques* »[16]. Il s'agit des systèmes informatiques, des données informatiques, des logiciels des bases de données, des réseaux informatiques etc. Sous l'angle de l'analyse pénale, lorsque ces nouvelles valeurs sont la cible d'agissements criminels, au moyen de procédés nouveaux (accès frauduleux, diffusion de virus etc.), il en résultait un vide juridique dans les législations[17]

En Afrique, le comblement de ces vides juridiques a exigé la protection pénale des systèmes informatiques (**a**) et la protection pénale des données informatiques (**b**).

a. La protection pénale des systèmes informatiques

Dans la société contemporaine de l'information, les systèmes informatiques, lieux virtuels du traitement de l'information, occupent une place stratégique dans la vie sociale. En Afrique, la plupart des entreprises et des administrations publiques fonctionnent à l'aide de systèmes, voire de réseaux électroniques garantissant l'interconnexion entre plusieurs systèmes. Aussi, sont-ils l'objet de manipulations, d'atteintes à leur fonctionnement et de diverses fraudes[18].

La plupart des instruments juridiques africains ont prévu une protection pénale générale des systèmes informatiques. Il importera d'abord de cerner les contours de cette notion de système informatique avant d'analyser les atteintes au système informatique.

- ***La notion de système informatique***

On retrouve une définition précise du système informatique dans l'article 1[e] de la Directive de la CEDEAO du 19 août 2011 ; il s'agit de « *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* »[19].

Cette approche du système est conforme aux définitions données à cette notion par la Convention de Budapest sur la cybercriminalité du 23 novembre 2001. Il peut s'agir d'un ordinateur pris isolément, d'un distributeur automatique de billets[20], d'un smartphone, d'une carte à puce etc.

---

[15] M.VIVANT, « A propos des biens informationnels », *J .C.P*, 1984, éd. G. I. 3132.

[16] J.DEVEZE, « Le vol des biens informatiques », *J.C.P.* 1985, I ,3210 ; J-P. BUFFELAN-LANORE, « La protection des biens informatiques », *P.A*, 6 juillet 1990, n° 81.

[17] M.THIOBANE, « Le paradis pénal du cyberspace » : www.osiris.sn/article2085.html ; H.D. NDIAYE, « Législation en matière d'Internet : c'est le désert total dans notre pays » : www.osiris.sn

[18] S. DE MAUPEOU, « De la vulnérabilité à la crise des systèmes d'information », in « *la criminalité numérique* », *Cah. Séc*, 2008, n° 6, Doc. fr, p. 122.

[19] V. également, art. III-1 du Projet de Convention Africaine sur la cybersécurité ; art. 2 Projet de loi-type portant sur la lutte contre la cybercriminalité dans les Etats Membres de la CEEAC/CEMAC ; art. 1[e] loi sénégalaise n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité ; art. 4 de la loi camerounaise n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité

[20] T.R.H.C Dakar, n° 1087 du 22 mars 2011, *affaire América DAVID, inédit.* Il a été jugé d'un mis en place par la banque le Crédit du Sénégal constitue une partie du système bancaire.

Les auteurs contemporains s'accordent pour reconnaître à l'Internet la qualification de système informatique, au sens légal du terme[21]. Le contexte contemporain est marqué l'apparition d'une délinquance des réseaux et l'utilisation par les hackers de techniques très perfectionnées leur permettant de « *zigzaguer* » à l'intérieur des systèmes ou entre différents systèmes transnationaux.

Récemment, dans l'affaire « *Pneuméca* » jugée par le tribunal régional hors Classe de Dakar le 18 septembre 2009[22] les juges sénégalais ont 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[23].

Les juges sénégalais ont également eu l'occasion de considérer que le système de transfert électronique d'argent dit « *Wari* » géré par la société Cellular system international[24] ainsi que le système de l'agence de voyage Delta permettant de faire des réservations et de gérer électroniquement les billets émis au profit de clients[25] peuvent être assimilés à des systèmes informatiques au sens légal du terme.

En théorie, il n'est pas nécessaire que le système informatique soit muni d'un dispositif de sécurité pour bénéficier de la protection pénale.

Mais, en pratique, la présence d'un dispositif de sécurité (mot de passe, dispositif de cryptologie etc.) constitue un moyen pour le juge d'établir la preuve de l'élément moral des différentes atteintes aux systèmes informatiques.

- **Les atteintes aux systèmes informatiques**

Les législations communautaires africaines protègent pénalement 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 et le maintien dans un système informatique.

L'accès frauduleux à un système informatique « *hacking* » ou piratage informatique est érigé en cyberinfraction par l'article 4 de la Directive de la CEDEAO. Ce texte sanctionne « *le fait pour toute personne d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un système informatique*»

Un jugement du Tribunal régional de Dakar du 18 septembre 2009[26] *a* eu l'occasion de proposer une définition précise de l'accès à un système. Selon le tribunal : «*l'accès*

---

[21] A. HOLLANDE et X.LINANT DE BELLEFONDS, *Pratique du droit de l'informatique, Logiciels, Systèmes Internet*, 6[e]édition, Delmas, 2008, p. 350 ; E. DREYER, *Droit pénal spécial, Ellipses*, 2008, p. 365.

[22] V. T.R.H.C Dakar, n° 4241/ 09 du 18 septembre 2009, *affaire Pneuméca, jugement inédit*

[23] TRHC Dakar, 2[e] Ch. Corr., 21 janvier 2010, *affaire Fulgence BAHI, jugement inédit.*

[24] T.R.H.C Dakar, du 17 avril 2012, *affaire du système WARI*, inédit

[25] T.R.H.C Dakar, n° 4423 du 20 décembre 2011, *affaire Eric Donys SIMEU et autres*, inédit

[26] T.R.H.C Dakar, n° 4241 du 18 septembre 2009, *affaire Pneuméca précitée.*

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 »

Il peut s'agir d'un forcement d'un dispositif de sécurité, de l'utilisation d'un code d'accès ou d'une adresse Internet obtenue par fraude ou même à l'aide d'un programme espion.

Il a été jugé que constitue l'infraction d'accès frauduleux à un système le fait pour le collaborateur d'une société spécialisée dans la vente de pneumatiques d'accéder aux données de l'ordinateur du directeur commercial de ladite société à son insu, avant de se faire envoyer dans sa propre boîte électronique des informations commerciales[27].

Dans l'affaire *Eric Donys SIMEU* jugée le 20 décembre 2011, le tribunal des flagrants délits de Dakar[28] a déclaré le prévenu coupable d'accès frauduleux à un système informatique pour avoir pénétré dans le système informatique de l'agence de voyage Delta, avant de procédé frauduleusement à une réservation de billets Dakar-Atlanta-Dakar, au profit d'un père de famille et de ses deux enfants moyennant le versement de la somme de 1.600.000 francs CFA. Récemment, un jugement du 17 avril 2012 du tribunal régional hors classe de Dakar, rendu à propos de l'affaire « *Wari* », a condamné pour accès frauduleux à un système, un ancien salarié de la société, gérant le système « Wari », qui s'est introduit dans ce système avant de procéder à des transferts frauduleux d'argent au profit d'un de ses amis.

Le maintien frauduleux dans un système est prévu par l'article 5 de la Directive de la CEDEAO. Ce texte sanctionne « *le fait pour toute personne de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique*». Cette infraction réprime 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, de se maintenir dans le système au lieu d'interrompre sa connexion. Dans un arrêt de la Cour de Cassation française du 3 octobre 2007[29], un salarié avait reçu, au cours de sa période d'essai, un code confidentiel permettant de se connecter gratuitement à une banque de données commerciales. La haute juridiction a jugé qu'il avait commis le délit de maintien frauduleux dans un système informatique, en utilisant pendant plus de deux ans ce code qui n'est accessible qu'aux personnes autorisées[30].

---

[27] T.R.H.C Dakar, n° 4241/09 du 18 septembre 2009, *jugement précité*.

[28] T.R.H.C Dakar, n° 4423 du 20 décembre 2011, *affaire Eric Donys SIMEU et autres, inédit*

[29] Cass.crim. 3 octobre 2007 ; *Dr. pén*, décembre 2007, comm, p. 37, n° 158 ;

[30] M. LECARDONNEL, « Utilisation d'un code d'accès au-delà de la période autorisé : maintien frauduleux », *Expertises*, Janvier 2008, Doct, p. 26

➢ **Les atteintes à l'intégrité des systèmes informatiques**

Les atteintes à l'intégrité des systèmes sont prévues par l'article 6 de la Directive de la CEDEAO du 19 août 2011 et par l'article 5 du Projet de loi-type CEMAC/CEEAC sur la cybercriminalité. Ces textes assurent aux systèmes d'information une protection similaire à celle dont bénéficient les biens corporels classiques contre les destructions dégradations et dommages. Ce texte érige en infraction « *le fait pour toute personne d'entraver, de fausser, de tenter d'entraver ou de fausser le fonctionnement d'un système informatique* ». Cette infraction protège surtout les systèmes contre les infections informatiques qui sont des programmes destinés à perturber le fonctionnement ou à détruire les éléments indispensables à leur fonctionnement normal (virus, informatique, chevaux de Troie etc.). Au Sénégal, dans le courant du mois de janvier 2008, le site d'information nettali.com a subi des actes de sabotage informatique, à la suite de la diffusion d'un cheval de Troie envoyé depuis son forum de discussion, ce qui a occasionné pendant un certain temps, l'indisponibilité de son serveur[31].

L'entrave est un comportement réalisé au moyen d'actions positives, ayant pour résultat d'empêcher l'aboutissement du traitement informatique[32]. L'entrave suppose une action positive, à l'exclusion de simples abstentions.

Un arrêt de la Cour d'Appel de Paris du 15 mars 1994 a condamné pour entrave au fonctionnement du système informatique une personne qui avait introduit une bombe logique dans le système d'une entreprise dans le but de garantir le paiement de redevances de maintenance.

Le « *mail bombing* », consistant à un envoi massif de courriers à un serveur, peut constituer une entrave au fonctionnement du système informatique, s'il a pour effet de perturber son fonctionnement[33]. Un jugement du tribunal de grande instance du Mans du 7 novembre 2003 a déclaré coupable du délit d'entrave au fonctionnement d'un système de traitement automatisé de données, une personne qui avait envoyé en masse des mails par le biais de fausses adresses électroniques à une société, en saturant ses boites électroniques[34]

L'action de fausser le fonctionnement du système constitue une action sur ledit système qui, sans empêcher son fonctionnement, lui fait produire un résultat différent de ce qui était escompté[35]. On peut citer les chevaux de Troie, comme forme d'action de fausser le fonctionnement du système. A l'image de la légende relatant la prise de Troie par les grecs,

---

[31] 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

[32] J. P. BUFFULAN, « Les nouveaux délits informatiques », *Expertises*, n° 104, 1988, p. 101.

[33] D. FOREST, « Nouvel éclat de jurisprudence sur le mail bombing », *Expertises*, mai 2007, p. 187.

[34] T.G.I Mans 7 novembre 2003, *Gaz. Pal.* 18-20 juillet 2004, p. 4, obs. E. Barby; V. dans le même sens T.G.I Paris 24 mai 2002, disponible http://www.juriscom.net; dans le même sens, TGI Nanterre, 8 juin 2006, *Expertises*, mai 2007, p. 187.

[35] M. VIVANT (dir.), *Lamy droit de l'informatique et des réseaux*, Lamy SA, 2009, p. 1934, n° 3281

cette technique frauduleuse consiste à insérer un programme apparemment inoffensif dans un système qui sera exécuté comme partie intégrante du programme. Elle permet de modifier de façon imperceptible, soit le système d'exploitation, soit le programme lui-même[36].

b. La protection pénale des données informatiques

La Directive du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO a entrepris de conceptualiser la notion de donnée informatique avant de décliner les différentes atteintes aux données.

- **Le concept de donnée informatique**

La «*donnée informatique*» désigne « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique* »[37].

La donnée informatique est la représentation numérisée de l'information, c'est-à-dire l'information ayant fait l'objet d'un traitement informatique. Il ne s'agit que d'un support dématérialisé de l'information, en tant que message porteur de signification destiné à être communiqué (une information peut avoir pour support le papier ou la pierre ou le papyrus). Sous ce rapport, toute donnée informatique est une information, mais toute information n'est pas forcément une donnée électronique.

- **Les atteintes aux données informatiques.**

Les infractions relatives aux données informatiques s'articulent autour des atteintes à leur confidentialité et des atteintes à leur intégrité.

➢ **Les atteintes à la confidentialité des données informatiques**

La confidentialité des données est garantie par l'infraction d'interception frauduleuse de données informatiques prévue par l'article 8 de la Directive du 19 août 2011, conçu par référence au délit classique de violation du secret des correspondances écrites[38].

Ce texte réprime le fait d'intercepter ou de tenter d'intercepter frauduleusement des données informatiques par des moyens techniques 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 électroniques, lors de leur transmission, conformément au principe du secret des correspondances électroniques.

Le tribunal de grande instance de Paris a déjà, par un jugement du 2 novembre 2000[39] , admis que le courrier électronique, qui relève de la correspondance privée, est couvert par le principe du secret des correspondances dans les conditions du droit commun[40].

---

[36] M.QUEMENER et J.FERRY, *Cybercriminalité. Défi mondial*, 2e édition, *Economica*, 2009, p.2

[37] V. article 2 de la Directive du 19 août 2011.

[38] V. art. 167 du Code pénal sénégalais.

[39] T.G.I Paris 2 novembre 2000, *J.C.P*, édit. G, 2000, n° 49, Actualité, p. 2219 ; *Gaz. Pal.* 6-7 décembre 2000, p. 49 ; *D.* 2000, Inf. Rap. p. 286 ; *Expertises*, décembre 2000, p. 369 ; Adde L. RAPP, « Secret des correspondances et courriers électroniques », *D.* 2000, n° 41, Point de vue, p. III.

Mais, pour être sanctionnée, l'interception doit être effectuée sans droit. En effet, certains impératifs liés à la sécurité nationale et à l'ordre public ont incité le législateur à autoriser les autorités chargées d'une enquête judiciaire à collecter des données relatives au contenu de communications. C'est du moins ce qui ressort de l'article III-55 du Projet de convention de l'UA. Ce texte permet au juge d'instruction, 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.

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

L'article 9 de la Directive de la CEDEAO incrimine l'endommagement, l'altération, la modification la détérioration, l'effacement frauduleux de données informatiques.

Ces atteintes à l'intégrité des données assurent une protection aux données similaires à celle dont jouissent les biens matériels classiques contre les destructions dégradations et dommages, prévus par les articles 406 et s. du Code pénal sénégalais. Il n'est pas nécessaire que les données informatiques soient contenues dans le système d'information. Ces atteintes recoupent des techniques de fraude comme la gomme, le tripatouillage ou le maquillage de données électroniques.

Dans l'affaire de la société « *Kajas* » jugée par la quatrième Chambre Correctionnelle du tribunal régional Hors classe de Dakar le 21 juin 2012[41], une jeune femme licenciée par la société « *Kajas* » a été déclarée coupable de détérioration frauduleuse de données informatiques au sens de l'article 431-13 du code pénal sénégalais issu de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité. La prévenue avait supprimé de son ordinateur portable de service des données relatives à la gestion de la société à une époque où le conseil d'administration devait se tenir.

Il faut préciser que la plupart des textes communautaires africains incrimine l'association de malfaiteurs informatiques. Il s'agit d'une association formée ou une entente établie en vue de la commission d'une ou de plusieurs infractions informatiques. Cette infraction vise surtout à appréhender les réseaux de cybercriminels, organisés en bandes (art. 15 de la Directive de la CEDEAO).

Quoi qu'il en soit, au Sénégal la politique de modernisation des incriminations pénales, a été complétée par un mouvement d'adaptation des infractions classiques aux TIC.

---

[40] En ce sens, V. « Le secret des correspondances est applicable aux messages électroniques », *D.* 2000, Inf. Rap. p. 286 ; X. BUFFET DELMAS et F.BITAN, « Le courrier électronique est protégé par le secret des correspondances », *Les échos*, 4 décembre 2000, p. 63

[41] T.R.H.C Dakar, 4e ch. n° 385 du 21 juin 2012, *affaire de la société Kajas, inédit.*

2. L'adaptation des incriminations classiques aux TIC.

L'analyse des textes pénaux africains a montré que lorsque les composantes immatérielles des TIC (systèmes, données, fichiers, logiciels etc.) sont l'objet de réalisation des actions malveillantes, selon des procédés connus de la législation, les juridictions étaient confrontées à l'inadaptation de la plupart des instruments de répression à leur disposition.

C'est certainement la raison pour laquelle, certains instruments juridiques africains ont ébauché un mouvement de dématérialisation des infractions contre les biens (a) et politique de modernisation de l'objet des atteintes au droit d'auteur (b)

a. La dématérialisation des infractions contre les biens

En effet, les législations pénales des Etats africains inspirées du code pénal français du colonisateur, sont surtout orientées vers la protection pénale de biens corporels, à l'exclusion des biens immatériels[42]. Pourtant, l'avènement de la société de l'information a fini par hisser l'information au statut de « *bien* » marchand ayant une valeur stratégique, très convoitée dans les rapports humains.Très vite, au-delà de la protection pénale spécifique dont bénéficie le bien informationnel[43], la protection pénale générale des informations numérisées (données d'entreprise, fichiers de clientèle, numéro de carte de crédit etc.) était devenu un enjeu stratégique de la lutte contre la cybercriminalité.

La Directive du 19 août 2011 portant sur la cybercriminalité a entrepris une politique de protection pénale de l'information, par la répression du vol, de l'escroquerie et du recel portant sur des données informatiques.

- **Le vol de données informatiques**

L'article 25 de la Directive de la CEDEAO se contente d'ériger en infraction le fait de commettre un vol portant les données informatiques[44].

En droit sénégalais, l'article 431-53 du Code pénal a consacré la théorie du vol d'information. Selon ce texte : « *la soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol* ». Désormais, il semble que les données électroniques contenues dans les serveurs peuvent être volées, à l'image des biens corporels classiques.

Le juge pénal sénégalais a eu l'occasion de faire application de l'article 431-53 du code pénal dans un jugement rendu par le tribunal régional de Thiès le 18 septembre 2012, à propos de l'affaire de l'Agence New Look Business. Dans cette espèce, P. Y., ingénieur informaticien,

---

[42] G. VERMELLE, « L'immatériel et la répression », in « *l'immatériel et le droit* », *Arch. phil dr*, tome 43, p. 213.

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

[44] V. art. III-41 de la Convention de l'UA.

chargé du service de la clientèle de l'Agence New Look Business, avait pendant son service, copié dans sa clé USB des données de l'agence relatives aux clients et aux actes de cession. Après avoir cessé ses fonctions à ladite agence, dans le courant du mois d'octobre 2011, il proposait à ses responsables, la remise de la clé USB moyennant le versement de la somme de 1.500.000 francs CFA. Il a été déclaré coupable de vol, par copiage des données.

Mais, cette décision est critiquable en ce que le vol suppose une soustraction frauduleuse, c'est-à-dire une dépossession du titulaire de la chose ; ce qui est difficilement admissible s'agissant des données électroniques copiées de leur support[45]. D'ailleurs, dans la nouvelle législation sénégalaise la possibilité d'un vol d'information consacrée suppose que soit établi un acte de soustraction par le juge, ce qui fait que le problème reste entier.

C'est certainement la raison pour laquelle, l'article 26 du Projet de loi-type CEMAC/CEEAC portant sur la cybercriminalité a contourné l'exigence de la soustraction, en incriminant sous la qualification de copiage frauduleux de données informatiques « *une personne qui copie ou tente de copier frauduleusement des données informatiques au préjudice d'un tiers* ».

- **L'escroquerie de données informatiques.**

L'article 25 de la Directive de la CEDEAO évoque également l'escroquerie portant sur des données informatiques. L'intégration de l'information dans l'assiette du délit d'escroquerie est particulièrement intéressante puisqu'elle permet d'assurer la répression de certains comportements frauduleux comme le phishing[46]., puisque le phisher est à la recherche d'informations confidentielles (mots de passe compte mail, numéro de carte bancaire, codes confidentiels etc.).

Il s'agit d'une technique d'«ingénierie sociale» consistant à exploiter, non pas une défaillance informatique, mais une «*faille humaine*» pour soutirer des informations personnelles à des internautes en leur envoyant un courrier électronique usurpant l'identité de banques, fournisseurs de services en ligne ou sites marchands[47].

L'arnaque débute par un mail envoyé par les fraudeurs au moyen d'une usurpation de l'identité d'une entreprise (banque, site marchand, etc.). Prétextant souvent d'une mise en place d'un nouveau système de sécurité ou d'une intervention technique sur le site. Les cyberescrocs invitent les clients à leur fournir des informations confidentielles[48]. Munis des identifiants et mots de passe ou des données personnelles ou bancaires des internautes

---

[45] En ce sens, S. DETRAZ, R. OLLARD, J-Ch. SAINT-PAUL, « Contre le vol d'information », in V. MALABAT, B. DE LAMY et M. GIACOPELLI (dir.), « *La réforme du code pénal et du code de procédure pénale. Opinio doctorum* », édition Dalloz, 2009, p. 107

[46] Ph. BELLOIR, « La répression pénale du phishing », *R.L.D.I* 2005/12, n° 349, p. 30 et s.; F. DUFLOT, « Phising : les dessous de la contrefaçon », *R.L.D.I* 2006/1, n° 366, p. 54.

47 B. AMAUDRIC du CHAFFAUT et Th. LIMOUZIN-LAMOTHE, « Une nouvelle forme de criminalité informatique à l'épreuve de la loi : le phising », *Expertises*, avril 2005, p. 140

[48] D. SANZ, « Un terrain nouveau d'action : la chasse aux données personnelles », in « *La délinquance électronique* », *Problèmes politiques et sociaux*, n° 953, octobre 2008, p. 47.

(numéro de client, numéro de compte en banque etc.), les fraudeurs pourront ainsi transférer directement l'argent sur un autre compte.

- **Le recel de données informatiques.**

Le recel de données électroniques est également érigé en infraction par l'article 25 de la Directive de la CEDEAO et par l'article 431-57 du Code pénal sénégalais[49]. Le législateur sénégalais évoque le recel d'information. Ainsi, cette nouvelle infraction peut bien avoir vocation à s'appliquer à l'hébergeur qui refuserait, en toute connaissance de cause, de retirer de son serveur des informations manifestement illicites (contenus pédopornographiques ou violents).

b. La modernisation de l'objet des atteintes au droit d'auteur.

En Afrique dans les textes relatifs au droit d'auteur, les législateurs visaient souvent parmi les œuvres protégeables au titre du droit d'auteur , dans des énumérations certes indicatives, les œuvres classiques de l'espace physique que sont les livres, les brochures, les conférences, les allocutions, les sculptures, les œuvres cinématographiques, les œuvres d'architecture, les œuvres photographiques le folklore[50]. Il en est ainsi par exemple de la loi n° 73-52 du 04 décembre 1973 relative à la protection du droit d'auteur.

Pourtant l'évolution technologique a vu naitre de nouvelles créations dites informatiques, à savoir les logiciels, les bases de données et les œuvres multimédia (site web, jeux vidéo etc.) qui sont de plus en plus l'objet d'atteintes de toutes sortes dans le cyberespace.

On constate dans la société de l'information, des copies serviles de logiciels, de extractions illicites de bases de données numériques, des reproductions illicites de sites web etc.

Devant l'incertitude de la répression pénale des atteintes dirigées contre les œuvres informatiques, l'OAPI a entrepris d'intégrer explicitement ces créations nouvelles dans le champ du droit d'auteur[51]. En effet, à la suite de l'arrêt Pacho rendu par la cour cassation française, le 7 mars 1986[52], les articles 5 et 6 de l'Annexe VII de l'Accord de Bangui du 02 mars 1977 instituant une Organisation Africaine de la Propriété Intellectuelle relatif à la propriété

---

[49] 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

[50] I .CAMARA, Le statut juridique de la contrefaçon des phonogrammes et œuvres littéraires et artistiques au Sénégal, *E.D.J.A*, Dakar, mars 1993, p. 10.

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

[52] Cass. Ass. Plén. 7 mars 1986, *affaire Pachot*, *D.* 1986, Jurisp. P. 405, note B. Edelman ; *JCP* G. 1986, II, 20631, note J.M. Mousseron, B. Teyssié et M. Vivant ; *RTD. Com* 1986, p. 399, Obs. A. Francon.

littéraire et artistique révisé le 24 février 1999, ont désormais inclus les logiciels et les bases de données dans la liste des œuvres de l'esprit[53].

La seule condition prévue pour la protection que ces créations informatiques est qu'elles présentent un caractère d'originalité. L'originalité est définie par l'article 7 de la loi du 25 janvier 2008 sur le droit d'auteur et les droits voisins comme la marque de la personnalité de l'auteur.

L'intégration des créations numériques dans les œuvres de l'esprit présente le mérite de permettre de sanctionner les atteintes dirigées contre ces œuvres sous la qualification de contrefaçon. Ainsi, dans l'affaire *Pressafrik* jugée par le tribunal régional Hors classe de Dakar le 19 janvier 2011[54], les juges ont considéré que le fait pour les sites kibar.net, galsentv.com, et seneweb.com de reproduire et de diffuser des informations du site pressafrik.com sans son autorisation et sans mentionner en liens hypertextes, la source de l'information, constitue une contrefaçon.

B. LES TIC : UN INSTRUMENT DE COMMISSION D'INFRACTIONS D'AFFAIRES.

De nos jours, l'espace numérisé qu'offrent les technologies de l'information et de la communication notamment l'Internet, est de plus en plus un puissant instrument permettant aux malfaiteurs de soutirer « *l'argent des autres* »[55]. Il s'agit d'une forme de cybercriminalité appelée « *cybercriminalité aspécifique* ».

Force est de constater que malgré la nouveauté du moyen technologique utilisé, le droit pénal commun a vocation à s'appliquer aux comportements cybercriminels facilités par les réseaux numériques (**1**). Cependant, les instruments juridiques africains de lutte contre la cybercriminalité ont envisagé de renforcer la répression pénale des cyberfraudes (**2**)

1. L'applicabilité du droit pénal commun.

Les données les plus récentes de la criminologie ont montré que la recherche du gain est de plus en plus présente dans l'action des délinquants informatiques[56]

Cependant, il serait excessif de considérer que le système pénal traditionnnel est mal adapté aux nouvelles pratiques frauduleuses des cybercriminels facilités par les TIC. En effet, en vertu du principe de la neutralité technologique, le juge peut, dans la plupart du temps, puiser dans l'arsenal pénal traditionnel des instruments de répression des agissements

---

[53] Au Sénégal l'intégration de ces créations informatiques dans la liste des œuvres de l'esprit a été réalisée par les art. 6 et 8 de la loi n° 2008-09 du 25 janvier 2008 sur les droits d'auteur et les droits voisins

[54] TRHC Dakar, 19 janvier 2011, *affaire Pressafrik, jugement inédit.*

[55] Sh. MORRIS, « L'ordinateur, instrument et facilitateur de criminalité », in « *La délinquance électronique* », *Problèmes politiques et sociaux*, n° 953, octobre 2008, p. 49.

[56] *Rapport de criminologie virtuelle McAfee*, disponible à l'adresse suivante http://www. 3d communication.fr/3dcomm/pdf/mcafeeetudecriminologievirtuelle.pdf

facilités par les réseaux électroniques. Les moyens technologiques employés ne perturbent pas sensiblement l'opération de qualification pénale.

A titre d'exemple, en Afrique, l'une des techniques frauduleuses les plus connues est le « scam » («*ruse*» en anglais) ou 419[57] . Cette arnaque est issue du Nigeria[58], ce qui lui a valu également l'appellation «*419*» en référence à l'article du Code pénal nigérian réprimant ce type de pratique[59]. Le « *scam* » consiste à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. Force est de constater que la plupart des techniques de fraude en ligne sont redevables des incriminations du droit pénal commun. Les tribunaux sénégalais ont à plusieurs reprises eu l'occasion de sanctionner l'escroquerie en ligne sur le terrain du droit commun de l'escroquerie[60].

Mais, face à la montée en puissance de l'escroquerie en ligne, certaines législations communautaires ont prévu d'ériger l'utilisation des TIC en circonstance aggravante de l'escroquerie. Il en est ainsi de l'article 30 du projet de loi-type CEMAC/CEEAC qui élève l'escroquerie commise via les systèmes et les réseaux informatiques au rang d'infraction aggravée.

La pratique frauduleuse du « *carding* » peut également relever des infractions classiques. Il s'agit du « *piratage de la carte bancaire par diverses techniques matérielles, logicielles ou subversives, aux fins d'obtenir et de revendre les données de cartes bancaires, de s'en servir pour effectuer des achats frauduleux, au préjudice du porteur légal* »[61]. Cette technique peut résulter d'un vol ou de la perte de la carte. A la suite de la copie des pistes magnétiques de la carte, les données récupérées sont recopiées sur de fausses cartes ou « *white plastics* » qui seront utilisées à des fins de fraude. Sur Internet, des sites ou des forums de discussion proposent des générateurs de numéros de cartes bancaires, des échanges d'informations sur le clonage de cartes bancaires et des méthodes de montage de puces[62]. Ces agissements sont pour la plupart du temps justiciables des délits de vol[63] ou d'escroquerie par usage de manœuvres frauduleuses[64].

---

[57] « Le Scam l'arnaque nigériane toujours en vigueur, Cyberpolice », disponible à l'adresse suivante : http://cyberpolice.over-blog.com/categorie-7445.html

[58] Ch. CORNEVIN, « L'arnaque à la nigériane », in « *la délinquance électronique* », *Problèmes politiques et sociaux*, n° 953, octobre 2008, p. 59 ; S. ROUJA, « De quelques faux clics et vrais escrocs », *R.L.D.I*, novembre 2008, p. 85 et s.

[59] Sur cette question, *Premier sommet de l'Afrique de l'ouest sur la cybercriminalité*, WACCS 2010, Abuja (Nigéria) 30 novembre- 2 decembre 2010: www.waccs.net

[60] T.R.H.C.Dakar, 15 mai 2007, inédit ; dans le même sens, T.R.H.C Dakar, n° 3927 du 05 septembre 2006, *affaire Agbola Ajibola et autres*, inédit.

[61] M. QUEMENER, « Cybercriminalité : la recherche de profit », in « *La criminalité numérique* », *Cah. Sécurité*, n° 6, octobre-décembre 2008, p. 143

[62] Sur cette question, M. QUEMENER et J. FERRY, *Cybercriminalité. Défi mondial*, 2e édition, *Economica*, 2009, p. 186.

[63] V. art. 364 du Code pénal sénégalais.

[64] V. art. 379 du Code pénal sénégalais.

Dans un jugement rendu par le tribunal régional Hors Classe de Dakar le 5 septembre 2006, à propos de l'affaire *Agbola Ajibola et autres*[65], la Division des Investigations Criminelles (DIC) a démantelé un réseau de cyberfraudeurs. A l'aide de divers matériels de confection de fausses cartes bancaires (références de cartes bancaires, procédés de fabrication de carte de crédit, disquettes d'ordinateurs etc.), ces derniers ont pu retirer de fortes sommes d'argent à partir de terminaux de paiement électronique de deux sociétés de location de véhicules.

2. Le renforcement de la répression des cyberfraudes.

Malgré l'applicabilité du droit pénal commun aux atteintes aux biens générées par la révolution informatique, les législations communautaires africaines ont entrepris de sécuriser la propriété privée dans le cyberespace.

D'abord, à l'image de la législation sénégalaise[66] et camerounaise[67], l'article 11 de la Directive de la CEDEAO a crée le délit de fraude informatique. Ce texte sanctionne le fait pour toute personne d'obtenir frauduleusement, pour soi-même ou pour autrui, un avantage matériel ou économique par l'introduction, l'altération, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système informatique.

Cette infraction sanctionne les manipulations informatiques réalisées en vue de porter atteinte aux biens d'autrui. Il s'agit d'une sorte d'escroquerie dirigée contre une machine. Dans l'affaire « *Fulgence BAHI* » [68], le tribunal régional Hors Classe de Dakar a jugé que le fait pour une personne d'utiliser une carte de paiement falsifiée, en accédant au terminal de paiement électronique d'une banque installé dans une bijouterie, en se faisant remettre des bijoux d'un montant de 07 millions de francs CFA, constitue une fraude informatique.

Ensuite, dans le cadre de l'UEMOA, les articles 15 et suivants de la loi uniforme du 3 septembre 2008 sanctionnent les infractions en matière de carte bancaire et autres instruments et procédés électroniques de paiement.

Il s'agit de la contrefaçon, la falsification d'une carte bancaire ou tout autre instrument électronique de paiement, l'usage ou la tentative d'usage d'une carte bancaire ou de tout autre instrument électronique de paiement contrefait, falsifié ou obtenu frauduleusement. Ce texte réprime également le fait d'accepter, de recevoir un paiement au moyen d'une carte bancaire ou de tout autre instrument électronique de paiement contrefait, falsifié ou obtenu frauduleusement[69].

---

[65] T.R.H.C.Dakar, n° 3927, 05 septembre 2006, *affaire Agbola Ajibola et autres, inédit.*

[66] V. art. 431-1 du Code pénal du Sénégal

67 V. art. 72 de la loi du 21 décembre 2010, relative à la cybersécurité et à la cybercriminalité au Cameroun.

[68] TRHC Dakar, 2e Ch. Corr., 21 janvier 2010, *Affaire Fulgence BAHI, jugement inédit.*

[69] J. P MARCHI, « Les fraudes en matière de crédit », *R.S.C*, 1979, p. 929 et s

Enfin, l'article 24 du Projet de loi-type CEMAC/ CEEAC envisage même la sanction de l'usurpation numérique, en incriminant une personne qui usurpe l'identité d'un tiers ou une ou plusieurs données permettant de l'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur à sa considération ou à ses intérêts[70]. Il s'agit souvent d'un puissant moyen de lutte contre la fraude sur les réseaux ; le cyberfraudeur peut utiler ainsi l'identité numérique d'un tiers (adresse mail, compte facebook, adresse IP etc.) en vue d'obtenir la remise de sommes d'argent par exemple.

II. LA MISE EN PLACE DE METHODES D'INVESTIGATION CONTRE LES CYBERINFRACTIONS D'AFFAIRES.

Malgré l'essor de la cybercriminalité, les modèles procéduraux en vigueur en Afrique ont été essentiellement conçus pour la conduite des investigations judiciaires en vue de la découverte d'objets matériels. Or, lorsque les cyberdélinquants utilisent les réseaux électroniques à des fins délictuelles, la nature dématérialisée de l'objet de l'activité infractionnelle (données informatique, système d'information, programmes), ne manque pas d'entrainer une dilatation des repères des techniques traditionnelles d'investigation judiciaire (perquisition, saisie, transport sur les lieux etc.)[71].

L'on assisté en Afrique à «*l'inadéquation des normes d'organisation du procès pénal* »[72]. Il en a résulté une certaine érosion des prérogatives des autorités judiciaires. Ainsi, les magistrats se sont retrouvés devant des difficultés pour transposer les solutions traditionnelles du système procédural aux nouveaux problèmes suscités par l'apparition des réseaux et devant l'impossibilité de recourir à de nouveaux mécanismes procéduraux en dehors des prévisions légales.

La Directive de la CEDEAO et le projet de loi-type CEMAC/ CEEAC ont institué de nouvelles méthodes d'investigation orientées vers la recherche de la preuve des cyberinfractions d'affaires (**A**) et vers la détermination des personnes responsables (**B**)

---

[70] F-J MATTHIOS, « La création d'un délit d'usurpation d'identité sur l'internet », *Gaz. Pal*, 26 juillet 2008, n° 208, p. 6 ; Th. VERBIEST, « La création d'un délit d'usurpation d'identité numérique » : www.droit-technologie.org

[71] V. Ch. MEUNIER, « La loi du 28 novembre 2000, relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. (belge) dr.pén.*, 2001, p. 657 ;Ch. FERAL-SCHUHL, « La collecte de la preuve numérique en matière pénale », in Dossier « *Cybercriminalité : morceaux choisis* », *Act.jur.pén.*, n° 3, mars 2009, p. 101

[72] 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. 207; Nd. DIOUF, « La procédure pénale à l'épreuve des nouvelles technologies de l'information », *Rev. Ass.sén.dr. pén* ., n° 5, 6, 7 et 8, 1997-1998, p. 14 ; P.A TOURE, « L'audit des normes applicables à la cybercriminalité », Communication, Séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal* ?», Dakar, 29 et 30 août 2005, p. 117 :

A. La recherche de la preuve des cyberinfractions d'affaires

Les droits communautaires africains ont eu tendance à élargir les pouvoirs d'investigation des juges, en esquissant une politique d'instrumentalisation des TIC à des fins probatoires (a). Cependant, cette irruption des techniques informatiques dans le processus de collecte de la preuve pénale n'est pas sans poser le débat de valeur des éléments de preuve électronique obtenus (b).

1. Le recours aux TIC à des fins probatoires

Pour restituer aux juges leurs pouvoirs répressifs, la Directive du 19 août 2011 a envisagé un aménagement des mécanismes probatoires classiques (a) et une institution de nouvelles techniques de recherche de preuve (b).

a. L'aménagement des mécanismes probatoires classiques

L'aménagement des dispositifs classiques de recherche de la preuve s'est traduit en législation par la consécration de la perquisition et de la saisie informatique

La perquisition informatique. L'article 30 de la Directive de la CEDEAO a étendu les prérogatives du juge en l'habilitant à opérer une perquisition dans un système informatique ou à une partie de celui-ci, lorsque des données stockées ce système sont utiles à la manifestation de la vérité.

Mais, si les données sont stockées dans un autre serveur situé en dehors du territoire national, l'article 677-36 Code de procédure pénale du Sénégal précise qu'elles sont recueillies par le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur (perquisition transfrontalière).

La saisie électronique. Lorsque le juge d'instruction découvre dans un système informatique des données qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, l'article 677-37 Code de procédure pénale permet au magistrat instructeur ou l'officier de police judicaire de saisir les données informatiques.

Techniquement, la saisie se fait par copiage sur des supports physiques de stockage informatique pouvant être saisis et placés sous scellés des données utiles pour la manifestation de la vérité, ainsi que celles qui sont nécessaires pour leur compréhension, dans hypothèse où les données saisies sont cryptées.

b. L'institution de nouvelles méthodes de recherche de preuve

Ces nouvelles procédures renvoient, en droit pénal communautaire de la CEDEAO, à la conservation rapide de données archivées et de l'interception de données relatives au contenu.

La conservation rapide de données archivées. Compte tenu de l'évanescence et de la volatilité des données informatiques qui sont souvent nécessaires à l'enquête, l'article 31 de la Directive de la CEDEAO permet à l'autorité judiciaire de 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. Cette mesure suppose qu'il y ait des raisons de penser que des données archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification. Il s'agit en réalité d'une mesure provisoire et conservatoire en attendant la réalisation d'une perquisition ou d'une saisie électronique.

L'interception de données de contenu. L'article 41 du Projet type CEMAC/CEEAC autorise les magistrats et les enquêteurs, 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. Ce mécanisme porte sur les données de contenu qui renseignent sur le contenu informatif d'un message. (données, vidéos, courriers électroniques, télécommunications etc.) Le juge peut également obliger un fournisseur de services, à collecter ou à enregistrer ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données. Le fournisseur d'accès est tenu de garder le secret.

La conservation des données de trafic. Une des particularités de la cybercriminalité est l'anonymat qu'elle assure aux cyberdélinquants qui se dissimilent derrière les réseaux. Ainsi, dans un contexte de développement des nouvelles techniques d'anonymisation sur les réseaux, l'identification des auteurs d'infractions en ligne est devenue l'une des questions les plus complexes du droit des TIC.

Le projet de loi type CEMAC, CEEAC a réglementé la technique de la collecte de données de trafic. Selon l'article 42 de ce projet de loi-type, le juge ou le procureur peut ordonner la collecte l'enregistrement en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Au Sénégal, l'article 4 de la loi sénégalaise du 25 janvier 2008 sur les transactions électroniques et l'article 35 de la loi camerounaise du 21 décembre 2010 ont mis à la charge des fournisseurs d'accès et d'hébergement une obligation de conservation de données de connexion[73].

[73] P. REYNAUD, « Le fournisseur d'accès et la conservation des données engendrées par les communications électroniques », *Comm. com. électr*, juin 2005, p. 19.

Les « *données de connexion* » ou « *données de trafic* »[74], par opposition aux « données de contenu », ne renseignent pas sur le contenu informatif d'un message. Ces « *mouchards électroniques* »[75] permettent l'identification de quiconque a contribué à la création d'un contenu illicite en ligne. Par exemple, l'adresse IP, la date et l'heure de connexion ou de déconnexion, les données administratives le nom, le prénom, l'adresse etc.[76].

Cette mesure de conservation des données d'identification des créateurs de contenus en ligne constitue un formidable mécanisme d'investigation pour les autorités judiciaires. Elle concerne surtout le magistrat instructeur chargé notamment d'identifier les personnes responsables des cyberinfractions. L'autorité judiciaire peut, conformément à l'alinéa 3 de l'article 4 de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, « requérir la *communication auprès des prestataires (fournisseurs d'accès et d'hébergement) les données ainsi conservées*».

Cependant, force est de constater que la mise en œuvre de ce dispositif est loin d'être effective dans les Etats africains.

2. La valeur des éléments de preuve électronique obtenus.

Le recours aux moyens électroniques dans le processus de collecte de la preuve pénale (perquisition, saisie électronique, interception de données etc.) pose en procédure pénale d'une part la question de la loyauté des preuves obtenues (a) et d'autre part le problème complexe de l'admissibilité de la preuve électronique en matière pénale (b).

a. La loyauté des éléments de preuve électronique obtenus.

En procédure pénale, si la preuve est en principe libre, son administration ne l'est pas.

Le principe de la loyauté de la preuve[77], qui « *impose à l'enquête un style* », a pour objet de prohiber l'utilisation de procédés déloyaux de ruses, d'artifices ou de stratagèmes par les autorités chargées de l'enquête et de l'instruction[78]. Le recours à ces méthodes de collation des preuves est sanctionné en jurisprudence par l'irrecevabilité des indices recueillis. C'est ce qui a été décidé par un arrêt de la Cour de cassation du 9 août 2006[79].

---

[74] G. MATHIAS et A.C LORRAIN, « Données de connexion : un état des lieux ou une première tentative de démêlage de la toile législative », *R.L.D.I*, décembre 2005, n°11, p. 48.

[75] J-F.MATTEI, « Traçabilité et responsabilité », in Ph. PEDROT (dir.), « *Traçabilité et responsabilité* », Economica, 2003, p. 35.

[76] V. art. 4 de la loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun.

[77] B. DE LAMY, « De la loyauté en procédure pénale brèves remarques sur l'application des règles de la chevalerie à la procédure pénale », in « *Le droit pénal à l'aube du troisième millénaire* », *Mélanges offerts à Jean PRADEL*, Cujas, 2006, p. 98 ; Ph. CONTE, « La loyauté de la preuve dans la jurisprudence de la chambre criminelle de la Cour de cassation : vers la solution de la quadrature du cercle ? », *Dr. pén.*, avril 2009, p. 13 et s.

[78] M. BLONDET, « Les ruses et les artifices de la police au cours de l'enquête préliminaire », *J.C.P* 1958, I, 1419 ; A. FAYE, « Le suspect dans les enquêtes de police », *Rev.Ass.sén.dr.pén.*, année 2010, n° 9, p. 19

[79] Cass.crim. 9 août 2006, *Procédures* 2006, comm. 278, obs. J. Buisson.

Dans cette espèce, un agent de la brigade des mineurs s'était connecté à un site de rencontres, en utilisant un pseudonyme et en se faisant passer pour un adolescent de quatorze ans. Par ce moyen, il était entré en contact avec une personne majeure, qui, sur sa demande, lui a adressé plusieurs photographies à caractère pornographique mettant en scène des mineurs. Par la suite, un rendez vous fut convenu avec ce dernier. Les enquêteurs se sont présentés au dit rendez vous avant d'interpeller le mis en cause. Il a été poursuivi de détention et de transmission d'images de mineurs à caractère pornographique en vue de leur diffusion. Par un arrêt du 11 mai 2006[80], la cour de cassation française a jugé que ce procédé porte atteinte au principe de la loyauté des preuves et au droit à un procès équitable, puisque qu'il constitue la provocation à la commission d'une infraction et la déloyauté d'un tel procédé rend irrecevable en justice les éléments de preuve obtenus par provocation[81].

b. L'admissibilité de la preuve électronique en matière pénale

Les enregistrements et traces informatiques (mail, données, images numérisées) peuvent-ils servir à prouver les infractions pénales ? Le numérique peut-il servir à forger la conviction du juge pénal ? C'est tout le débat de la recevabilité de la preuve électronique en matière pénale.

En vertu de l'article 414 du Code de procédure pénale sénégalais la preuve est libre en matière pénale. Les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.

Sous ce rapport, les données informatiques (images numérisées, SMS, courriers électroniques etc.) peuvent prouver la commission d'infractions, à la seule condition qu'elles soient discutées à l'audience. La Chambre sociale de la Cour de cassation française dans son arrêt du 23 mai 2007[82] s'est prononcée en faveur de la recevabilité des SMS comme éléments de preuve d'un harcèlement sexuel commis par un employeur envers son employée.

L'arrêt de la Cour d'Appel de Dakar du 17 avril 2009 rendu à propos de l'affaire du navire « Lobella », a admis la preuve d'un vol en réunion commis dans un navire au moyen d'un enregistrement par système de vidéosurveillance.

Cependant, pour sécuriser la preuve numérique, l'article 32 de la Directive de la CEDEAO dispose désormais « *l'écrit électronique est admis comme preuve en matière d'infraction à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et*

---

[80] Cass.crim. 11 mai 2006, *Bull. crim.* , n° 132 ; *D.* 2006, IR, 1772 ; *R.S.C* 2006, p. 848, note FINIELZ

[81] En ce sens, Ph. BELLOIR, « Déloyauté du stratagème et de la provocation policière dans la recherche d'une infraction sur Internet », *R.L.D.I*, décembre 2006, n° 22, p. 34.

[82] Cass.soc., 23 mai 2007, *Droit et procédure* 2007, n° 6, p. 339, obs. A. BOBANT ; *JCP* 2007, éd. G, II, 10140, note L. WEILLER.

conservé dans des conditions de nature à en garantir l'intégrité ». Cet encadrement juridique de la preuve électronique se justifie par le caractère manipulable et volatile du numérique.

B. La détermination des personnes responsables des cyberinfractions d'affaires

La multiplicité des intervenants techniques dans la chaîne de diffusion de l'information en ligne (fournisseurs d'accès, d'hébergement, de contenus, fournisseurs de liens hypertextes etc.) ne permet pas de situer sans difficultés les responsabilités pénales sur les réseaux. C'est pourquoi la Directive de la CEDEAO a envisagé un aménagement des mécanismes de responsabilité pénale. Cet instrument communautaire a consacré le principe de la responsabilité pénale des personnes morales en matière de cybercriminalité (**1**) et a allégé le régime de responsabilité des intermédiaires techniques (**2**)

1. La consécration de la responsabilité pénale des personnes morales

L'article 27 de la Directive du 19 août 2011 a consacré le principe de la responsabilité pénale des personnes morales pour les infractions prévues par ladite loi, commises pour leur compte par leurs organes ou représentants[83]. Il s'est surtout agit de prendre en compte la diversité des acteurs du cyberespace susceptibles de voir leur responsabilité engagée pour des actes répréhensibles. En effet, la plupart des intermédiaires techniques (fournisseurs d'accès et d'hébergement etc.) sont des personnes morales.

L'article 28 de la Directive énonce que la personne morale responsable sera « *passible de peines proportionnées et dissuasives, qui comprennent des amendes pénales et civiles* ».

En droit sénégalais, les peines encourues par les personnes morales vont de l'amende sont 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.

2. L'allégement de la responsabilité pénale des intermédiaires techniques.

Les instruments communautaires africains n'ont pas envisagé d'encadrer les conditions d'engagement de la responsabilité des fournisseurs d'accès et d'hébergement ; ce qui constitue une grande lacune de la stratégie de lutte contre les cyberfraudes.

Le fournisseur d'accès Internet assure en principe une fonction purement technique. Il assure à ses clients la connexion au réseau Internet. Par exemple la SONATEL Multimédia

[83] V. art. III-44 de la Convention sur la cybersécurité de l'UA.

au Sénégal. En droit sénégalais l'article 3 1) de la loi sénégalaise n° 2008-08 du 25 janvier 2008 sur les transactions électroniques définit les FAI comme « *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*».

Cependant, en vue d'éviter la délocalisation des serveurs des prestataires techniques, les standards juridiques internationaux, repris par certaines législations modernes comme celle du Sénégal, ont posé un principe d'irresponsabilité pénale du fournisseur d'accès, s'il se limite à son rôle technique de transporteur d'informations sur le réseau.

Quant aux hébergeurs, ils sont définis par l'article 3 2) de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques des « *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* ». L'hébergeur dispose en réalité d'un espace disque dur dans lequel il propose à ses clients, à titre onéreux souvent, d'héberger leurs sites web.

L'article 3 3) de la loi sénégalaise sur les transactions électroniques a prévu un système de responsabilité conditionnelle des hébergeurs. Ils ne peuvent être déclarés pénalement responsables des contenus illicites qu'ils hébergent que dans deux cas :

- s'ils avaient effectivement connaissance de l'activité ou de l'information illicite (des contenus illicites par exemple)
- si, dès le moment où ils en ont eu connaissance, ils n'ont pas agi promptement pour retirer ces informations ou en rendre l'accès impossible.

Mais, l'hébergeur ne peut voir sa responsabilité pénale engagée en raison des contenus hébergés que si ces contenus sont manifestement illicites (contenus de pornographie enfantine, contenus de fraude, racistes ou xénophobe etc.)

La doctrine et la jurisprudence estiment que l'hébergeur peut être poursuivi du chef de complicité par fourniture de moyens ou de recel d'information.

CONCLUSION

L'élaboration et la mise en œuvre dans les espaces communautaires africains d'une cyberstratégie de lutte contre la cybercriminalité d'affaires aura le mérite de favoriser la gestation d'un véritable droit pénal des TIC ou d'un cyberdroit pénal, régulateur d'une société africaine de l'information à dimension humaine inclusive ouverte, aussi bien dans ses aspects substantiels que processuels. Ce nouveau droit pénal des réseaux devrait prendre en charge dans ses prévisions l'immatérialité des comportements cybercriminels ainsi que l'anonymat des délinquants.

Mais, le phénomène cybercriminel est une criminalité internationale qui ignore les balises physiques de frontières étatiques. Il est donc nécessaire d'envisager en Afrique un renforcement de la coopération international la cybercriminalité. A cet égard, la convention africaine sur la cybersécurité constitue une avancée majeure dans la lutte régionale contre le phénomène. Mais, force est de constater que la Convention de l'UA n'est pas un instrument international de lutte contre le cybercrime, pour être limitée aux Etats africains.

En l'état actuel, en l'absence d'un traité international sur la cybercriminalité à l'échelle des Nations Unies, les Etats africains pourraient explorer la voie de l'adhésion à la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité. En effet, cette convention est ouverte à l'adhésion même des Etats non membres du Conseil de l'Europe.

Par ailleurs, de nos jours, on s'accorde pour admettre qu'un traitement efficient de la cybercriminalité suppose le recours à l'approche de « *cybersécurité* ». Cette nouvelle démarche procède d'une approche globale et holistique de la stratégie de lutte contre la cybercriminalité, intégrant toutes ses dimensions. Il s'agit au-delà de la modernisation des normes juridiques, de prendre conscience de la nécessité du renforcement des capacités et de spécialisation des autorités judiciaires en charge de la cyberdélinquance (vers une cyberpolice et une cybermagistrature), de l'amélioration des moyens matériels et logistiques à la disposition des organes répressifs et de la promotion de la culture de la cybersécurité.

Cette approche globale de la répression des agissements déviants du cyberespace, contribuera à inscrire les pays africains dans la croisade internationale contre la cybercriminalité, qui constitue une sérieuse menace pour la sécurité des réseaux et développement de la société de l'information.