La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'Ouest

Anmonka Jeanine-Armelle Tano-Bian

UNIVERSITE PARIS DESCARTES

FACULTE DE DROIT

ECOLE DOCTORALE SCIENCES JURIDIQUES, POLITIQUES,

ECONOMIQUES ET DE GESTION - ED 262

CENTRE MAURICE HAURIOU (CMH)

LA REPRESSION DE LA CYBERCRIMINALITE DANS LES ETATS DE L'UNION EUROPEENNE ET DE L'AFRIQUE DE L'OUEST

Thèse pour le Doctorat en Droit Public de l'Université de Paris Descartes

(*Arrêté Ministériel du 07 août 2006*)

Présentée et soutenue publiquement par :

Anmonka Jeanine-Armelle TANO-BIAN

Jeudi 28 mai 2015

JURY

Directeur de Thèse :

Mademoiselle **Annie GRUBER**, Professeur agrégé de Droit Public à l'Université Paris Descartes

Membres du Jury :

Madame Sylvie **CIABRINI-ROUSSEAU**, Maître de Conférences de Droit public - H. D. R à l'Université Paris Est Créteil **RAPPORTEUR**

Monsieur **Bertrand WARUSFEL**, Professeur agrégé des facultés de droit à l'Université de Lille 2 **RAPPORTEUR**

Monsieur **Daniel DORMOY**, Professeur agrégé à l'Université Paris Sud

Monsieur **Fereydoun KHAVAND**, Maître de conférences de Droit public – H. D. R. à l'Université Paris Descartes

AVERTISSEMENT

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à son auteur.

DEDICACE

A ma fille Kyra et à mon fils Joryel, qui ont été une source de motivation supplémentaire dans la réalisation de ce travail.

A mon époux SEKONGO Poganagnachien pour ces années d'isolement imposées et de soutien.

A mon papa adoré Aka Emmanuel, qui, en plus de son soutien parental, a mis à ma disposition son réseau professionnel avec ses collègues médecins notamment à l'Organisation Mondiale de la Santé (OMS), lesquels m'ont éclairé dans l'usage de la documentation relative à la *cybermédecine*.

A maman chérie Béatrice, qui a souvent été présente en s'occupant de mes enfants, me permettant ainsi de me libérer des obligations pour aller travailler en bibliothèque.

A mes frères Jean-Christian, Wilfried-André, Jean-François et Thierry-Jean qui m'ont tant manqué durant toutes ces années d'éloignement.

REMERCIEMENTS

Je remercie particulièrement ma directrice de thèse Mademoiselle Annie GRUBER, Professeur agrégé de Droit Public, qui a non seulement accepté d'assurer la direction de mes recherches, mais a toujours été très disponible pour me rencontrer, discuter de mon travail, et guider mes pas. Elle m'a permis d'accéder à divers documents difficilement accessibles et dont le contenu s'est révélé très approprié pour le traitement de mon sujet.

Ce travail n'aurait pas eu d'aboutissement sans l'aide de plusieurs personnes telles que mon tuteur de Reims et de mes amis pour leur soutien indéfectible. Je leur exprime ici ma reconnaissance.

Je remercie également les personnes rencontrées lors des divers colloques de formation et de découverte comme Monsieur AMAND Marc et son entreprise Ileads Consulting pour tous les travaux de soutien et de recherches réalisés ensemble avec une attention particulière, Maître KASSI Simplice pour ses diverses contributions notamment à ce travail de recherches, à des mises en relation avec des professeurs de l'Université d'Abidjan.

Mes remerciements s'adressent également à diverses personnes de multiples structures : il s'agit d'une part, pour la jurisprudence et la constitution des documents en annexes de Monsieur KOUASSI KOUADIO Jacques, Magistrat à Abidjan, du Docteur Mouhamadou LO, Directeur de la Commission Informatique et Libertés du Sénégal, pour sa contribution à l'enrichissement de ma jurisprudence surtout du Sénégal. D'autre part, du Commandant DJAHA et de son équipe de la Cellule Nationale de Traitement des Informations Financières (CENTIF) d'ABIDJAN, de Mlle KOUASSI Emmanuella du Computer Response Team de Côte-d'Ivoire (CI-CERT) ainsi que toute l'équipe.

Pour la France, je remercie Monsieur Didier GASSE de la Commission Nationale d'Informatique et des Libertés (CNIL), le personnel de la Brigade pour les Enquêtes Financières et contre les Technologies de l'Information (BEFTI), avec la collaboration active de Madame la Commissaire en Chef Anne SOUVIRA, et de Monsieur Julien OLINET.

Au niveau des structures européennes, il me faut témoigner de ma gratitude à Mme KWASNI du Conseil de l'Europe et à Mme AGHA de la même structure pour leur disponibilité et la mise à disposition des documents de travail du Conseil de l'Europe.

Quant à l'Organisation Mondiale de la Santé (OMS), à Genève et à Abidjan, mes remerciements s'adressent aux Docteurs DZENOWAGIS Joan, AL SHORBAJI, YACTAYO Sergio, STREIJFFERT- GARON Chantal et TANO-BIAN Aka pour leur participation active sur les questions relatives à la cyber-médecine et la cyber-santé.

Ces remerciements s'adressent également aux personnes d'Esri France qui m'ont épaulé et soutenu : Marie-Jeanne NANOU, Aurelien HEMERY, Jean-Michel CABON et toutes les personnes de cette entreprise pour leur assistance et leur aide.

Je remercie également madame YAO Philomène pour sa contribution dès le début de ce travail, EFFOUA épouse ZADI Bélinda et son époux ZADI Prudence, FATO Charles et son épouse SERY Bathe, pour leur soutien psychologique et moral au quotidien ainsi que tous ceux qui m'ont soutenu financièrement comme l'Etat de Côte-d'Ivoire par le biais du Service social dédié aux étudiants. Je remercie spécialement Monsieur Christian BENJAMIN qui m'a aidé et guidé pour les problèmes techniques.

Enfin mes amis juristes, et docteurs ERENON Dominique Désiré, OKOU Urbain, DURAND Lucille et SEVASTOPOULOU Zoi pour les lectures, et le soutien intellectuel, moral et amical.

A toutes les personnes qui m'ont soutenu de près ou de loin durant ces années de travail et de recherche pas toujours évidentes.

SOMMAIRE

CARTE DE L'UNION EUROPÉENNE

CARTE DE L'AFRIQUE DE L'OUEST

SIGLES ET ABREVIATIONS

ABS: Antiblockiersystem

ACP: Association des pays de l'Afrique des Caraïbes et du Pacifique

ACTA: Anti- Counterfeiting Trade Agreement

ADPIC : Accord sur les aspects des Droits de Propriété Intellectuelle qui touchent au Commerce

Aff. : Affaire

AFRI: Annuaire Français de Relations Internationales

AFRINIC: African Network Information Center

AIEA : Agence Internationale de l'Energie Atomique

AJ : Actualité Juridique

ALPA : Association contre la Piraterie Audiovisuelle

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ANSUT : Agence Nationale du Service Universel des Télécommunications

APE : Accord de Partenariat Economique

ARCEP : Autorité de Régulation des Communications Electroniques et des Postes

AREVA : Groupe français spécialisé dans les métiers de l'énergie, et dont le nom est inspiré de l'abbaye AREVALO en Espagne.

ARJEL : Autorité de Régulation des Jeux En Ligne

ARPA: Advanced Research Project Agency

ARPANET: Advanced Research Project Agency Network

ASIP : Agence des Systèmes d'Information partagés de Santé

ATCI : Agence de Télécommunications de Côte-d'Ivoire

ATRPT : Autorité Transitoire de Régulation des Postes et Télécommunications

B2A: Business to Administration

B2B: Business-to-Business

B2C: Business to Consumer

BBC: British Broadcasting Corporation

BEFTI : Brigade d'Enquêtes sur les Fraudes contre les Technologies de l'Information

BEI: Banque Européenne d'Investissements

C-SIS: Système Central du Système d'Informations Schengen

C2C: Consumer-to-Consumer

CAN-SPAM ACT: Controlling the assault of non-solicited pornography and marketing Act

CARI: Colloque Africain sur la Recherche en Informatique et Mathématiques Appliquées

Cass.: Cour de cassation en France

CEA : Commission Economique des Nations Unies pour l'Afrique

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

CERT : Computer Emergency Response Team

CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques

CIRT : Centre de Traitement des Infractions sur le Réseau et les Télécommunications Civ.: Chambre civile de la Cour de cassation en France

CLUSIF : Club de la sécurité des Systèmes d'Informations Français

CNAC : Comité National Anti- Contrefaçon

CNIL : Commission Nationale Informatique et Libertés

CNUCED : Conférence des Nations Unies sur le Commerce et le Développement

Com. : Chambre commerciale de la Cour de cassation en France

Crim. : Chambre criminelle de la Cour de cassation en France

DADVSI: Droit d'Auteurs et aux Droits Voisins dans la Société de l'Information

DDOS: Denial Distributed Of Service

DGCCRF : Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes

DHCP: Dynamics Host Configuration Protocol

DITT : Direction Informatique des Traces Technologiques

DNRED : Direction Nationale du Renseignement douanier et des Enquêtes Douanières

DOS: Denial of Service

ECHELON: nom de code de services de renseignements

EDVAC: Electronic Discrete Variable Automatic Computer

EEE: Espace Economique Européen

EFCC: Economic and Financial Crimes Commission

ENIAC: Electronical Numerical Integrator and Computer

ENISA: European Network and Information Security Agency

F CFA: Franc de la Communauté Financière Africaine

FAI: Fournisseur d'Accès Internet

FBI: Federal Bureau Investigation

FIRST: Forum for Incident Response and Security Teams

FNT: Fond National des Télécommunications

GIABA : Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent

HAAC : Haute Autorité de l'Audiovisuel et de la Communication

HADOPI: Haute Autorité pour la Diffusion des Œuvres et de la Protection des droits sur Internet

HTML: Hyper Text Markup Language

ICANN: Internet Corporation for Assigned Names and Numbers

IMPACT : International Multilateral Partnership Against Cyber Threats ou Partenariat Multilatéral International contre les Cyber-menaces.

IP: Internet Protocol

JAI : Justice et Affaires Intérieures

J-CAT : Joint Cybercrime Action Taskforce

JIRS : Juridiction Interrégionale Spécialisée

JOCE : Journal Officiel des Communautés Européennes

JORCI : Journal Officiel de la République de Côte-d'Ivoire

JORF : Journal Officiel de la République Français

JORS : Journal Officiel de la République du Sénégal

JOUE : Journal Officiel de l'Union Européenne

JPCERT: Japan Computer Emergency Response Team Coordination Center

LCEN : Loi pour la Confiance dans l'Economie Numérique

LOPPSI : Loi pour la Programmation et la Prévention de la Sécurité Intérieure

NCA: National Crime Agency

NCCU: National Cyber Crime Unit

NIST: National Institute of Standards and Technology

NSA : National Security Agency

N-SIS : Système informatique national du système d'information Schengen

NTIC : Nouvelles Technologies de l'Information et de la Communication

OCDE : Organisation pour la Coopération et le Développement Economique

OCLCTIC : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

ODR : Online Dispute Resolution

OIC-CERT : Organisation de la Coopération Islamique - Computer Emergency Response Teams

OMPI : Organisation Mondiale pour la Propriété Intellectuelle

PAP : Particulier A Particulier

PDA : Personal Digital Assistant

PICyAN : Plateau d'Investigations Cybercriminalité et Analyses Numériques

PLCC : Plateforme de Lutte Contre la Cybercriminalité

RTM : Robert Tappan Moris

SAFARI: Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus

SAT-3: South Atlantic 3.

SEC: Securities and Exchange Commission

SGSDN : Secrétariat Général de la Sécurité et de la Défense Nationale

SIM: Subscriber Identity Mobile

SIS: Système d'Informations Schengen

SQL: Structured Query Language

SIRENE: Supplementary Information Request at the National Entry

STCE : Série des Traités des Communautés Européennes

STE : Série des Traités Européens

StGB: Strafgesetzbung: Code pénal allemand

STIC: Système de Traitement des Infractions Constatées

SYSWEB : Système de Surveillance du Web

TFUE : Traité sur le Fonctionnement de l'Union Européenne

TIC: Technologies de l'Information et de la Communication

TLD: Top Level Domain

TUE: Traité de l'Union Européenne

UCLA: University of California Los Angeles

UCSB: University of California Santa Barbara

UE: Union Européenne

UEMOA: Union Monétaire Ouest-Africaine

UIT: Union Internationale de Télécommunications

UMP : Union pour un Mouvement Populaire

UNCTAD : United Nations Conference on Trade and Development

UNODC : United Nations Office on Drugs and Crime

UNECA : United Nations Economic Commission for Africa

VITIB : Village des Technologies et de la Biotechnologie

VPN : Virtual Private Network

WEP: Wireless Equivalent Privacy

WIFI: Wireless fidelity

INTRODUCTION

En droit, tout comportement humain ou toute action humaine qui cause du tort à autrui est répréhensible. Les actes humains pouvant tomber sous le coup de la **répression** sont assez variés. On distingue aujourd'hui la criminalité ordinaire d'une criminalité spécifique qu'on désigne sous le vocable de la **cybercriminalité**. Celle-ci s'entend d'un ensemble d'actes humains liés à l'usage des Technologies de l'Information et de la Communication (TIC). C'est ainsi que tout effort intellectuel pour appréhender le phénomène cybercriminel ne peut se détacher de trois démarches préalables.

Tout d'abord, il est nécessaire de procéder à une présentation succincte de l'évolution de la communication pour comprendre les bouleversements engendrés par l'informatique, nouvel outil de communication. (I).

Ensuite, ce nouvel outil très performant qu'est l'informatique suggère le meilleur et le pire dans ses usages. C'est dire d'une part, qu'il propose des aspects positifs par le biais des bons usages qui peuvent en être faits, et d'autre part, il présente des angles négatifs à travers les dérives qu'il occasionne. On apprécie dès lors l'outil informatique et ses déviances (II).

Enfin, au titre des déviances, il faut faire le point sur les mauvais côtés et surtout la nécessité de protection qui apparaît. C'est à ce stade qu'intervient la cybercriminalité. Elle s'érige en paroxysme du mauvais usage de l'informatique et des outils de communication traditionnelle (III).

I- LA COMMUNICATION ET SON EVOLUTION

Il y a lieu de rappeler fort utilement ici que la communication est au service de l'homme en ce qu'elle permet à celui-ci d'échanger avec son semblable, d'exprimer sa pensée, ses volontés, ses idées, ses convictions, etc. Cependant, comme tout outil utilisé par l'homme, la communication est de nos jours détournée à des fins criminelles.

Depuis ses origines, l'homme a toujours éprouvé le besoin de communiquer. Ce besoin se concrétise par l'usage de divers outils, lesquels ont considérablement et substantiellement évolué au fil des découvertes humaines (de la prise de conscience de

son environnement aux diverses mutations et changements de cet espace vital). C'est à cette conclusion qu'aboutit BERGSON dans son ouvrage *l'évolution créatrice*[1], lorsqu'il montre que chacune des modifications ou changements de l'homme est « une *espèce de création. Et de même que le talent du peintre se forme ou se déforme, en tout cas se modifie, sous l'influence même des œuvres qu'il produit, ainsi chacun de nos états, en même temps qu'il sort de nous, modifie notre personne, étant la forme nouvelle que nous venons de nous donner.* (…). Selon ce philosophe, « *notre cerveau, notre société et notre langage ne sont que les signes extérieurs et divers d'une seule et même supériorité interne. Ils disent, chacun à sa manière, le succès unique, exceptionnel, que la vie a remporté à un moment donné de son évolution* »[2]. Et c'est grâce à la prise de conscience des rapports et de la matérialité des choses que l'homme communique avec ses pairs. Il ressort de ces analyses, que l'Homme a recours à la communication pour extérioriser la conscience qu'il a de son environnement.

Et la communication répond à plusieurs définitions. Communication vient du verbe communiquer, qui selon le dictionnaire français Le Robert[3], est le fait d'établir une relation avec quelqu'un. C'est une relation dynamique qui intervient dans un fonctionnement, un échange de signes, de messages entre un émetteur et un récepteur. Le second sens donné est transitif. Il s'agit de communiquer quelque chose à quelqu'un. Une troisième explication considère la communication comme le moyen technique par lequel les personnes communiquent : il est alors question de transmission, on parle par exemple de communication téléphonique. Enfin, une quatrième définition de la communication renvoie à l'ensemble des techniques médiatiques d'information et de publicité.

Il découle de cette multiplicité de définitions de la communication que le mot désigne d'abord la relation entre deux personnes. Il s'agit du lien qui unit ces deux personnes. Ensuite, la communication est considérée comme l'action de ces deux

---

[1] **BERGSON Henri**, L'évolution créatrice, 80ème édition, Paris, PUF, 1957, Collection Bibliothèque de philosophie contemporaine, la version initiale date de 1907.

[2] **BERGSON Henri**, Idem, p. 157.

[3] Dictionnaire pratique de la langue Française, le Robert, éditions France Loisirs avec l'autorisation des Editions Le Robert, 2002, p. 317.

personnes, pour souligner dans un troisième sens le support auquel elles ont recours pour échanger. Echanger qui implique de mettre en relief l'objectif de l'action évoquée depuis le début : transmettre l'information. A la lecture des définitions précédentes, la communication semble impliquer la transmission de l'information. Dès lors, que recouvre le vocable de l'information ?

Tout d'abord, l'information est un nom commun féminin issu du latin *informatum,* et signifie selon le Dictionnaire Le Robert[4] , *un renseignement ou un événement qu'on porte à la connaissance d'une personne, d'un public.* Dans une seconde acception, l'information est définie comme ce qui peut être transmis par un signal ou une combinaison de signaux (message) selon un code commun et par un canal et ce qui est transmis est matérialisé comme étant l'objet de connaissance ou de mémoire. Autrement dit, un simple signal peut constituer une communication, un code en est un symbole. A titre d'illustration, les feux tricolores en matière de code de la route. De plus, l'idée de transmettre la connaissance par « le système de bouche-à-oreille », ou « téléphone arabe » est une autre manière de communiquer et c'est le moyen grâce auquel les personnes qui ont reçu cette information se cultivent et l'enregistrent[5].

Qu'il s'agisse de la définition du mot communication ou de celle de l'information, les deux notions semblent s'impliquer l'une et l'autre.

C'est en cela que Monsieur GUEDON, professeur canadien de littérature comparée, à Montréal et auteur de l'ouvrage intitulé « la planète cyber internet et cyberespace »,

---

[4]Dictionnaire pratique de la langue Française, le Robert, éditions France Loisirs avec l'autorisation des Editions Le Robert, 2002, p. 909.

[5] Selon le dictionnaire le REVERSO, le téléphone arabe est la *transmission très rapide d'une information par le bouche à oreille, l'information pouvant être altérée au final*, voir pour une version en ligne : http://dictionnaire.reverso.net/francais-definition/t%C3%A9l%C3%A9phone%20arabe. Selon le dictionnaire Le nouveau petit Robert, édition millésime 2010, p. 2520, le téléphone arabe est aussi le téléphone de brousse qui correspond à une transmission rapide des nouvelles par des relais de messagers ou d'informateurs.

La référence à la région arabe est liée au fait que les populations échangeaient entre elles uniquement d'une personne à l'autre, dans les pays nord -africains pendant la colonisation notamment. De la sorte, les informations étaient déformées du fait de la transcription inexacte des informations par la personne à laquelle elle a été communiquée. Cf. Le nouvel observateur - *Article du 3 juillet 2003.*

publié en 1996 aux éditions Gallimard en Italie, s'interroge sur le fait de savoir si l'information véhiculée suppose nécessairement la communication ou un échange[6].

Le dictionnaire français le Robert culturel, fait une excellente mise en relation des deux mots (ou concepts) lorsqu'il précise que « l'idée de communication correspond à des réalités plus anciennes que le sont les échanges nécessaires au fonctionnement et à la survie des systèmes complexes[7]. Les réalités les plus anciennes exigent un retour aux sources primitives de l'humanité c'est-à-dire à l'époque de la préhistoire.

La préhistoire est surtout étudiée au XIXe siècle (en 1859) lorsque les travaux de Jacques BOUCHER de PERTHES[8] sont reconnus par la communauté scientifique internationale. Cette très vaste période est subdivisée en plusieurs époques : il s'agit du paléolithique, du mésolithique[9] et du néolithique[10]. L'histoire de l'humanité est marquée dès la préhistoire par l'art[11], la culture notamment les peintures, les fresques rupestres. La première partie de l'ère préhistorique encore appelée l'ère de la pierre taillée a été datée grâce à la découverte dans les grottes[12], des représentations artistiques multiples et des premiers outils[13]. En effet, à l'analyse des fouilles archéologiques effectuées dans les

---

[6] Cf. **GUEDON Jean-Claude**, La planète cyber internet et le cyberespace, Gallimard, 1996, p12-13

[7] Dictionnaire culturel en langue française, le Robert édition 2005, p 1704 et 1705

[8] Cf. **Schleicher Ch. Jacques Boucher de Crèvecœur de Perthes**, 1788-1868. In: Bulletin de la Société préhistorique de France. 1932, tome 29, N. 5. pp. 230-233. **RICHARD NATHALIE**, L'institutionnalisation de la préhistoire. In: Communications, 54, 1992. pp. 189-207.

[9] Cf. **DERRUELLE Jean**, De la préhistoire à l'Atlantide des mégalithes : les leçons du Radiocarbone édition France-empire : P87 : on appelle mésolithique ou âge moyen de la pierre, une époque intermédiaire entre le paléolithique, âge ancien de la pierre taillée et le néolithique, âge récent de la pierre polie ; **AMIEL Olivier**, l'invention de la préhistoire, Anthologie, Textes choisis préfacés par Nathalie RICHARD collection Agora les Classiques, éditions PRESSES POCKET, 1992.

[10] Néolithique étant l'âge de la pierre polie, cf. note précédente.

[11] Cf. **MOHEN Jean - Pierre**, Arts et Préhistoire, Naissance mythique de l'humanité, FINEST SA : Editions Pierre Terrail, Paris 2002, 207p.

[12] Cf. **MOHEN Jean - Pierre**, Arts et Préhistoire, Naissance mythique de l'humanité, à la page 157, l'auteur décrit le thème de l'abstrait à l'aide de deux grands traits obliques s'emboîtant dans deux traits obliques plus petits. Cette manière de peindre est définie comme un usage au temps de la fréquentation de la grotte entre 15516 et 17190 ans avant notre ère.

[13] Multiples et mondiales dans la mesure où les fouilles concernent l'Afrique avec les rochers de Tanakom dans le désert de l'Aïr au Niger, de l'Europe avec les grottes à El Conde, La vina, Cueto de la Mina dans les Austries, en Amérique, dans la grotte de Panther Cave, à proximité de la rivière Pecos dans le Séminole

grottes de Lascaux, en Dordogne, en France[14], les hommes de la préhistoire expriment leurs angoisses, leur peur sur la pierre des grottes dans lesquelles ils vivent[15]. De ce fait, l'art est un moyen de représenter la vie quotidienne[16], les activités de chasse, les relations entre les animaux, l'organisation sociale, la conception de la femme[17]. D'ailleurs, le bâton de commandement du chef est l'un des signes marquants de l'art pariétal de même que le sorcier[18]. Cette manière de s'exprimer qu'est l'art, évolue de la représentation des images aux écritures. *« C'est à partir des traces du gibier que les premiers hommes devaient déduire les informations dont ils se servaient pour la chasse. Toutefois, les signes utilisés pour échanger ne suffisent plus. L'idée de fixer et de transmettre l'information est partie du besoin de dénombrer les troupeaux et d'évaluer les richesses : on passe de l'image au dessin-pictogramme*[19] *»*. Les outils de communication comme les dangers changent et l'écriture apparaît.

Trois mille cinq cents ans avant Jésus-Christ, apparaît le premier système graphique, c'est l'ancêtre de l'écriture cunéiforme. Deux centaines d'années plus tard, soit en 3300 de la même époque, les petites tablettes avec des tracés d'un pictogramme

---

Canyon au Texas (page 111 de art et préhistoire de Jean-Pierre MOHEN) et enfin l'Océanie avec les fouilles de 1960 faites dans le Vanuatu par J. GARANGER avec sur l'ile Efate la grotte ornée d'un personnage masculin (p118).

[14] Cf. **MOHEN Jean-Pierre**, Art et préhistoire, Naissance mythique de l'humanité FINEST SA : Editions Pierre Terrail, Paris 2002, 207p.

[15] Cf. **DAMS L.**, L'art paléolithique de la grotte de Nerja, Malaga, Espagne, collection BAR. International series, publié à Oxford, BAR, 1987

[16] Les représentations murales dans les cavernes au paléolithiques : grottes de El Conde, La vina, Cueto de la Mina dans les Austries, en Amérique, dans la grotte de Panther Cave, à proximité de la rivière Pecos dans le Séminole Canyon au Texas (page 111 de art et préhistoire de Jean-Pierre MOHEN) et enfin l'Océanie avec les fouilles de 1960

[17]Cf. **MOHEN Jean-Pierre**, Art et préhistoire, Naissance mythique de l'humanité, FINEST SA : Editions Pierre Terrail, Paris 2002, 207p.

[18] Cf. **BREUIL H.**, « *Un dessin de la grotte des Trois frères (Montesquieu-Avantès) Ariège* In: Comptes-rendus des séances de l'Académie des Inscriptions et Belles-Lettres, 74e année, N. 3, 1930. pp. 261-264 ; **LEROI-GOURHAN A.**, l'art pariétal : langage de la préhistoire, collection l'homme des origines, éditions Jérôme Million, Grenoble, 2009, P. 87 ;

[19]Cf. **MOGINET Stefan François**, Du Calame à l'ordinateur, l'évolution graphique de l'écriture arabe, Publié à Méolans-Revel, Atelier Perrousseaux, DL 2009, Italie, p7-11.

sont retrouvées sur le site d'Uruk. Ces tracés sont ceux des Sumériens[20], les intendants des temples de la ville d'Uruk[21], en Mésopotamie[22]. C'est pourquoi l'invention de l'écriture leur est attribuée. Cette première forme d'écriture est dite cunéiforme et évolue au contact des Akkadiens[23], qui lui apportent l'alphabet.

L'alphabet est en réalité une transformation de l'écriture cunéiforme. C'est en 3200 avant Jésus-Christ[24] qu'apparaissent les hiéroglyphes. Cette forme d'écriture avec des signes [25] se trouve sur les pyramides et à l'intérieur des tombeaux des pharaons[26], rois d'Egypte. C'est pourquoi, elle est considérée comme l'une des premières formes de l'écriture que nous utilisons aujourd'hui. L'écriture, par ses utilisations, est à l'origine de mutations importantes[27]. A titre illustratif, les saintes écritures de la Bible retracent le moment d'écriture important dans l'histoire. Ce sont les tables de lois données à Moïse au

---

[20]Cf. **SENECAL Didier**, Chronologie de l'histoire du monde, édition Le grand livre du Mois, 2001, p. 17 ; Paul TOSCANNE, les signes sumériens dérivés (les Gunû), préface de M. J. Oppert, Paris : E. Leroux, 1905.

[21] Cf. **Jean BOTTERO**, Mésopotamie : l'écriture, la raison et les dieux, Paris, collection Folio. Histoire éditions Gallimard, 1997.

[22] C'est une écriture en forme de clou ou en coin d'où son appellation d'écriture cunéiforme : ce sont les Sumériens qui l'ont inventé, cf. **GLASSNER Jean-Jacques,** Écrire à Sumer : l'invention du cunéiforme, Paris, Éd. du Seuil, collection L'univers historique, 2000.

[23] Naissance de l'écriture : cunéiformes et hiéroglyphes : Galeries nationales du Grand Palais, 7 mai-9 août 1982, Paris, Éditions de la Réunion des musées nationaux, 1982 ; http://classes.bnf.fr/dossiecr/in-cunei.htm

[24] Cf. **ALPHANDARI Y**., A la découverte des hiéroglyphes, Collection : Castor doc : civilisations : junior, éditions Flammarion, Paris, 1999, p. 15 : « les hiéroglyphes naissent en Egypte vers 3200 avant J-C, soit un siècle après la première écriture de l'Histoire, apparue en Sumer en Basse- Mésopotamie.

[25]Cf. **ALPHANDARI Y**, A la découverte des hiéroglyphes, **Collection :** Castor doc : civilisations : junior, éditions Flammarion, Paris, 1999, p. 17 à 21 : « : les Egyptiens désignent l'écriture par l'expression « les paroles du dieu ». Ce sont les grecs qui beaucoup plus tard, nommeront hiéroglyphes, dérivé du grec *hierogluphica*, « caractères gravés sacrés » ; les Egyptiens disent *médounetcher*. Dans les hiéroglyphes, *il existe 3 catégories d'hiéroglyphes : les idéogrammes qui représente un mot au moyen d'un signe unique ; les phonogrammes : qui exprime un ou plusieurs sons et les déterminatifs : qui sont des signes qui ne se prononce pas, qui ne se traduisent pas ; ils servent uniquement à préciser le sens d'un mot.*

[26] **SERJEVAN F**., Le tombeau de Nakhtamon à Deir-al-Madina : paléographie, Le Caire, Institut français d'archéologie orientale, Paris, AFPU, 2011, imprimé en Egypte

[27] Les échanges et les manières de communiquer changent avec l'invention de l'écriture: les hommes arrivent à mieux comptabiliser et matérialiser leurs échanges commerciaux. Les tablettes retrouvées et commentées par l'école des Hautes Etudes en sont la preuve : **SCHEIL Jean-Vincent**. Catalogue sommaire de la collection des tablettes cunéiformes de l'École Pratique des Hautes Études. In: Ecole pratique des hautes études, Section des sciences historiques et philologiques. Annuaire 1932-1933. pp. 3-27.

Mont Sinaï dans le livre de l'Exode[28]. En effet, il n'y a pas d'écriture avant la rencontre entre Dieu et le prophète Moïse au mont Sinaï. Il faut interpréter à travers ces faits, la nécessité de transmettre des écritures (témoignages) aux générations futures. Tandis que les paroles s'en vont, les écritures restent. D'où la place importante de l'écriture dans la communication. Les changements multiples introduits par l'écriture conduisent les êtres humains, à améliorer leur manière d'échanger des informations[29]. Ainsi, le recours aux messagers porteurs de courriers évolue.

La transmission du courrier se fait d'abord de main en main, à l'image d'Hermès[30] dans la Rome antique. Ensuite, au cours de la Renaissance, ce sont les messagers royaux, appelés les Veredarii[31], qui acheminent les courriers[32]. C'est Cyrus, roi de Perse qui invente le système des postes à relais[33]. Cette technique est, selon plusieurs historiens, importée de la pratique chinoise[34]. Les difficultés rencontrées lors de ces échanges[35]

---

[28] Livre de l'Exode chapitre 19 et suivants de la Bible TOB : les dix commandements

[29] Histoire de la poste : sur le site de la poste : http://www.laposte.fr/legroupe/Nous-connaitre/Histoire/Histoire-de-La-Poste/Histoire-de-La-Poste2.

[30]Cf. **GONZALES Antonio**. Has epistulas Hermès tulit. Lettres et porteurs de lettres dans la Correspondance de Pline le Jeune. cf.: Dialogues d'histoire ancienne. Vol. 24 N°2, 1998. pp. 73-87.

[31]Cf. **AUDOLLENT Aug**., Les Veredarii émissaires impériaux sous le Bas-Empire. In: Mélanges d'archéologie et d'histoire T. 9, 1889. pp. 249-278.

[32]Cf. **TACK- SCHERPENBERGHS** Murielle, Le courrier d'Érasme. In: Revue belge de philologie et d'histoire. Tome 68 fasc. 2, 1990. Histoire - Geschiedenis. pp. 291-304.

[33]Cf. **BERTIN François**, La poste du messager à cheval au courrier électronique, éditions Ouest-France, collection du musée de Paris, 1999.

[34] Idem, p. 10 et 11 : la transmission des premiers courriers se fait à pied. L'invention de la poste peut être attribuée aux chinois dès le XIIIème siècle avant notre ère. L'homme restera pendant longtemps le vecteur puis au Ive siècle avant JC, le cheval va peu à peu le supplanter. C'est à cette époque que le roi de Perse, Cyrus crée le premier réseau de relais permettant aux cavaliers d'échanger sans perdre de temps leurs chevaux fatigués contre des montures fraîches ; voir également Les postes à relais de chevaux chinoises, mongoles et mameloukes au XIIIe siècle : un cas de diffusion institutionnelle. In: La Circulation des nouvelles au Moyen Âge. XXIVe Congrès de la S.H.M.E.S. (Avignon, juin 1993). Rome: École Française de Rome, 1994. pp. 243-250. (Publications de l'École Française de Rome, 190).

[35] Le transport des courriers à dos de cheval impliquent de remplacer les chevaux souvent fatigués et ces remplacements ne facilitent pas une transmission efficace d'un point à un autre, cf. François Bertin, La poste du messager à cheval au courrier électronique, éditions Ouest-France, collection du musée de Paris, 1999.

conduisent à adopter de nouveaux processus comme le transport du courrier par les facteurs urbains en 1760[36].

Parallèlement à l'évolution en Europe, le continent africain adopte des modes de communication différents. L'Afrique accorde une place particulière à la gestuelle[37]. Au Vème et VIème siècle de notre ère, dans les royaumes notamment des dynasties, des empires dont les plus marquants restent l'empire du Mali[38] avec la légende *Soundiata Kéïta*, ou encore le royaume des Ashanti *« Ashante »* au Ghana, c'est l'oralité qui préside[39]. Toutes les informations, l'annonce de l'arrivée d'un étranger dans la région, la manière de l'accueillir ou de vanter ses mérites ou exploits et même son départ, tout est spécifique et obéit à un processus et un rituel particuliers. A titre illustratif, les griots dans la culture malinké surtout présents dans le nord de l'Afrique subsaharienne, principalement avec l'empire Songhay[40] et du Mali assument cette fonction de communication. Ces griots sont à la fois des orateurs poètes et chantres aux timbres vocaux reconnus et marqués par une dimension sacrée. Ils ont une mission particulière. Grâce à leur art, ils savent amadouer et vanter les mérites, ils transmettent à leur auditoire les émotions (tristes ou joyeuses). Ils utilisent la parole et souvent la musique[41] pour toucher et sensibiliser ceux qui les écoutent. La parole est sacrée[42]. Les peuples communiquent à l'aide d'instruments de musique comme les tam-tams[43], les

---

[36] http://www.laposte.fr/legroupe/LeGroupe2/Nous-connaitre/Histoire/Les-grandes-dates-cles/Chronologie-de-1708-a-1796 : création du Facteur de ville en France.

[37] Cf. **BADUEL- MATHON Céline**, le langage gestuel en Afrique occidentale : Recherches bibliographiques. In: Journal de la Société des Africanistes. 1971, tome 41 fascicule 2. pp. 203-249.

[38] Ces empires sont situés pour la plupart dans le Golfe de Guinée : cf. **Pierre KIPRÉ** « Sur la périodisation de l'histoire de l'Afrique de l'Ouest : le Golfe de Guinée », *Afrique & histoire* 1/2004 (vol. 2), p. 85-96.

[39] Cf. **CALAME-GRIAULE Geneviève**, 1987, *Ethnologie et langage. La parole chez les Dogon*, Paris, Institut d'Ethnologie (1ère éd. 1965).

[40] Cf. **CISSOKO Mody Sékéné**, Tombouctou et l'empire Songhay, édition L'Harmattan, 1996.

[41]Cf. Sory Camara, Gens de la parole : essai sur la condition et le rôle des griots dans la société malinké, Ed. Karthala, 1992, Paris.

[42] Cf. **PERSON Yves**, Tradition orale et chronologie in *Cahiers d'Études Africaines*, Vol. 2, Cahier 7 (1962), pp. 462-476, EHESS.

[43] Cf. **GASTON W.**, *Atumpan*i : le tam-tam parlant : anthropologie de la communication, Paris, Budapest, éditions L'Harmattan, 2004

xylophones[44]. La danse est également un autre moyen d'expression[45] et elle est surtout une forme de communication ; c'est à travers les expressions du corps que les signes, les images sont décrits et interprétés pour véhiculer le message souvent codé. La mort d'un roi, la fête des ignames[46], les fêtes de générations, les changements de saison des cultures obéissent à un rituel spécial quant à la divulgation de l'information et les échanges. Les échanges commerciaux ainsi que les conquêtes entre peuples de cette partie de l'Afrique marquent le Xème siècle et les suivants. C'est par exemple le cas avec la dynastie des Ashanti (écrit *Asante*) au royaume du Ghana plus, dans le sud de cette région[47]. Ce n'est qu'au XXème siècle que certains auteurs de littérature comme Amadou Hampaté Ba, au Sénégal, décident de transmettre par écrit, ce qui jusqu'alors, est enseigné et appris oralement[48]. D'ailleurs, lors de la conquête coloniale de l'Afrique, les explorateurs découvrent des peuples qui échangent par la danse, les signes, la parole. Rien n'est écrit[49]. Tout comme l'Europe, l'Afrique passe de la parole à l'écriture.

Mais les évolutions de la communication ne se limitent pas à ces vagues de bouleversements des habitudes. En ce sens, des découvertes plus révolutionnaires voient le jour. C'est la volonté de parfaire les relations et d'améliorer les échanges qui prend le dessus.

Dès 1793, Chappe et ses frères inventent le télégraphe. Cet outil permet de diminuer les

---

[44] Cf. **BIYELE Franck François**, Nouvelles approches des problématiques de communication sur l'Afrique subsaharienne: représentations, idéologie et instrumentalisation, préface de Michael Palmer, édition l'Harmattan, Paris, 2007

[45] cf. **BADUEL – MATHON Céline**, Le langage gestuel en Afrique occidentale : Recherches bibliographiques. In: *Journal de la Société des Africanistes*. 1971, tome 41 fascicule 2. pp. 203-249

[46] Cf. **PERROT Claude Hélène**, « Du visible à l'invisible : les supports du pouvoir en pays akan (Afrique de l'Ouest) », *Bulletin du Centre de recherche du château de Versailles ;* cf. **JANSEN Jan**, *Epopée, histoire, société. Le cas de Soundjata, Mali et Guinée*, 2001, Paris, éditions Karthala

[47] Cf. **PESCHEUX Gérard**, le royaume Asante, Ghana : parenté, pouvoir, histoire du XVIIème au XXème s, éditions Karthala, France, 2003.

[48] Voir à pour cela, **ASSI Diané**, *AMADOU HAMPATE BA, Ecrivain du XXe siècle ou l'Etrange Destin de la Tradition Africaine*, Thèse de Doctorat, sous la direction de Mr le Professeur Jacques BRENGUES, publié en France, Rennes, en 2008.

[49] Voir à ce titre, Le langage des tam-tams et des masques en Afrique : une littérature méconnue, Maître Titinga Frédéric Pacéré, Paris édition l'Harmattan, 1991 ; Tradition orale et nouveaux médias, Xe FESPACO, Bruxelles : FESPACO : OCIC, 1989.

délais de communication[50]. Il s'appuie sur l'utilisation de signaux électriques se propageant sur un fil électrique.[51] Il est remplacé en 1837 par le télégraphe électrique de Morse. La raison officielle est le nombre peu important de messages que le télégraphe de Chappe permet de transférer.

La centralisation du réseau commence avec le télégraphe électrique Morse qui, selon les autorités administratives, présente plus d'avantages. Il aurait des capacités supérieures et plus avantageuses et cela dure tout au long du dix-neuvième siècle. Par la suite, le télégraphe même morse ne suffit plus, il montre ses imperfections en ce qu'il exige de combiner des données binaires[52]. Mais une autre raison inavouée existe en France : l'Etat a monopolisé le télégraphe de Chappe grâce à une loi de 1837 et l'a confié aux militaires[53]. Louis Philippe, Roi des Français propose une loi pour monopoliser les lignes télégraphiques : c'est la loi du 2 mai 1837 sur le monopole de l'Etat des lignes télégraphiques, comportant un article unique signé par Louis Philippe et adoptée par les Chambres[54]. Pour des raisons de sécurisation, l'Etat français évite de mettre à la portée du public cet outil de communication pouvant être utilisé à d'autres fins que la diffusion des informations. Il en est ainsi des raisons militaires ou même le fait que les populations civiles pourraient utiliser ce moyen de communication comme moyen de pression sur les institutions étatiques.

Un parallèle est ainsi fait à la limitation dans les usages des médias et des réseaux de communication. Il faut mentionner que ces attitudes étatiques renferment les prémisses des sanctions entreprises en cas de fraude à ces lois limitatives.

---

[50] Cf. **BROCHANT Christian**, Histoire générale de la radio et de la télévision en France, Paris : la Documentation française, 1994.

[51] Cf. **FDIDA S.,** Des autoroutes de l'information au cyberespace, édition Flammarion, 1997, imprimé en France, Collection DOMINOS dirigée par Michel SERRES et NAYLA FAROUKI, 126 pages.

[52] Cf. **GUILLAUME Marc**, L'empire des réseaux, éditions DESCARTES & Cie, 1999, Paris, p.46

[53] Idem, page 10 du livre.

[54] Loi du 2 mai 1837 sur le monopole de l'Etat des lignes télégraphiques, article unique, signé par Louis Philippe, cf. : **BROCHANT Christian**, Histoire générale de la radio et de la télévision en France, « Comité d'histoire de la radiodiffusion » Tome I, 1921-1944. - Bibliogr. vol. 1, p. 54-56.

1876 est une année marquante dans l'évolution des moyens de communication : c'est l'ère du téléphone inventé par Graham Bell. La communication est verbale et le codage change. Dans ce système il n'est plus question de signaux analogiques mais il s'agit de fréquence[55].

A la fin du dix-neuvième siècle, naît le premier média : la radio qui se révèlera être une arme redoutable au vingtième siècle avec la propagande nazie. La radio va servir pour véhiculer les idées nazies en touchant plusieurs niveaux de populations dans le même temps. Elle sera dénoncée par Radio Londres, la radio de la résistance et la ritournelle « RADIO PARIS MENT, RADIO PARIS MENT, RADIO PARIS EST ALLEMAND » de même que l'ensemble des messages radiophoniques du même type[56] témoignent[57] d'une instrumentalisation politique d'un outil de communication. Mais il faut reconnaître que la radio présente également des avantages multiples et c'est grâce à ce média qu'a été possible l'appel du 18 juin 1940 du Général De Gaulle, retransmis par la BBC[58]la diffusion du discours du général De Gaulle. De ce point de vue, elle revêt un aspect positif au cours de cette période particulièrement douloureuse et catastrophique en Europe[59].

Aux technologies de diffusion de l'écriture et du son, vient s'ajouter la télévision qui elle, permet la diffusion des images. Selon l'encyclopédie LAROUSSE[60], le mot télévision évoque *d'abord la diffusion d'émissions par ondes hertziennes ou leur distribution par câble. Or, cette technique permet aussi soit de visualiser instantanément*

---

[55] Cf. **FDIDA S.**, des autoroutes de l'information au cyberespace, édition Flammarion, 1997, imprimé en France, Collection DOMINOS dirigée par **SERRES Michel** et **FAROUKI Nayla**, 126 pages.

[56] Cf. Dr **FRIEDRICH**, un journaliste allemand vous parle 1er recueil, Causeries faites au micro de Radio Paris, du 20 avril au 1er Juin 1941, Paris éditions Le Pont, 1941, 24p.

[57] Fréquence radio : British Broadcasting C et des pratiques comme la distribution de tracts : cf. : Propagande en faveur de l'Allemagne nazie. Tracts, 1940- 1944, 92 pièces ; **GRUAT Cédric**, Hitler à Paris : juin 1940, Paris, Ed. Tirésias, DL 2010, collection Lieu et mémoire

[58] Cf. **Charles de GAULLE**, Paroles d'un chef, Extraits des discours prononcés à la radio du 18 juin au 1er août 1940 par le Général de Gaulle ; Discours, messages et déclarations du Général de Gaulle, du 18 juin 1940 au 8 octobre 1941 publié chez Le Caire : Revue des conférences françaises en Orient, 1941.

[59] Difficile période du fait de la guerre entre les Etats en Europe et des déchirements psychologiques qui ont pu s'en suivre.

[60] http://www.larousse.fr/encyclopedie/nom-commun-nom/t%C3%A9l%C3%A9vision/96390

une image sur un écran, soit de la transmettre à distance, soit encore de l'enregistrer sur une bande magnétique.

Les essais de la télévision remontent aux années 20. En effet, c'est le 29 décembre 1923 que Vladimir Kosma Zworykin dépose le brevet d'un tube analyseur d'image, l'iconoscope[61].
Les premiers essais de laboratoire de transmission d'un visage par télévision commencent en 1924.

Tous ces outils de communication (télégraphe, radio, téléphone, télévision) se limitent à la transmission d'informations. Un autre cap reste à franchir pour arriver à concevoir le cyberespace : c'est le traitement d'informations. Et l'ordinateur répond parfaitement à cette fonction.

II- L'OUTIL INFORMATIQUE : POUR LE MEILLEUR ET POUR LE PIRE

Le premier à poser le principe de traitement des données est John Von Neumann dont les conceptions utilisées à des fins stratégiques répondent exactement aux attentes de l'armée américaine[62]. Le premier ordinateur apparaît en 1940 aux Etats-Unis. La particularité de cette découverte est l'absence de clarté sur la complexité de son système. Dans le même temps, plusieurs autres projets sont initiés dans le domaine scientifique et ce, en vue d'élaborer des programmations de calcul et des applications d'ingénierie. En 1944, tous les meilleurs ingénieurs de l'Ecole de l'Université de Pennsylvanie travaillent sur le grand projet de calculateur électronique connu sous le sigle ENIAC (Electronical Numerical Integrator And Computer). Il est financé par l'Army Ordnance qui attend

[61] Cf. **ZWORYKIN Vladimir K**. décrit le mécanisme de fonctionnement de la télévision dans le document officiel « Televison system » publié sous le numéro *2, 107,464*, United States Patent Office, février 1938.

[62] Cf. **ROJAS Raùl and HASHAGEN Ulf**, The first computers, History of computing, Editions Cambridge (Mass) MIT press, 2000.

l'ordinateur le plus performant pour le Laboratoire de Recherches Balistiques (Ballistics Research Laboratory) [63]. Des recherches sont menées par Eckert et Mauchly pour améliorer l'ordinateur, jugé énergivore. Les deux scientifiques s'associent pour élaborer une technologie de pointe entre 1946 et 1957[64]. Ils parviennent à créer l'ordinateur capable de stocker des programmes et l'appellent : Electronic Discrete Variable Automatic Computer (EDVAC)[65].

Dans cette dynamique scientifique de performance, dès 1957, le ministère de la Défense crée l'agence de projets de recherches avancées, en anglais Advanced Research Project Agency (ARPA) dont l'objectif est de renforcer les développements scientifiques à visées militaires. Il *s'agit clairement de faciliter l'accès à distance des chercheurs aux rares gros ordinateurs et l'expérimentation de la technologie des paquets*[66]. On est encore au stade de la recherche et c'est beaucoup plus tard que la commutation des paquets connaît un essor remarquable. Par cette technologie, les *données sont divisées en petits paquets ou datagrammes, qui peuvent prendre différents itinéraires pour atteindre leur destination*[67]. Le message véhiculé peut donc être divisé en plusieurs morceaux et parvenir à plusieurs destinataires. Ce système de commutation permet aux données informatiques de s'inter-échanger. La technique existe en Angleterre depuis 1968[68]. Derrière cette motivation américaine, se cache la compétition technique avec son rival

---

[63]Cf. **W. ASPRAY**, JOHN VON NEUMANN and the Origins of Modern Computing, Edition 1990, Massachusetts Institute Technology, P. 34 et s.

[64]Cf. **NORBERG A. L.**, Computer and Commerce: a study of technology and Management at Eckert-Mauchly Computer Company, Engineering Research Associates and Remington Rand, 1946-1957, Editions MIT Press.

[65] Cf. **ANIS Jacques**, Texte et ordinateur : l'écriture réinventée, collection : Méthodes en sciences humaines, publication : Paris ; Bruxelles: De Boeck université, 1998.

[66] Cf. **ANIS Jacques**, Texte et ordinateur : l'écriture réinventée, collection : Méthodes en sciences humaines, publication : Paris ; Bruxelles : De Boeck université, 1998 p. 181 ; Lire également Defense Advanced research Project agency (Etats-Unis)**,** DARPA neural network study, October 1987-February 1988, AFCEA international press, 1992 ;
Alex Roland et Philip Schiman, Strategic Computing : Darpa and the quest of machine, 1983-1993, collection History of computing, Cambridge, Mass : MIT Press, 2002.

[67] Cf. **ANIS Jacques**, Texte et ordinateur : l'écriture réinventée ?, op.cit. p. 180

[68] Cf. **ANIS Jacques**, Texte et ordinateur : l'écriture réinventée ?, op.cit. p. 181

légendaire l'URSS[69]. De sorte que, poussés par leur ferme conviction de devancer l'URSS sur le plan des télécommunications, les Etats- Unis d'Amérique ont recours aux chercheurs universitaires. Ces derniers doivent proposer à l'armée un moyen de mettre en place un réseau de communication militaire capable de résister aux attaques nucléaires[70].

Il s'ensuit que, de la construction d'un réseau sécurisé pour l'armée, les universitaires parviennent à créer un réseau informatique reliant plusieurs ordinateurs. Ce qui a conduit en 1968 au premier réseau informatique. C'est véritablement le 21 novembre 1969, que s'opère la première connexion entre plusieurs ordinateurs de différentes universités américaines, connectées entre elles. *Les universités de Californie, Santa Barbara (UCSB), l'Institut de Recherches de Stanford et Université de l'Utah sont reliées à un « nœud » situé à l'Université de Californie, Los Angeles (UCLA) et permettant de diriger vers son destinataire, où qu'il se trouve sur le réseau, le message envoyé par un ordinateur distant.*[71]

C'est dans ces conditions que la première conférence internationale sur les communications informatiques, a lieu du 24 au 26 octobre 1972, à Washington[72]. Les Etats comme la France et la Grande Bretagne travaillent dès lors à l'élaboration de leur propre réseau. Tous les Etats ressentent alors le besoin de créer leur propre protocole de communication commun à tous ces réseaux. Ce besoin s'accentue avec la place qu'occupe désormais l'information. La méfiance de tous les Etats est liée au fait qu'avec le premier choc pétrolier, en 1973, l'information apparaît comme une ressource

---

[69] Idem, p. 181 : c'est l'année de Sputnik, le premier satellite artificiel de la terre, lancé par l'URSS et voir également **Suzanne LABIN**, Compétition, URSS-USA économique militaire culturelle : collection l'ordre du jour, éditions de la table ronde paris VIIe, 1962.

[70] Cf. **GUEDON**, la planète cyber, internet et le cyberespace, éditions GALLIMARD.

[71] Cf. **GUISNEL J.**, Guerres dans le Cyberespace, services secrets et internet, éditions la Découverte, Paris, 1995, p. 5 à 8

[72] Cf. **STANLEY W.**, Computer communications : impacts and implications/ International Conference on Computer Communication, Washington, 1972 ; **ANIS Jacques**, Texte et ordinateur : l'écriture réinventée, collection : Méthodes en sciences humaines, publication : Paris ; Bruxelles : De Boeck université, 1998, p 181.

stratégique[73].C'est dans cette ambiance de recherches technologiques qu'est créé, en 1974, l'Inter Networking[74] Group chargé de construire ce protocole commun.

L'outil internet est ainsi créé. Or son usage n'est efficace que parce qu'il est une ressource informatique qui s'intègre dans un espace qu'il est convenu d'appeler réseau. Selon S. GHERAOUTI-HELIE[75], le réseau (Network) est constitué d'un ensemble collaboratif de ressources informatiques de transmission offrant des services permettant de réaliser : le partage des ressources informatiques interconnectées, la mise en relation des applications et des personnes, l'exécution des programmes à distance, le transfert d'informations.

Mais l'immensité de ces possibilités ne suffit plus. La technologie se développe davantage et on est à l'ère des nouvelles technologies de l'information et de la communication désignées par le sigle NTIC. Ces technologies incluent la numérisation, les traitements des signaux et l'apparition de l'informatique communicante[76]. Dès cet instant, les réseaux de télécommunication connaissent une activité considérable. Aux réseaux traditionnels constitués par les réseaux téléphoniques, se substituent une nouvelle forme de communication : la commutation des paquets jusqu'alors au stade de l'expérimentation et qui prend dès lors une place prépondérante par la suite[77].

Cet ensemble des réseaux qui opèrent des échanges entre eux, est caractérisé par son immatérialité. Il répond à une appellation particulière : le cyberespace. Il est un mot tiré de l'anglais des Etats-Unis *« cyberspace »*. Il a été inventé par le romancier William

---

[73] Sur cette question cf. p101 de l'empire des réseaux, op cit. supra 11, note 43 : et à la page 46 du livre, la Russie entre en ligne de compte, Staline est un passionné des écoutes téléphoniques dans la mesure où il considère le téléphone comme un moyen révolutionnaire. C'est d'ailleurs pour cette raison qu'il était opposé à Trotski.

[74] Terme utilisé pour la première fois par **KAHN Robert** lors de la première conférence mondiale des télécommunications à Washington DC en 1972.

[75] Cf. **GHERAOUTI-HELIE S. et DUFOUR A**. « de l'ordinateur à la société de l'informatique », éd PUF.

[76] Cf. Panorama sommaire des nouvelles technologies de l'information et de la communication, étude réalisée par le Sénat, en ligne sur : http://www.senat.fr/panocomm.html.

[77] Cf. P. 14 du panorama précité où est clairement présentée la volonté d'expérimenter cette technologie.

GIBSON[78]. Il le nomme aussi « info sphère ». Selon cet auteur américain de science-fiction, il s'agit d'un espace utopique dépourvu de murs où circule l'information. Il invente ce terme en 1984 et il faut reconnaître que sa conception du cyberespace cadre effectivement avec la réalité dans la mesure où il n'existe en fait aucune frontière en matière de réseaux numériques et particulièrement en ce qui concerne les autoroutes d'échange des informations prises globalement.

D'une manière générale et selon le sens commun, le dictionnaire LAROUSSE, Grand Usuel[79] définit le cyberespace comme un environnement résultant de la mise en œuvre de systèmes de réalités virtuelles ou de l'utilisation de réseaux télématiques internationaux.

Quant au dictionnaire DIXEL des éditions le Robert[80], il précise que le cyberespace est un nom masculin issu de l'anglais *cyberspace* et signifie *l'espace de communication créé par l'interconnexion mondiale des réseaux (internet).*

Pour compléter cette définition technique, la télématique est définie par le même dictionnaire comme « l'ensemble des techniques qui combinent les moyens de l'informatique avec ceux des télécommunications »[81]. Le dictionnaire de SENSAGENT[82] définit à son tour, le cyberespace comme un réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants.

---

[78] L'auteur GIBSON a défini le cyberespace dans son roman « NEUROMMANCER », Paris, 1984, édition J'ai Lu. Cf. **WALL D**., Cybercrime, the transformation of crime in the transformation age, Polity, United Kingdom, 2007, p.10.

[79] Dictionnaire LAROUSSE, Grand Usuel, dictionnaire encyclopédique in extenso, Mars 2007, édition LAROUSSE

[80] Dictionnaire DIXEL 2011, éditions Le Robert, p 480.

[81] Idem, p. 1859

[82] Dictionnaire en ligne à consulter sur http://www.sensagent.com/

En France, l'Agence Nationale de Sécurisation des Systèmes d'Information (ANSSI) définit le cyberespace comme *l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques*[83].

Il se dégage de ces définitions, une pluri dimension du cyberespace : il est à la fois virtuel[84] et réel[85]. Il prend surtout en compte des réseaux mondiaux et des aspects des télécommunications.

Dans le cyberespace, les informations, les images et les sons évoluent. Il fait intervenir les logiciels reliés qui communiquent entre eux par l'intermédiaire de la fibre optique[86]. La fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Elle offre un débit d'informations nettement supérieur à celui des câbles coaxiaux (ou enveloppant) et supporte un réseau " large bande " par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.[87]

Ces évolutions technologiques progressives d'internet et des réseaux de télécommunication conduisent à la récupération de cet outil par les usagers civils. Il faut à ce sujet noter la rapidité avec laquelle l'informatique s'est incrustée dans les usages quotidiens. En moins d'une génération, l'implantation de l'outil informatique s'est faite et ce support est adopté dans tous les secteurs d'activité humaine. En effet, à l'origine, internet et les réseaux afférents ont été créés pour servir de support à l'armée

---

[83]Cf. Défense et sécurité des systèmes d'information stratégie de la France, ANSSI, 2011, citée par **Bertrand BOYER** dans son ouvrage Cybertactique conduire la guerre numérique, éditions NUVIS, Paris 2014, p. 25.

[84] Virtuel parce que le chemin emprunté par les informations ou données dans le cadre des transferts et de l'outil informatique ne sont pas visibles à l'œil nu. Ils ne sont pas matériels et restent loin des réalités palpables.

[85] Réel pour exprimer le fait que les données utilisées sont des éléments tirés de la vie quotidienne notamment les informations sur les personnes telles que le nom, prénom, adresse géographique, activité ou encore état de santé.

[86] Cf. **WAUTELET**, La naissance du cyberespace, in les cyber conflits, internet, autoroutes de l'information et cyberespace : quelles menaces ?, éditions Complexe.

[87] cf. http://www.science.net/?onglet=glossaire&definition=2937, consulté le 03 janvier 2012.

américaine[88]. La récupération par les civils se traduit par l'usage quotidien d'internet comme support de travail aussi bien par les administrations, les entreprises que les particuliers. Cette utilisation de l'outil informatique n'est pas sans conséquence sur les données propres aux personnels, dans l'art, l'éducation, la formation.... A chaque connexion, l'internaute laisse un certain nombre d'informations, d'empreintes, des traces dont la protection ou la sécurisation n'est pas toujours garantie. Ce qui va poser le problème de la gestion et du contrôle de ces informations. En d'autres termes, quel usage fait-on de ces données ? Existe-t-il un moyen de protéger ces informations et usages privés ?

Ces interrogations se justifient par le fait que par exemple, en France, l'administration dispose dans ses fichiers de nombreuses informations concernant les utilisateurs de l'outil informatique.
Dès lors, se développe une volonté à la fois sournoise ou occulte de la part de l'Etat de vouloir utiliser ces informations à l'insu des personnes concernées, et de centraliser ces informations sous la forme de Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus. C'est le projet SAFARI dévoilé par l'article du journal Le Monde du 21 mars 1974 titré « Safari ou la chasse aux Français ». Il *vise à centraliser les fichiers administratifs en attribuant à chaque citoyen un identifiant unique. Ce numéro serait le même utilisé dans tous les administrations publiques de l'Etat français*[89]. Cette manière de procéder de l'Etat français, en l'absence de tout débat démocratique, est en contradiction avec les recommandations du Conseil d'Etat et s'apparente à une violation

---

[88] C'est au cœur de la guerre froide en 1962 qu'est apparue la nécessité d'un réseau technologique performant et suffisamment décentralisé : la commutation des paquets : cf. **ANIS Jacques** : texte et ordinateur : l'écriture réinventée, p. 181.

[89] Le journal Le Monde du 21 mars 1974 titre « *SAFARI ou la chasse aux français* » et cet article de Philippe BOUCHER accentue le débat des données personnelles des français en le portant sur la place public. Voir également les dossiers du Sénat notamment « 1977 - 1978 : le Sénat invente les autorités administratives indépendantes », consultable en ligne cf. http://www.senat.fr/evenement/archives/D45/context.html.
Voir également **LAMARCHE T.** et al. , Fichiers et Libertés : le cyber-contrôle : 25 ans après, éditions L'harmattan, Paris, 2003, Collection Terminal n° 88, informatique, culture, société.

des libertés[90]. Le Conseil d'Etat émet auparavant des inquiétudes quant à la protection des données circulant via l'utilisation de l'informatique dès 1969. Ses recommandations rendues en 1971 se résument essentiellement à l'impact de l'informatique sur les libertés individuelles.

Ainsi, les voix s'élèvent pour dénoncer ces pratiques cachées de l'administration[91].

Par conséquent, la question de la protection des données personnelles des usagers d'internet va se poser. En effet, la crainte de voir bafoués les principes de libertés et le besoin de garantir la sécurité des informations personnelles justifient la mise en place d'une politique de protection des données personnelles des administrés notamment avec la création de la Commission *Informatique et Libertés* par le premier ministre Pierre MESSMER. Le premier rapport à l'issu des séances de travail de cette commission, est le rapport TRICOT[92], remis en juin 1975.

Plusieurs réflexions ont été menées et des débats relatifs à la protection des données des personnes sont tenus. Dans cette vague de discussions, les parlementaires interviennent et parmi eux, le député Jean FOYER établit le rapport FOYER[93] contenant les craintes liées à l'informatique et principalement le traitement des données collectées par l'intermédiaire de l'informatique. Les débats sur la loi Informatique et Libertés commencent le 04 octobre 1977, lors de la Commission CHENOT[94], du nom du vice-

---

[90] Les recommandations du Conseil d'Etat datent de 1971 à la suite de sa saisine par le Gouvernement en 1969 quant à l'examen des risques de l'usage de l'outil informatique sur les libertés individuelles : cf. Rapport n° 3125 de M. FOYER, tome I.

[91] Notamment l'article précité de Philippe BOUCHER. Compléter pour une étude détaillée et poussée avec l'article de **GRUBER A.**, Le système français de protection des données personnelles, in *Petites Affiches* n° 90 – 4 mai 2007.

[92] Cf. Rapport TRICOT de juin 1975, cf. http://www.assemblee-nationale.fr/histoire/informatique-et-libertes/1ere_seance_rforni.asp.

[93] Rapport n° 3125 de M. **FOYER**, tome I, ce rapport a été annexé au procès verbal de la Commission CHENOT. Il est disponible et consultable sur le site du Sénat, cf. http://www.assemblee-nationale.fr/histoire/informatique-et-libertes/rapport3125_Foyer_tome1.asp#_ftn2.

[94] La Commission informatique et Libertés a été créée pour proposer des règles de protections de la vie privé de des libertés des citoyens. Elle dépendait du Garde des Sceaux et était présidée par Bertrand CHENOT.

président au Conseil d'Etat Monsieur Bernard CHENOT Ces débats traitent du devenir des données collectées au regard des procédés électroniques déployés et en plein essor au lendemain de la seconde guerre mondiale. Ces utilisations diverses répondent au besoin de traiter des informations en évitant le risque de les déformer *lors de la transformation des données collectées en données-résultats*[95]. Dans les lignes du rapport CHENOT, les concepts étudiés (à savoir la protection des données et l'exercice des libertés) revêtent un caractère restrictif avec la liste des actes concernés par les règles proposées. Le rapport CHENOT parle en effet de traitement de données spécifiques et des libertés individuelles. Plusieurs débats ont lieu avec des votes pour certains amendements dans leur intégralité et d'autres qui se trouvent plus généralisés. C'est à la suite de cette commission CHENOT que naît la loi informatique et Libertés du 6 janvier 1978[96]. La loi Informatique et Libertés aborde quant à elle, le principe de libertés d'une manière plus générale[97]. Cet important dispositif législatif que représente la loi informatique et libertés, est plusieurs fois modifié pour s'adapter aux évolutions[98].

---

[95] Cf. Informatique et Libertés, Rapport FOYER au tome 1, p. 3, op. cit.

[96] Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés publiée au Journal Officiel du 07 janvier 1978

[97] Le tome 2 du rapport FOYER présente sous forme de tableau comparatif les amendements tels qu'ils ont été modifiés : cf. annexe

[98] Texte de loi plusieurs fois modifié par les lois suivantes :

- Loi N°88-227 du 11 Mars 1988 relative à la transparence financière de la vie politique parue au JORF du 12 mars 1988 page 3290;

- Loi n° du 16 décembre 1992 relative 92-1336 à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur, parue au JORF n°298 du 23 décembre 1992 page 17568 ;

- Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1) parue au JORF n°152 du 2 juillet 1994 page 9559 ;

- Loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle parue au JORF n°172 du 28 juillet 1999 page 11229 ;

- Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations parue au JORF n°88 du 13 avril 2000 page 5646 texte n° 1

- et la Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1) parue au JORF n°182 du 7 août 2004 page 14063 texte n° 2

C'est le lieu de préciser que la France a été inspirée par l'Allemagne et les pays du nord de l'Europe c'est-à-dire la Suède[99], la Norvège et la Finlande. [100]

En effet, depuis 1766, il existe en Suède un principe de publication et de publicité des documents administratifs et les solutions ont été adaptées à l'ordinateur[101]. En ce qui concerne la protection de la vie privée, c'est à la suite du Land de la Hesse en Allemagne, que les pays scandinaves se classent parmi les premiers dans l'élaboration de législations protégeant les données personnelles des individus. Dans le but de conserver des informations personnelles et de les garder secrètes tout en les protégeant par des textes législatifs, il n'est certainement pas encore question de criminalité.

Toutefois, les différents législateurs ont dû réfléchir à cette problématique. Les nombreuses mutations et évolutions technologiques de l'outil Internet et informatique laissent envisager l'hypothèse de détournement des informations par exemple.

III- LA CYBERCRIMINALITE ET SES PROBLEMES

D'un certain point de vue, l'Organisation pour la Coopération et le Développement Economique (OCDE) est à l'initiative des réflexions entreprises par les pays de l'Union européenne sur les questions de protection contre la fraude informatique[102]. Dès les années 80, et précisément en 1982, des experts de l'OCDE

---

[99] Loi de 1973 sur la protection des données en Suède, cf. actes du colloque sur les registres informatisés dans le secteur public (en droit civil, pénal et administratif) des 2 et 4 octobre 1995, p. 265.

[100]Cf. **STRÖMHOLM Stig**, Ordinateurs et droit (A propos d'un projet de loi suédois sur les ordinateurs) in: Revue internationale de droit comparé Vol.25N°1, Janvier-mars 1973. pp. 55-67. Voir également dans le Rapport du député M **GOUZES Gérard**. Il précise qu'au moment de l'adoption de la loi du 6 janvier 1978, seuls la Suède et le Land de la Hesse, respectivement en 1973 et 1970 possédaient en Europe une législation relative aux traitements automatisés des informations nominatives, cf. Rapport GOUZES, n° 3526 Assemblée nationale 2004 in Informatique et libertés protection des personnes physiques à l'égard des traitements de données à caractère personnel les, éditions de Journaux officiels, octobre 2004

[101]Cf. **STRÖMHOLM Stig**, Ordinateurs et droit (A propos d'un projet de loi suédois sur les ordinateurs). In: Revue internationale de droit comparé. Vol. 25 N°1, Janvier-mars 1973. pp. 55-67.

[102] Dans ce cadre, l'OCDE a émis sous forme de recommandation des lignes directrices relatives à la sécurité des systèmes d'information : cf. Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité, Les présentes *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* ont été adoptées

définissent la cybercriminalité comme un « délit informatique ». Selon ces experts, le délit informatique s'entend de *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement informatique de données et/ou de transmissions de données*[103]. Cette définition de l'OCDE en 1982 est aujourd'hui dépassée dans la mesure où elle ne rend pas suffisamment compte du vaste ensemble qu'est la cybercriminalité de nos jours. La cybercriminalité englobe en effet beaucoup d'autres actes que nous développerons plus loin.

Il convient de noter que dès les premières heures d'implantation de l'informatique et du traitement de données, l'OCDE envisage les éventuelles dérives[104]dans son document relatif aux recommandations du conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Il faut remarquer qu'il n'est pas réellement question de développement informatique en tant que tel[105]. Et pourtant, l'Organisation pour la Coopération et le Développement Economique incite les pays d'Europe à insérer dans leur droit pénal respectif des dispositions protégeant de la fraude informatique. Cette incitation est apparue explicitement dans le rapport de l'OCDE de 1986[106].

Dans la société contemporaine, Internet, est devenu au fil des années plus qu'un outil de travail, un véritable support d'éducation, instrument d'acquisition et de vérification des connaissances personnelles, un moyen de communication et plus

---

sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037ème session, le 25 juillet 2002.

[103] Cf. **ALTERMAN H.** et **BLOCH A.** : la fraude informatique, Paris, Gaz. Pal, 3 sept. 1988, p. 530.

[104] Cf. Recommandation du conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel du 23 septembre 1980 in OCDE, Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, Paris, OCDE, 2002. Il s'agit de la première étude réalisée sur l'impact d'internet les

[105]Cf. O.C.D.E., La fraude liée à l'informatique : analyse des politiques juridiques, Paris 1986.

[106] Les lignes directrices relatives à la protection des données personnelles ont été édictées en 1980 dans les recommandations précitées en note 103. Elles sont réaffirmées en 1985. Pour prendre la forme de rapport en 1986 sur la base duquel la précédente analyse des politiques a été faite et publiée en 1986. Elles ont par la suite a été complétés en 1992 par l'OCDE puis en 1998 et enfin en 2002. Il apparaît sous la forme actualisée de 2002 cf. OECD (2002), *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OECD Publishing.

largement une source d'accès à l'information. En d'autres termes, il constitue une des caractéristiques de la société contemporaine quel que soit le continent considéré. Nous en voulons pour preuve les diverses utilisations faites de l'internet à savoir les échanges de données professionnelles et personnelles entre internautes publics ou privés (photos, images, documents). Ces multiples utilisations de l'outil internet ainsi que des éléments comme la numérisation, les échanges de données sont source de dérives dans la mesure où elles facilitent des intrusions dans les ordinateurs de la part de certaines personnes mal intentionnées[107].

En effet, les informations échangées sur internet ne sont pas forcément des informations vraies, vérifiées, scientifiques d'une part, et peuvent être porteuses d'une intention d'autre part. Les personnes touchées étant nombreuses, elles peuvent avoir des effets négatifs. L'accès facile à l'internet dans n'importe quelle partie du monde soulève des problèmes d'utilisation et d'interprétation de l'information véhiculée : lorsqu'une information est donnée, plusieurs personnes peuvent y avoir accès. Dès lors qu'une information est publiée aux Etats- Unis, les personnes vivant à Madagascar en sont informées, pourvu qu'elles aient un accès à l'internet. On en arrive à des comportements dépassant la sphère de la simple récupération des données des usagers à leur insu. C'est l'ère des attaques multiformes, des vols des données et aussi des échanges d'informations utilisées à des fins malicieuses et ayant notamment pour objectif de porter atteinte à l'ordre public. Partant, la protection des données à un degré supérieur est nécessaire. Il s'agit de la problématique de la surveillance de la communication sur internet sans que cela ne porte atteinte à la liberté des internautes quant à l'utilisation de cet outil.

Ces dernières manifestations et tous les dérapages conduisent à s'interroger de la manière suivante : peut-on envisager la suspension d'internet, en France, au moins pour une durée de vingt-quatre heures pour des questions de sûreté ou de sécurité nationale

[107] C'est-à-dire, des personnes qui cherchent à nuire à d'autres avec ou sans raison, ou alors ces personnes intrusives qui profitent de ces attaques pour utiliser contre leur gré les informations personnelles dérobées et par conséquent en faire des sources de chantages de tous genres.

comme c'est souvent le cas dans certains pays tels que la Chine[108]? Est-ce qu'en cas de menaces graves à l'ordre public, (cas de terrorisme) internet peut-il être suspendu ?

C'est tout naturellement qu'on peut répondre par l'affirmative en raison de la gravité des menaces. Il s'agit de cas extrême. Qu'en est-il de la cybercriminalité traditionnelle (à moindre mesure en comparaison à l'usage d'internet à des fins terroristes)?

Pour comprendre ce qu'est la cybercriminalité, il faut tout d'abord expliciter les premiers cas de délinquance informatique à savoir les intrusions informatiques. A l'origine, les informaticiens développent un jeu informatique à but purement ludique « Core War[109]. Il consiste dans l'écriture d'un programme capable de créer des copies de lui-même tout en cherchant à éliminer les programmes adverses. Ceci a été observé au début des années 80. C'est dire qu'il est question de prévoir des éventuels détournements. Ce *Core War* deviendra ce qu'on appelle aujourd'hui le virus informatique. Le virus est une catégorie d'infection informatique selon la classification d'Adleman. En effet, les infections informatiques se subdivisent en deux groupes. D'une part les infections simples qui se déclinent soit en bombe logique soit en chevaux de Troie et d'autre part les infections

---

[108] Suspension de Google en Chine pendant les élections pour des raisons politiques notamment en 2010, puis récemment en 2012 cf. Journal Les Echos du 12 novembre 2012 : «*Cette nuit en Asie: censure massive pour Google en Chine* ».

Cet article est l'occasion pour les journalistes de révélé qu'il est quasiment impossible depuis quelques jours d'accéder aux services en ligne proposés par Google. L'article est également disponible en ligne : http://www.lesechos.fr/economie-politique/monde/actu/0202378590397-cette-nuit-en-asie-censure-massive-pour-google-en-chine-509687.php; voir également pour la même question de censure, le journal Les Echos de septembre 2011, partie actualité : *Google rencontrait des problèmes avec la Chine.*

Le quotidien Le Parisien dans un article du 20 mars 2010 intitulé *Google, la presse chinoise se déchaîne* révèle un commentaire de l'agence Chine Nouvelle qui accuse Google d'être un instrument politique des Etats-Unis et d'être lié aux services de renseignements américains dans les termes suivants : *"Certains internautes chinois qui préfèrent utiliser Google ne savent peut-être pas encore que, en raison des liens étroits entre Google et les services de renseignements américains, les historiques des recherches sur Google seront conservés et seront utilisés par les agences de renseignements américains".*

[109] Cf. O.C.D.E., La fraude liée à l'informatique : analyse des politiques juridiques, Paris 1986; voir également le dossier réalisé par le club de la sécurité des systèmes d'information français (CLUSIF): dossiers techniques sur *les virus informatiques*, décembre 2005, Espace Menaces.

autoreproductrices à savoir les vers et les virus[110]. En effet, c'est en1986 que l'improbable se produit : le premier cas d'infection dans le monde des « *Personal Computer* » ; il s'agit d'une part de « *Basit et Amjad Farooq Alvi* » pour le virus BRIAN et d'autre part du virus VIRDEM[111] imputable à l'action de Ralf Burger. On parle à cette même époque de l'apparition de vers malveillants[112]dont le plus marquant reste RTM qui a atteint internet, le 2 novembre 1988. Il porte les initiales de son créateur Robert Tappan Moris. Une partie non négligeable d'infection a été évaluée à 5% du réseau. C'est d'ailleurs cet incident qui est à l'origine de la création, en 1988, en Angleterre, à l'Université de Carnegie Mellon[113], d'Equipes de réponse aux urgences informatiques en anglais (Computer Emergency Response Team) en abrégé CERT. Ces structures sont mises en place pour répondre en urgence aux victimes d'attaques informatiques. Il s'agit de programme dans le domaine de la cybersécurité[114].

A partir de 1989, un grand développeur de virus, Dark Avenger en Bulgarie[115], facilite la propagation des virus en imaginant de nouveaux procédés. Dès lors en 1989 est lancée une alerte au virus Data crime, programmé pour exécuter un formatage bas, du niveau du premier cylindre des disques durs qu'il a infectés. Il détruit la table d'allocation

---

[110] Cf. **FILIOL Eric** a étudié la question en appui avec les travaux ADLEMAN, chercheur américain et avec un autre chercheur **Fred COHEN** de la même époque. Il apporte davantage de précisions dans une étude intitulée *Concept et avenir de la virologie informatique.*

[111] Dossiers techniques du groupe VIRUS réalisé par le Club de la sécurité des systèmes d'information Français (CLUSIF).

[112] Cf. **PAGET F.**, Vers et virus-Classification, Lutte virale et Perspective, édition DUNOD, p.49 : ce virus a été découvert en mars 1989. Il concernait la Hollande et la France.

[113] L'Université Carnegie Mellon de Londres favorise la création des CERT. Cf. notamment l'historique sur http://www.cert.org/csirts

[114] La cybersécurité est définie par Esteral Consulting comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ». Cette définition est citée *dans l'étude sur la Cyberdéfense et Cybersécurité au sein des institutions européennes*, réalisée par Esteral Conslting à la demande de la délégation aux affaires de sécurité du Ministère français de la Défense.

[115] Cf. **PAGET F.**, Vers et virus-Classification, Lutte virale et Perspective, édition DUNOD, p.53 : ce virus a été découvert en mars 1989. Il concernait la Hollande et la France ; À la poursuite de Dark Avenger : l'affaire des virus au goût bulgare / dossier réuni et présenté par **Pascal LOINTIER** avec **Anna BAKALOVA**, **Vesselin BONTCHEV, Vassil HABOV** et la participation de **Bryan CLOUGH** et **Paul MUNGO** et de **Vladimir KOSTOV**, Paris éd. Dunod tech, 1993

des fichiers entraînant la perte des données[116]. A la suite de ce grand développeur, les ordinateurs sont contaminés via les courriers électroniques. Dix ans plus tard, en 1999, le virus W32/Sk@M, est créé et ouvre une longue liste de virus[117]. Il est question d'une contagion virale mail par mail. C'est ensuite, le virus W97M/Melissa@MM qui infecte les boîtes mail par groupe de 50. En 2000, la vitesse de contagion s'accroît et prend une autre dimension importante dans la mesure où le ver VBS/Loverletter@MM permet une propagation grâce à une pièce jointe[118]. Il suffit alors de cliquer sur ladite pièce jointe pour que l'ensemble des contacts du correspondant aient le message envoyé. Ce message favorise dès lors la contagion de leur ordinateur. Les performances augmentent avec le format Hyper Text Markup Language (HTML) grâce auquel une seule prévisualisation suffit à infecter la machine.

Les outils de contagion ont eux aussi changé au fil du temps et des évolutions techniques. Les disquettes étaient les premiers outils de propagation des virus. Les développeurs de virus s'orientent ensuite vers d'autres supports contenant des données notamment les *Personal Digital Assistant* (PDA), les téléphones portables. Les virus sont donc perfectionnés et parviennent même à infecter les appareils via des SMS : c'est le cas avec W32 Liberty[119]. On observe ainsi une dangerosité grandissante au fil des années : parti dans les débuts des années 90 d'un simple défi d'infecter (pour tester les performances techniques) des ordinateurs, les intérêts des développeurs de virus muent pour prendre des formes criminelles. C'est désormais un besoin de collecter des informations par des intrusions informatiques pour, par la suite, revendre contre de fortes sommes, ces informations frauduleusement collectées.

---

[116]Cf. **PAGET F**, Vers et virus-Classification, Lutte virale et Perspective, édition DUNOD, p.49 op. cit. ; Voir également sur cette question **FILIOL Eric**, les virus informatiques : théorie, pratique et applications édition Springer, collection IRIS, Paris 2000.

[117] Cf. **FILIOL Eric**, les virus informatiques : théorie, pratique et applications, édition Springer, collection IRIS, Paris 2000.

[118] Dossier les virus informatiques, rédigés par l'association CLUSIF ; Voir également p 295 du livre de **PAGET François**, Vers et virus - Classification, lutte antivirale et perspectives, édition DUNOD.

[119] Idem

Par l'intermédiaire des outils de collecte d'informations, les virus s'incrustent dans le système qu'ils piratent. Ils détruisent les programmes ou les rendent inaccessibles pour s'installer et communiquer les informations stockées sur le disque dur local de l'ordinateur ou le support infecté[120]. Le virus est défini par le vocabulaire des TIC comme un « l*ogiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné. »*[121].

Les virus constituent dès lors, à la fois une menace pour les particuliers, les entreprises et les administrations. En effet, les attaques réalisées à l'encontre des informations échangées ou stockées sur des serveurs d'entreprises notamment les banques, consistent pour certaines dans l'intrusion des systèmes d'information pour s'approprier ces données et les utiliser dans d'autres contextes, c'est-à-dire les pirater, les vendre, à l'insu des véritables propriétaires de ces données. En ce qui concerne les particuliers, ces attaques les exposent à la divulgation des données personnelles notamment les cartes bancaires, dossier médical, passé judiciaire.

Les virus créent une atmosphère d'insécurité des données stockées. Cette atmosphère d'insécurité des données des individus mais aussi des administrations, des entreprises liées à l'usage des nouvelles technologies, pousse les concepteurs de systèmes informatiques à recourir à des pratiques protectrices. Au plan technique, les informaticiens décident de répondre à ces pratiques malveillantes. Ils conçoivent des techniques spécifiques de lutte contre ces attaques informatiques. Parmi ces moyens de

---

[120] Cette technique est souvent utilisée par les pirates et les voleurs de données pour dérober des informations. Une telle pratique a été à l'origine de l'arrestation d'un salarié américain Timothy Lloyd de la société OMEGA : cette affaire a été jugée par les tribunaux. **Timothy LLOYD** a occasionné le blocage du système informatique de l'entreprise OMEGA INGENIEERING, son employeur, grâce à l'insertion d'une bombe informatique à l'intérieur du système informatique. Cf. **Nico PRAT et Antoine DUBUQUOY**, les Miscellanées d'internet, édition Fertjaine, 2012 et pour une version en ligne, cf. http://www.ultimes.fr/informatique/les-5-piratages-informatiques-les-plus-celebres-32/.

[121] Vocabulaire des techniques de l'information et de la communication (TIC) 2009, *Termes, expressions et définitions publiés au journal officiel du 20 mai 2005*, Commission générale de terminologie et de néologie.

lutte contre les attaques informatiques, il y a les anti-virus, les pare-feu de protection, les anti-spam, les courriers indésirables dans les boîtes de réception de messagerie (ou boîte mail).

L'anti-virus est défini comme un logiciel[122] de protection dont le but est de détecter la présence de logiciels malveillants (comme par exemple les chevaux de Troie dans un ordinateur ou dans des périphériques amovibles (CD, DVD, clé USB,...) pour vérifier que les fichiers qui y sont présents ne contiennent pas de virus connus[123].

C'est réellement en 1991 que les concepteurs comme SYMANTEC, IBM, McAfee, et autres proposent ces techniques de lutte contre les intrusions par des vers encore appelés virus. Les anti-virus confectionnés pour combattre les vers malveillants semblent inefficaces puisque les intrusions ont lieu malgré l'installation d'un anti-virus sur un ordinateur. En réalité, les anti-virus ne sont pas toujours des freins résistants. Les développeurs de virus trouvent sans cesse des moyens pour contourner les règles de sécurité ou les codes composés par les anti-virus. Pourquoi ces instruments censés faire obstacle à ces intrusions non désirées ne suffisent pas ?

Face à l'inefficacité apparente de ces anti-virus et pares feux, certains fabricants comme APPLE ont créé des ordinateurs et appareils ne nécessitant aucun recours à l'antivirus. Cette manière de procéder pourrait constituer une solution. D'autres solutions comme les code de verrouillage ou des techniques de cryptologie[124], des codes sécurité et autres mots de passe dans les entreprises ou les sociétés complèteront la liste en vue de

---

[122] Le logiciel est lui-même défini par le vocabulaire des techniques de l'information et de la communication (TIC) comme l'ensemble des programmes, de procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données, Journal officiel du 22 septembre 2000.

[123]Cf. Définition donnée sur le site de la sécurité informatique :http://www.securite-informatique.gouv.fr/gp_mot4.html

[124] L'article 28. I de la loi n° 90-1170 du 29 décembre 1990, parue au Journal officiel de la République Française du 30 décembre 1990 page 16439 définit les prestations de cryptologie comme toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet.

garantir la sécurité des échanges de données mais aussi assurer un stockage préservé des informations.

Sur le plan juridique, l'inquiétude de sauvegarde des libertés des individus par rapport à leurs données personnelles (libre consentement donné en connaissance de cause pour figurer dans un fichier par exemple) a mué pour devenir un souci de protection des informations contre les virus susceptibles d'endommager ces données, de les faire disparaître ou même de s'en approprier à d'autres fins.

Les systèmes législatifs deviennent plus sévères et l'idée de sanctionner les « voleurs de données ou pirates » fait son chemin.[125] C'est dire qu'au fil du temps, les problématiques de sécurité s'accentuent avec l'évolution considérable de la communication : de l'oralité à l'écriture, de l'écriture à l'échange des informations en passant par leur traitement via l'ordinateur et le réseau. Ainsi, les problématiques de sécurité, tout en englobant un souci de protection contre les dérives de l'administration à l'égard des administrés, se préoccupent aussi aujourd'hui de la sécurité des données personnelles de tous les utilisateurs du réseau. En d'autres termes, l'insécurité créée par l'usage des technologies de l'information est sans cesse grandissante et s'accroît à mesure des avancées technologiques. En cela, certaines personnes se servent des supports de communication dont Internet à des fins malsaines, différentes des usages classiques et traditionnels. Elles n'hésitent pas à en faire un moyen de commettre des actes répréhensibles, interdits par les textes de lois en vigueur. Certaines des infractions concernent directement les utilisateurs s'agissant de leurs données personnelles enregistrées ou échangées via Internet. D'autres sont relatives aux attaques des systèmes ayant servi de support lors de l'utilisation d'Internet.

Ces infractions commises par le biais d'Internet recouvrent le vocable de cybercriminalité. Comment définir ce terme qui fait appel à divers éléments à savoir la communication, les données personnelles, leur traitement et les technologies de

[125] On observe un durcissement des différentes lois et adaptation des infractions pénales notamment avec dans le code pénal dès 1984 des infractions comme l'intrusion informatique, ou l'accès frauduleux ou encore le maintien frauduleux dans un système informatique.

l'information ? S'agit-il seulement une notion générique regroupant dans leur globalité les infractions commises par le biais d'Internet, ou plutôt d'une partie de ces actes ?

Jusqu'en 2010, la cybercriminalité n'est pas un mot défini par le dictionnaire français. On trouve cyber, et d'autres substantifs composés à partir de ce préfix emprunté à l'anglais *cyber*. Il sert à former des noms en rapport avec le multimédia, Internet, le Web.

Et le premier mot de la série des noms avec cyber est la cybernétique.

Il faut considérer la conception de la cybercriminalité contenue dans le Préambule de la Convention sur la cybercriminalité du Conseil de l'Europe dite « de Budapest » du 23 novembre 2001, entrée en vigueur le 1er juillet 2004. Aux termes des dispositions du Préambule, *la cybercriminalité est la criminalité dans le cyberespace*[126].

Le dictionnaire DIXEL de l'édition Le Robert de 2011[127], définit la cybercriminalité en ces termes : *« ensemble des activités illégales effectuées par l'intermédiaire d'internet.* »

Le problème que pose cette définition est qu'internet semble être assimilé à n'importe quel réseau de communication. Or, il ne faut en aucun cas sous-estimer cet outil.

Quant à l'Organisation des Nations Unies (ONU), elle considère la cybercriminalité comme : « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes et des données qu'ils traitent* ». L'Organisation des Nations Unies estime de manière plus large que la cybercriminalité est entendue de tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec ce système[128]. De cette considération, il faut clairement entendre que la

---

[126] Convention sur la cybercriminalité du Conseil de l'Europe publiée dans la Série des Traités Européens n° 185, publiée au Journal Officiel de la République Française du n°120 du 24 mai 2006 page 7568 texte n° 2 grâce au décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001.

[127] Définition de la cybercriminalité, Dictionnaire Le Robert 2011.

[128] Dixième congrès des Nations Unies à Vienne « la prévention du crime et le traitement des délinquants », 10-17 avril 2000 disponible sur http://www.uncjin.org.

cybercriminalité peut très bien avoir pour moyen un système pris isolément mais également un ensemble de systèmes c'est-à-dire le réseau de communication formé par les différentes composantes.

Apparaît ainsi la globalité et le caractère général de la cybercriminalité : il s'agit donc d'un terme générique désignant un groupe d'infractions qui répondent aux attaques des systèmes soit directement soit par le biais d'un système informatique ou d'un réseau de télécommunications.

L'ONU a désigné l'Union Internationale de Télécommunications (UIT) comme responsable des questions relatives aux technologies. C'est ainsi que l'UIT, dans son guide pour comprendre la cybercriminalité[129], définit le terme de la cybercriminalité par référence au cyber-délit. Ce vocable est lui-même défini par référence à d'autres documents comme *toute activité mettant en jeu des ordinateurs ou des réseaux en tant qu'outil, cible ou lieu d'une infraction.*

En dehors des frontières européennes, le département de la justice américaine (United States Department of Justice) définit la cybercriminalité comme *une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa perpétration*[130].

Cette conception américaine de la cybercriminalité est discutable en ce qu'elle ne tient pas compte de tous les acteurs cybercriminels éventuels notamment le receleur ou le complice d'actes cybercriminels.

Quant à l'office de police suisse, elle définit la cybercriminalité comme *l'ensemble de nouvelles formes de criminalité spécifiquement liées aux technologies de l'information, et*

---

[129] Guide pour comprendre la cybercriminalité, Ressources sur la législation relative à la cybercriminalité, Division applications TIC et cyber-sécurité, Département des politiques et stratégies Secteur du développement des télécommunications de l'UIT, avril 2009.

[130] Cf. U.S. Département of Justice : http://www.justice.gov/ et voir également page 22 de la thèse de M **CHAWKI** « Combattre la cybercriminalité ».

de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels[131]. La définition suisse paraît beaucoup plus satisfaisante.

Outre ces institutions (ONU, Union Internationale de Télécommunications, OCDE, et Département de la justice américaine), d'autres organismes comme le Computer Emergency Response Team (CERT) / Service propose la définition suivante : *les incidents commis par des initiés (des salariés actuels ou anciens ou des entrepreneurs(contractuels)) qui ont intentionnellement excédé ou ont employé improprement un niveau autorisé de réseau, le système, ou l'accès de données de manière à affecter la sécurité des données de l'organisation, des systèmes, ou des opérations quotidiennes d'affaires. Les incidents incluant n'importe quel compromis, manipulation, accès non autorisé excédant l'accès autorisé, falsification, ou la mise hors de service de n'importe quel système d'information, réseau, ou des données. Les cas examinés ont aussi inclus ceux dans lesquels il y avait une tentative non autorisée ou illégale de voir, divulguer, récupérer, supprimer, changer ou ajouter des informations*[132]. »

Par ailleurs, Daniel MARTIN appréhende la cybercriminalité sous un autre aspect. Il considère que : « *la malfaisance visant la haute technologie est une nouvelle forme de criminalité qui recouvre l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels*[133]». Il faut convenir que cette définition englobe le phénomène tant sur ses aspects physiques visuels que virtuels et techniques.

---

[131] Cf. Rapport 2003 de l'Office de police Suisse, Département fédéral de justice et police, Berne, juin 2003, p26.

[132] Cf. **FRANCHIN F.** et **MONNET R.**, le business de la cybercriminalité, publication Lavoisier, p. 20: la version originale de la définition*: "incidents perpetrated by insiders (current or former employees or contractors) who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organization's data, systems, or daily business operations. Incidents included any compromise, manipulation of, unauthorized access to, exceeding authorized access to, tampering with, or disabling of any information system, network, or data. The cases examined also included any in which there was an unauthorized or illegal attempt to view, disclose, retrieve, delete, change or add information. »*

[133]Cf. **MARTIN D. et MARTIN F-P**, Cybercrime : menaces, vulnérabilités et ripostes, PUF, criminalité internationale, 2001.

Quant à Steven FURNELLE, il distingue la cybercriminalité assistée par ordinateur de la cybercriminalité exclusivement liée à l'émergence d'internet. Selon lui, la première catégorie préexistait sous une forme différente avant internet et il s'agissait des discours racistes, de la fraude à la carte bleue par exemple. La seconde catégorie concerne le hacking, c'est-à-dire les intrusions frauduleuses, les attaques virales et leurs déclinaisons[134].

A la suite de ces deux propositions de définitions (celle de MARTIN et de FURNELLE), il est possible de retenir que le cyberespace est l'environnement dédié aux technologies de l'information et de la communication mais surtout qu'il est le lieu d'échange des réseaux formés par ces technologies.

La Commission européenne de Libertés et des Droits du citoyen estime que c'est un concept générique qui regroupe deux types de phénomènes à savoir d'une part la criminalité spécialement liée à l'informatique et d'autre part les infractions à l'aide des nouvelles technologies informatiques[135]. A ce stade précis, mentionnons que l'informatique est née avant les technologies de l'information qui, elles, se sont perfectionnées au fil du temps et se sont améliorées grâce aux usages et applications de leurs utilisateurs.

Quant à la Convention sur la cybercriminalité du 23 novembre 2001, appelée Convention de Budapest du Conseil de l'Europe, elle précise que la CYBERCRIMINALITE englobe trois catégories d'activités criminelles que sont d'abord les formes traditionnelles de criminalité (vol), ensuite la publication de contenus illicites par voie électronique et enfin les infractions propres aux réseaux électroniques c'est-à-dire les attaques visant les systèmes d'information, le déni de service et le piratage[136].

---

[134] Cf. **FURNELLE S.,** Cybercrime Vandalizing the information Society, Addison-Wesley 2002.

[135] Actes du Colloque organisé par la Commission Nationale de l'Informatique et des libertés (CNIL) et l'université Panthéon-Assas-Paris II - Sénat - 7 et 8 novembre 2005**.**

[136] Convention sur la cybercriminalité du Conseil de l'Europe publiée dans la Série des Traités Européens n° 185, www.coe.int/cybercrime.

Au niveau national français, le ministère de l'intérieur a également défini la cybercriminalité comme « *le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet*»[137]. Dès lors, il convient de s'interroger sur l'impact d'Internet quant à la vie privée des personnes. Autrement dit, Internet n'est-il pas révélateur de notre faiblesse en matière de sécurité et de protection de notre vie privée?

Concernant le continent africain, la cybercriminalité est appréhendée de manière différente : ce continent est présenté comme un paradis pour les cybercriminels.

Le Nigéria, en particulier, est réputé pour la criminalité des internautes, depuis cet Etat[138]. Cela peut paraître étonnant dans la mesure où dans cette partie du monde, très peu de personnes (en comparaison aux continents américain et européen) possèdent une connexion au réseau internet. Il en découle dès lors la question de l'origine de la cybercriminalité ou les justifications de la prolifération du réseau sur l'ensemble du continent africain de manière général et dans la partie ouest-africaine en particulier.

Pris singulièrement, il apparaît impossible que la faible connectivité des personnes au réseau facilite la cybercriminalité.

A l'inverse, en tenant compte des technologies de l'information et de la communication, d'une manière globale, il convient de raisonner autrement. C'est dire que la cybercriminalité ne doit pas être appréhendée uniquement sous l'angle de la connexion au réseau internet. Les autres composantes des réseaux numériques doivent également être considérées. Elles constitueront ainsi un des aspects importants des investigations et de la sanction des infractions qu'elles favorisent.

---

[137]Définition de la cybercriminalité donnée par le ministère français de l'intérieur, cf. http://www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite/presentation-cybercriminalite/view

[138] Le Nigéria est tristement célèbre du fait des attaques dites de scam 419, voir par exemple l'article *Cybercriminalité : les méthodes et les foyers des arnaqueurs,* in Afrique Expansion Magazine du 19 juillet 2011. Voir également *La cybercriminalité en pleine expansion en Afrique* in les Afriques sur http://www.lesafriques.com/medias-reflexion/la-cybercriminalite-en-pleine-expansion-en-afrique.html?Itemid=308?articleid=5067.

La cybercriminalité prend donc en compte à la fois internet et les techniques de l'information et de la communication. Les téléphones, les bippers, et autres appareils de communication sont impliqués. Il ne faut pas minimiser le fait qu'en Afrique notamment de l'Ouest, la téléphonie est plus utilisée, parce que plus accessible aux populations que des appareils informatiques du type ordinateur. L'acquisition de l'ordinateur représente pour la plupart des foyers à revenus moyens, un luxe. C'est en cela qu'il faut prendre en compte les infractions qui sont opérées par ce moyen de communication.

La cybercriminalité renvoie à la criminalité commise sur la toile[139], ou la criminalité commise à travers les outils numériques. Or, la criminalité recouvre à la fois les crimes, les délits et les contraventions. Dès lors, les infractions commises sur internet et par le biais des technologies de l'information et de la communication obéissent-elles à la nomenclature ou à la classification traditionnelle des infractions prévues par le code pénal ? La réponse à cette question mérite un rappel.

Traditionnellement, l'idée qu'on a du crime en droit pénal classique, c'est qu'il est constitué de trois éléments à savoir l'élément légal, l'élément intentionnel et l'élément matériel.

L'un des apports de notre travail est de montrer la différence qui existe entre le délit ou le crime relevant du droit commun et le délit ou le crime lié à l'usage des technologies de l'information et de la communication. En effet, en plus des éléments classiques précités de la criminalité ordinaire, le cybercrime est constitué d'un quatrième élément qui peut être considéré comme d'*ordre spatial* : son déploiement dans le cyberespace. C'est l'élément constitutif singulier, déterminant pour qu'on puisse parler de cybercrime. A titre d'exemple, le vol est un délit ordinaire mais dès lors qu'il est transposé dans le cyberespace, il devient un *cyberdélit*. Un élève qui subtilise un stylo de son collègue commet un délit de droit commun qu'on qualifie de vol. En revanche, si l'élève en question récupère des données de ce même collègue via un système

[139] La toile est une autre désignation du réseau internet, cf. le dictionnaire anglais Collins le web comme la toile.

informatique sans l'autorisation préalable de ce dernier, il commet un vol qualifié plutôt de *cyberdélit*.

A un degré plus important quant à la gravité de l'infraction, l'article 221-5-1 du code pénal français qualifie de crime « *le fait de faire à une personne des offres ou des promesses ou de lui proposer des dons, présents ou avantages quelconques afin qu'elle commette un assassinat ou un empoisonnement* ». Transposé dans *l'espace cyber*, le fait par exemple de commettre des abus sexuels contre des enfants par le canal des sites numériques constitue un *cybercrime*. C'est le cas par exemple de la diffusion d'images pédopornographiques.

Pour une ébauche de réponse, Mohamed CHAWKI a précisé dans sa thèse[140], soutenue en 2009, une typologie de la cybercriminalité en comparant les éléments propres à la France à ceux des Etats-Unis. Les résultats de ses recherches ont permis de classifier les actes cybercriminels selon des critères différents en fonction de l'Etat considéré.

En France, le code pénal classe les infractions selon la gravité (entre crimes et délits) alors qu'aux Etats-Unis, des catégories d'actes sont créées et diffèrent d'un Etat à l'autre.

Ainsi, le code pénal californien, (section 502) définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Ce code considère le fait d'accéder ou de permettre intentionnellement l'accès à tout système ou réseau informatique afin a) de concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ; b) d'acquérir de l'argent, des biens ou des services, dans le but de frauder ; c) d'altérer, de détruire ou d'endommager tout système, réseau, programme ou données informatiques.

Quant au Code pénal du Texas (section 33.02), il va plus loin : il considère comme cybercriminalité le fait d'accéder à un ordinateur, à un réseau, ou à un système informatique sans avoir l'autorisation de son utilisateur.

Toutes ces précisions sont importantes pour la détermination de la sanction attachée au degré de gravité de l'acte commis. Il s'agit de faire correspondre

[140] Cf. **CHAWKI M**., Combattre la cybercriminalité, édition de Saint Amans, Perpignan 2009.

l'incrimination à la peine qui s'attache à l'infraction décrite. En s'appuyant sur la définition d'origine de la règle de droit pénal, c'est en fonction de la gravité de l'acte, qu'est déterminée la sanction.
Et l'article L111-1 du code pénal dispose à cet effet que *« Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement. Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention»*.

Face à ce phénomène, les gouvernements en place ainsi que les divers législateurs n'entendent pas rester inactifs d'où la question de la répression de la cybercriminalité, objet de notre travail. Cette prise de conscience du danger des usages abusifs et des détournements d'internet et des réseaux numériques s'est accentuée avec les attentats, du 11 septembre 2001[141] aux Etats-Unis d'Amérique. Ce douloureux événement a été l'occasion pour les Etats du monde de se rendre compte de la sollicitation accrue des réseaux numériques et des canaux afférents par les criminels. Les technologies de l'information ont été lors de cette attaque meurtrière un moyen pour les terroristes de commettre leurs actes. C'est pourquoi, à l'heure actuelle, tous les réseaux mafieux de terrorisme, d'antisémitisme, de crimes contre l'humanité via les réseaux numériques, de crimes pédopornographiques, de trafic d'armes, de drogues et de blanchiment d'argent intègrent la sphère de la lutte contre la cybercriminalité[142].

Sanctionner les cybercriminels est de ce fait, au cœur des politiques des Etats de l'Union Européenne mais également de ceux de l'Afrique de l'Ouest. Dès lors que comprend la répression de la cybercriminalité. Sanctionner est-il synonyme de punir ? Que la sanction soit négative ou positive, que signifier sanctionner ?

---

[141] Cf. **WEYEMBERGH Anne**, Juris-classeur Europe Traité, Fascicule 2700 coopération judiciaire pénale, 1er mai 2009.

[142] Notamment avec la décision-cadre du 13 juin 2002 relative à la lutte contre le terrorisme, négociée et adoptée dans les mois qui ont suivi les attaques terroristes du 11 septembre 2001 *(Cons. UE, déc.-cadre n° 2002/475/JAI, 11 sept. 2001 : Journal Officiel des communautés européennes 22 Juin 2002 s.).*

Lors d'un colloque en 2003 organisé par l'Association des doctorants et des jeunes docteurs de l'université Jean Moulin de Lyon, Nathalie MALLET-BRICOURT et ses collaborateurs ont tenté de définir la sanction pénale[143]. Les différentes approches de la sanction pénale pourraient constituer un support à la réponse de la répression des intrusions informatiques, des atteintes aux systèmes informatiques ou encore du vol des données personnelles et de leur utilisation frauduleuse. Dans cette optique, l'élaboration d'une recherche quant à la répression de la cybercriminalité dans ces Etats sera particulièrement formatrice. En effet, il s'agira de comparer les deux systèmes de sanction au niveau de leurs règles et de la pratique qui s'ensuit.

L'analyse des échecs ou des succès de la répression de la cybercriminalité au sein de l'Union Européenne peut-elle servir de correctifs dans l'élaboration de la sanction du phénomène en Afrique de l'Ouest ? L'inverse est-il aussi possible ?

L'interrogation est intéressante à plus d'un titre dans la mesure où premièrement, ce sujet est d'actualité surtout avec la mise en place effective de règlementations dans les pays dits jeunes comme ceux d'Afrique. Il nous sera ainsi permis à travers cette approche de la cybercriminalité d'observer comment se fait la sanction de ces infractions en Europe et l'adaptation des règles européennes- si elle est faite- aux pays africains.

Deuxièmement, se cache un intérêt éducatif derrière cette recherche. S'informer sur les dangers que recouvre internet favorise l'apprentissage des rouages c'est-à-dire des techniques et attitudes à adopter pour se protéger des attaques potentielles.

Troisièmement, il est fréquent de constater que la cybercriminalité nuit à la stabilité politique mais surtout à l'équilibre économique. L'ampleur du phénomène est source de méfiance de la part des investisseurs à l'égard des systèmes informatiques des pays en cause.
Or, la santé des systèmes informatiques est un facteur qui, de nos jours, influence particulièrement les considérations économiques vues de l'extérieur.

---

[143]Cf. **MALLET-BRICOURT N.**, La sanction, colloque du 27 novembre 2003.

Quatrièmement, cette étude s'oriente également dans la recherche d'un meilleur moyen de régulation des réseaux numériques ; ce qui nous conduit ainsi à analyser les mesures actuelles prises pour garantir et assurer une bonne gouvernance de ces réseaux. Il faut mentionner à ce stade que les enquêtes de terrain ont été déterminantes dans la mesure où elles ont considérablement modifié l'idée théorique de départ sur la procédure coercitive aussi bien au sein de l'Union Européenne qu'en Afrique de l'Ouest.

L'approche préliminaire aurait conduit à considérer qu'il n'y a aucune répression de la cybercriminalité en Afrique de l'ouest, à la différence de l'Europe où les sanctions sont sans cesse renouvelées et adaptées.

En second lieu, le fait de présenter les coercitions de l'Europe peut se justifier par l'avance qu'a prise ce continent quant aux risques et abus générés par l'utilisation des technologies de l'information et de la communication. Par opposition de cette avance, l'équipement numérique se met en place en Afrique de l'Ouest. C'est pourquoi, elle est abordée dans une seconde acception : les réseaux numériques et téléphoniques (en ce qui concerne leur implantation et évolution) sont dérivés (pour la plupart) de ceux qui existaient déjà sur les continents américain et européen.

Le projet de cerner l'ensemble de la répression de la cybercriminalité dans les Etats membres de l'Union Européenne et ceux de l'Afrique de l'Ouest peut paraître vaste quant à l'espace géographique concerné. Le choix de la délimitation géographique est volontaire.

Pour qui est originaire de la Côte-d'Ivoire, les dérives de l'utilisation d'Internet ne peuvent laisser indifférent. La Côte-d'Ivoire a souffert d'une longue crise politique (entre 1998 et 2010) qui s'est soldée par des affrontements militaires avec des conséquences sociales mais également des retombées économiques désastreuses. Dans ce pays, c'est-à-dire en Côte-d'Ivoire et en Afrique de l'Ouest, le développement de l'information apparaît comme un vecteur de développement, malgré toutes les difficultés qu'il doit affronter et corriger comme l'Union Européenne a dû le faire depuis plus longtemps.

Au moment des recherches sur le sujet qui nous occupe, les crimes relatifs aux réseaux numériques et plus largement les technologies de l'information et de la communication commencent à prendre des dimensions plus importantes alors même

qu'aucune législation appropriée n'est mise en place. Les carences législatives et règlementaires, lorsque la législation existe, sont l'occasion pour les chercheurs de confronter la situation en Afrique de l'Ouest avec celles plus avancées des Etats de l'Union Européenne.

Afin de donner une dimension adaptée à ce travail comparatif, la recherche s'articulera autour de la mise en place de la politique de lutte (Première partie) et de la répression effective de la cybercriminalité (Deuxième partie) dans l'Union Européenne et en Afrique de l'Ouest.

PREMIERE PARTIE :

LA MISE EN PLACE DE LA POLITIQUE DE LUTTE CONTRE LA CYBERCRIMINALITE

En Europe tout comme en Afrique, les législations s'emploient à édicter des textes qui évoluent au fur et à mesure des innovations technologiques. C'est aussi l'occasion de s'interroger sur les conditions d'accès des Etats africains à l'innovation technologique et sur leurs retards. Dans une société sans cesse modernisée et en perpétuel mouvement, les Etats européens, et les autres Etats comme ceux des autres continents n'ont pas d'autres alternatives que d'échanger leurs solutions du fait des problèmes communs dont les questions relatives à l'interopérabilité des réseaux affectés.

L'interopérabilité, au sens de la décision 2004/387/CE du Parlement européen et du Conseil en date du 21 avril 2004[144], est la capacité qu'ont les systèmes, les technologies de l'information et de la communication (TIC), ainsi que les processus de fonctionnement qu'ils permettent, à échanger des données et de permettre le partage des informations et des connaissances. L'interopérabilité contribue pour une part importante à l'utilisation interchangeable d'une même technologie entre concurrents sur le marché de la communication. Les logiciels peuvent servir d'éclairage sur ce point : en effet, un même logiciel peut être utilisé différemment (c'est-à-dire proposer des services variés) par des sociétés concurrentes sur le marché des technologies. Il est aussi interchangeable à l'intérieur d'un réseau précis. La question de l'interopérabilité est connexe aux problèmes liés à la cybercriminalité et permet surtout de prendre du recul et de mesurer l'ampleur des conflits susceptibles de naître. Ces conflits doivent être résolus et ce, dans le contexte de partage, tout en tenant compte de l'absence de limite géographique qu'implique l'espace virtuel créé par internet et les autres médias qui s'en servent.

La prise en compte de ces dimensions virtuelles, sans limite, est la justification du recours à la notion de mondialisation. Cette notion pourrait constituer une piste de réflexion dans la recherche d'issues pour mettre fin à la cybercriminalité.

---

[144] Décision 2004/387/CE du Parlement européen et du Conseil du 21 avril 2004 relative à la fourniture interopérable de services paneuropéens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens (IDABC) rectifiée par décision 2004/387/CE du parlement européen et du conseil du 21 avril 2004 relative à la fourniture interopérable de services paneuropéens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens, JOUE L 185/25 du 18.05.2004. La définition figure au point f de l'article 3 de la décision.

La mondialisation est généralement comprise comme un élargissement spatial et une intensification des interactions économiques et culturelles régionales ou globales[145]. D'un point de vue économique, Théodore Levitt, en 1983, considère que *« Les firmes doivent apprendre à travailler comme si le monde était un grand marché unique* »[146]. C'est seulement dans les années 80 que le terme même de la mondialisation est popularisé par Ohmae, un consultant japonais chez McKinsey[147].

Seize ans plus tard, en 1999, dans son rapport d'information sur la mondialisation[148], le député Robert Blum définit la mondialisation par les formes qu'elle épouse. Selon ce rapport, il s'agit premièrement des transactions commerciales (le commerce mondial des marchandises), deuxièmement de la forme industrielle par l'intermédiaire des flux des investissements directs à l'étranger et enfin troisièmement de la forme de la globalisation financière. La mondialisation a pour conséquence l'association de tous les Etats du monde au développement des économies pour ne laisser aucun des pays (quel que soit leur statut de pays développés, industrialisés ou en voie de développement) en marge de la recherche de solutions aux problèmes mondiaux. C'est dans ce cadre de la mondialisation que s'inscrit la lutte contre la cybercriminalité, phénomène transfrontalier.

---

[145] Cf. **GOLDBLATT D**., **HELD D**., **MCGREW A**., **PERRATON J.,** "Economic Globalization and the Nation-State Shifting Balances of Power", *Alternatives*, Vol 2, No. 269-285,1997 ; voir également **MOREAU DEFARGES P.** qui précise dans son que sais-je, la mondialisation, page 21 que « du XVIe au XXe siècle, la mondialisation c'est-à-dire l'inscription de toutes les sociétés dans une histoire unique, est indissociable de la constitution des empires coloniaux.

[146] Cf. **LEVITT Théodore**, The Globalization of Markets, Harvard Business Review, Harvard, mai - juin 1983. Et en complément voir **DAGORN R**., une brève histoire du mot mondialisation, GEMDEV, Mondialisation. Les mots et les choses, Paris, Karthala, 1999, p.187-204.

[147] Cf. **OHMAE K.,** La triade, émergence d'une stratégie mondiale de la puissance traduit de l'anglais au français par Chantal Pommier, titre d'origine « *Triad power : the coming shape of global competition*, édition Flammarion, Paris, 1985 ; et voir également **BAUDRAND V.** et **MARIE HENRY Gérard**, La mondialisation, collection studyrama, 2006, Paris, p. 13.

[148] Rapport d'information sur la mondialisation, Assemblée nationale, rapport déposé par la Commission des affaires étrangères et présenté par M. **BLUM Roland**, sous la 11e législature, Paris : Assemblée nationale, 1999, collection Les documents d'information / Assemblée nationale, Commission des affaires étrangères, ISSN 1240-831X, p.83-99. Le rapport a été publié le 24 novembre 1999.

Dans cette mesure, les deux continents, africain et européen, entretiennent des relations de collaboration et de coordination. Ce qui nous conduit à étudier comparativement l'élaboration de la politique répressive en Europe et dans les Etats ouest-africains. C'est dans ce cadre que la cybercriminalité prend une dimension importante à travers l'élaboration de sa répression au sein de l'Union européenne (Chapitre 1). La même interrogation apparaît tardivement dans les Etats de l'Afrique de l'Ouest (chapitre 2).

Voir également en complément de ce rapport l'article de **FLIGSTEIN N.**, « *Rhétorique et réalités de la mondialisation* », article de la recherche en sciences sociales, 1997, volume 119 p36-47, qui reprend les formes de la mondialisation, précisée dans le rapport précité.

CHAPITRE 1 :

L'ELABORATION DE LA REPRESSION DE LA CYBERCRIMINALITE EN EUROPE

Dans toute société organisée, la nécessité de définir ou de concevoir des lois est toujours motivée par des comportements humains. Les lois relatives au domaine de la cybercriminalité n'échappent pas à cette vérité. En effet, c'est en raison de l'usage nuisible que des individus font des technologies de l'information et de la communication que les Etats sont amenés à légiférer. En un mot, c'est la cybercriminalité qui aboutit à la mise en place d'une politique de répression. Celle-ci apparaît légitime dès lors qu'il s'agit de protéger divers intérêts[149].

La cybercriminalité ne revêt pas les mêmes formes dans l'espace européen et en Afrique de l'Ouest. Cette différence de situation appelle naturellement des solutions spécifiques. En dépit de ces particularismes, le crime lié au cyberespace reste un phénomène essentiellement transfrontalier, d'où l'importance pour l'Europe et pour l'Afrique de l'Ouest de coopérer sur un plan stratégique, légal, militaire et financier. Il est important de souligner que, en matière de réaction répressive face au délit cybercriminel, les Etats-Unis sont considérés comme les précurseurs[150].

---

[149] Intérêts des individus, des sociétés ou entreprises, des administrations publiques ou privées, des Etats et des organisations internationales.

[150] Le premier Etat à légiférer sur les infractions informatiques est l'Etat de Floride en 1978 avec la loi sur les fraudes et les intrusions informatiques cf. The Florida Computer Crimes Act. La lutte contre la cybercriminalité aux Etats Unis commence avec l'affaire du « *Flagler Dog Track* » selon l'expression « CIA » pour Confidentiality Integrity and Availability en 1990 : les anarchies créées par les protestataires de la mise en place de l'accord Nord-Américain coïncident avec le lancement technologiques de l'internet. On aboutit à une désobéissance civile électronique marquée par les techniques de blocage et d'intrusion contre laquelle l'Etat américain va lutter, à compter de cette date. cf. *The Electronic civil disobedience and Other Unpopular* Ideas, Brooklyn, NY : Autonomedia, 1996, p. 18 (traduction française : *La résistance électronique et autres idées impopulaires*, Paris, L'Éclat, 1997. Dès 1993, chaque Etat sauf le Vermont aux Etats-Unis possède un statut punissant les délits informatiques. De plus, la loi du 13 septembre 1994 incrimine déjà la diffusion des virus informatiques. cf. *Counterfeit Access Device and Computer Fraud dans Abuse Act 1984, Computer Fraud and Abuse Act (CFAA) 1986 et les lois du 13 septembre 1994.* Cf. également **CASEY Eoghan**, Digital evidence and computer crime, 2nd edition, Elsevier Academy press, 204, p24.

L'analyse de la législation et l'étude des organismes chargés de sa mise en œuvre imposent la connaissance des sources de la cybercriminalité (section 1). Il nous faut analyser les moyens facilitant la commission de ces actes. Pourquoi un comportement d'un internaute est-il constitutif d'infraction, et pas un autre ? Cette perception des sources de la cybercriminalité permet de mettre l'accent sur la protection notamment des données personnelles figurant sur la toile. Quel est le niveau de cette protection ? En quoi la conservation de ces données par les sites d'hébergement des administrations concernées (caisse d'assurance maladie, caisse d'allocations familiales, administrations fiscales et services bancaires ou autres) pourrait faciliter un vol d'identité par exemple ou pourrait l'empêcher ? Quelles sont les garanties offertes par la loi française, par la règlementation européenne ?

Les technologies évoluent continuellement. Par conséquent, les législations doivent être adaptées et suivre cette évolution. Est-ce le cas, quelles que soient les circonstances des actes commis ? C'est à la lumière des instruments juridiques mis en place au sein de l'Union Européenne qu'il faudra apprécier la stratégie coercitive de la grande criminalité informatique (section 2).

Section1 : Les sources de la cybercriminalité

Les sources renvoient non seulement aux terreaux mais aussi aux causes de la commission d'actes cybercriminels. La cybercriminalité est née à la suite de l'utilisation des outils informatiques ainsi que du réseau internet. Or, ces infrastructures sont en perpétuelle évolution, ce qui implique des mutations et des innovations.

Les délinquants qui ont fait de ces systèmes leur lieu, outil et objet de commission d'infractions s'adaptent à ces innovations et sont parfois même en avance sur les techniques inventées en vue de parer à leurs attaques.

La rapidité des adaptations des cybercriminels est inquiétante et exige de comprendre les justifications et les fondements de ces comportements afin de pouvoir y pallier.

A travers les sources, il s'agit de répertorier, les facteurs qui favorisent le développement de la cybercriminalité. Ce sont ces indicateurs qui permettent de mieux cerner les problématiques de répression.

En effet, pour résoudre convenablement un problème, il faut d'abord le comprendre. Or comprendre la cybercriminalité, et surtout maîtriser son évolution, pour parvenir à la stopper, revient à explorer ses fondements afin de se prémunir contre les actes répréhensibles.

La cybercriminalité est certes le fait de personnes qui portent atteinte à des règlementations. Mais, elle est aussi et surtout rendue possible parce que des individus laissent des traces à ces criminels pour commettre leurs exactions ; ces traces peuvent être laissées consciemment ou inconsciemment. Et, la modification des habitudes de consommation est déterminante dans la commission de la cybercriminalité (§1).

Si la consommation permet à la cybercriminalité d'évoluer, il faut mentionner que cette criminalité particulière progresse en passant par diverses formes. C'est en partant des diverses utilisations du cyberespace elles-mêmes que l'on voit apparaître une évolution de la cybercriminalité. Cette évolution s'adapte au modus operandi.

C'est dans les diverses utilisations évolutives du cyberespace que naît et se développe la cybercriminalité. Il faut donc voir les transformations de l'usage que l'on peut faire de la haute technologie pour constater la progression de la cybercriminalité. (§2).

§1 -Les habitudes de consommation, ferments de la cybercriminalité

Avec l'arrivée des technologies de l'information (comme la numérisation par exemple) en plus d'internet et des autres médias à savoir la télévision, la radiotéléphonie, les habitudes de consommation sont modifiées (A). Qu'il s'agisse d'étudiants, de professionnels quelle que soit la branche d'activité, le réflexe est celui de travailler systématiquement par le biais de l'internet ou des moyens numérisés. Par exemple, enregistrer une nouvelle adresse ne se fait plus uniquement en se déplaçant au bureau de poste mais se fait via le site internet de la poste, ou encore par l'intermédiaire d'une interface de connexion où les usagers ont la possibilité d'enregistrer leurs données (noms,

prénoms, ancienne adresse, nouvelle adresse géographique et même numéro de téléphone) contre paiement en ligne de la somme liée à cette prestation. S'agissant des étudiants, les recherches sur différents sujets abordés ne se fait pas en bibliothèque dans des livres en amont. C'est internet et les réseaux afférents qui sont les premiers consultés. Ce n'est que par la suite que les recherches sont corroborées par des écrits dans les livres. Or c'est l'attitude inverse qui devrait être privilégiée. Il en résulte un recours continuel aux réseaux numériques dont les plus sollicités sont les réseaux sociaux, nouveaux cadres de vie des populations quelle que soit la couche sociale considérée (B).

A- Le changement des habitudes

Les habitudes se sont transformées avec l'usage des réseaux électroniques. Sont ainsi concernés aussi bien les achats et le commerce (a) que l'expression de la démocratie par internet plus spécialement la procédure du vote électronique (b).

a- Les changements des habitudes d'achat et de e-commerce

La dématérialisation de l'ensemble des systèmes de paiement, le recours à la monétique c'est-à-dire *l'ensemble des activités liées au paiement numériques et particulièrement au paiement par carte*[151] et les nouvelles habitudes d'achat sans déplacement favorisent la cybercriminalité. En effet, de plus en plus, les consommateurs d'aujourd'hui ont recours aux services en ligne même pour faire leurs courses quotidiennes et ils ne sont pas les seuls puisque les entreprises et l'administration publique font de même. On parle de commerce électronique.

L'Organisation Mondiale du Commerce (OMC) définit dans une acception très large, le commerce électronique comme l'ensemble des activités de production, de publicité, de vente et de distribution de produits effectuées par l'intermédiaire des réseaux de télécommunication[152]. Cette conception trop large ne fait pas intervenir les acteurs[153].

---

[151] Cf. **HALLEPEE D**., l'univers de la monétique : histoire, fonctionnement et perspectives, collection Faits de société, 2009.

[152] Cf. **OMC**, Le commerce électronique et le rôle de l'OMC rédigé par **BACCCHETTA Marc**, **LOW Patrick**, **MATOO Aaditya** et a., Genève OMC, 1998; PCA international: Strengthening relations with Arab and Islamic countries through international law: e-commerce, the WTO dispute settlement mechanism

C'est pourquoi, il convient de la compléter par la conception de l'Organisation pour la Coopération et le Développement Economique (OCDE).

Dans une acception nuancée, l'OCDE considère le commerce électronique comme « la vente ou l'achat de biens ou de services, effectués par une entreprise, un particulier, une administration ou toute autre entité publique ou privée, et réalisés au moyen d'un réseau électronique »[154].

Quant à la loi française sur la confiance en l'économie numérique du 21 juin 2004, dite Loi LCEN[155], elle considère, en son article 14 que le commerce électronique est *l'activité économique par laquelle une personne propose ou assure à distance la fourniture de biens ou de services* ». En s'appuyant sur ces deux définitions, il est possible de dire que le commerce électronique est une forme de vente ou d'achat qui emprunte les réseaux numériques et qui concerne aussi bien les entreprises que les particuliers. Ainsi, à côté de l'échange électronique entre entreprises, souvent appelé **B2B** (acronyme anglais de *Business to Business*), il y a le commerce électronique à destination des particuliers, ou **B2C** (pour *Business to Consumer)*. Il s'agit de sites web marchands, du type télé-achat. Pour illustration, la technique des courses à distance, comme *Auchan Drive*, en France, permet à partir d'un certain montant d'effectuer ses courses via le site de l'enseigne commerciale. L'acheteur ne se déplace plus, il utilise le site internet pour ses opérations et en paie le montant via l'interface numérique de l'hypermarché choisi. Pour un exemple plus international, le prestataire eBay propose toutes sortes de ventes de biens sur sa plateforme numérique.

---

and foreign investment: paper emanating from the PCA international law seminar, October 12, 2001, collection of the permanent court of arbitration, Peace Palace paper, The Hague: Klumer, 2002.

[153] Comme le souligne à juste titre **BRASIER Audrey** dans son mémoire de DESS intitulé *le commerce électronique* : *une opportunité pour l'Afrique*, mémoire soutenue en 2003 à l'Université Panthéon-Sorbonne à Paris.

[154] Documents de travail de l'OCDE, Conférence interministérielle de l'OCDE : un monde sans frontière concrétiser le potentiel du commerce électronique 1998, Ottawa 7-9 octobre 1998, Direction de la Science de Technologie et de l'industrie, Comité de Paris, OCDE, 1998.

[155] Loi n° 2004-575 du 21 juin 2004 publiée au JORF n° 0143 du 22 Juin 2004, texte n°2.

Dans la même acception, le commerce électronique peut intervenir uniquement entre les particuliers et là on parle de **C2C** (c'est-à-dire *Consumer to Consumer*). Dans ce cadre, les sites web favorisent la vente entre particuliers (immobilier, bourses, annonces, échanges...). Par exemple en France, le site: de particulier à particulier (*PAP*) permet aux personnes privées de mettre des annonces de vente ou d'achat de leurs biens immobiliers. Enfin, l'échange électronique existe dans les relations entre les entreprises privées et le gouvernement, et là il est question de souvent B2G (*Business to Government*) ou **B2A** (*Business to Administration*). L'illustration est celle des sociétés éditrices qui proposent des logiciels pour les systèmes d'information aux ministères.

En plus de consommer en ligne, les usagers, recourent régulièrement aux réseaux en ligne ; ces derniers sont de plus en plus sollicités même pour des conversations. Or, toutes ces nouvelles manières de consommer qu'on peut dénommer *l'e-consommation* empruntent les réseaux numériques et laissent des données (ou des traces) sur ces réseaux. Ces données sont, de la sorte, susceptibles d'être interceptées d'autant plus que la sécurité n'y est pas forcément assurée. D'ailleurs, les consommateurs qui achètent par le biais des sites internet sont souvent victimes d'arnaques soit de la part des vendeurs directement, soit de la part de pirates, qui détournent les données bancaires pouvant être stockées du fait des transactions effectuées. C'est dire que le risque est bel et bien existant. Bien que des systèmes sécurisés de paiement sont établis notamment au regard des exigences de systèmes bancaires, les risques de fraude et de contournement par les cybercriminels existent.

Au titre des mutations liées à internet, l'expression de la démocratie emprunte la voie du vote électronique.

b- La tentation du vote électronique

Le vote électronique est aujourd'hui une nouvelle habitude dans les Etats.

Le vote électronique est une procédure qui soulève des questions de sécurité suffisante. Le cas des élections à la présidence de à l'Union pour un Mouvement Populaire (UMP), en France, du vendredi 28 novembre au samedi 29 novembre 2014 permet de remettre en cause la sécurisation des réseaux numériques. Il existe ainsi les possibilités de changer les résultats de ces votes électroniques notamment par falsification des résultats d'un vote par un candidat adversaire. Les résultats de ces élections sont « *émaillés de bugs* »[156].

Le bug a été explicité de manière éloquente par les journalistes dans les lignes qui suivent : « *Vous ne remarquez rien ? L'un de nos éditeurs – pointilleux – a eu la bonne idée de recompter. Et là, c'est carrément bizarre. On commence par additionner les voix qui se sont portées vers les candidats. Le total donne bien 155 285, le nombre de suffrages exprimés. Jusque-là, tout va bien. Mais la Haute autorité mentionne aussi 434 bulletins blancs. Il était en effet possible de cocher une case « vote blanc » au lieu de soutenir l'un des candidats. En additionnant, les suffrages exprimés (155 285) et les bulletins blancs (434), on trouve 155 719. Soit une différence de 132 voix avec le nombre affiché de votants (155 851).* »

Les résultats peuvent être liés à de simples bugs techniques mais ils soulignent la fragilité du système ; c'est une voix laissée aux cybercriminels ou hackers capables de facilement entrer dans les bases de données de ces votes et changer le contenu. Dès lors, il serait souhaitable de ne pas encourager ce type de vote notamment au plan national. Même si en ce qui concerne l'UMP ce bug n'a pas eu un impact très élargi mais compte tenu de l'absence de garantie, de fiabilité totale, ce vote électronique reste à parfaire.

---

[156] **R. NOYON et T. NOISETTE**, Vote électronique, oups il manque des voix dans le décompte de l'UMP, Rue89 du 02 décembre 2014, voir en ligne : rue89.nouvelobs.com/2014/12/blague-manque-voix-decompte-resultats-lump-256351.

A l'origine, Internet est mis en place pour servir les intérêts de défense nationale et militaire puis pour des recherches universitaires. Il revêtait dès lors, un caractère non commercial[157]. Cet objectif de base change lorsqu'Internet est commercialisé et est sorti de son cadre universitaire et de recherches. Partant, les influences d'internet dans les habitudes de consommation sont les signes de mutations d'internet. Il est passé de moyen occulte à un instrument public et que les usagers entendent exploiter à toutes fins dont le recours systématiques aux réseaux sociaux d'échange.

Dans le meilleur des cas, les mutations peuvent être bonnes. Mais elles peuvent à l'inverse être mauvaises dans le pire des cas. Ce qui conduit à voir de plus près l'usage des réseaux électroniques et des réseaux sociaux qui sont des formes d'échanges particulièrement proches de l'usager.

B- L'usage des réseaux électroniques et des réseaux sociaux

L'usage des réseaux électroniques et sociaux peut déboucher sur la commission d'actes relevant de la cybercriminalité (a). C'est ainsi que les législateurs sont amenés à encadrer ces nouveaux espaces d'expression des internautes (b).

a- La définition et les caractéristiques des réseaux sociaux

Dès 1969, James Clyde Mitchell définit les réseaux sociaux comme « un ensemble spécifique de relations entre un nombre défini de personnes, avec la propriété supplémentaire, que ces liens dans leur ensemble peuvent être utilisés pour interpréter le comportement social des personnes impliquées »[158]. Les réseaux sociaux sont des pages privées créées par les personnes physiques comme morales en vue de partager des événements, des photos, bref, en vue d'échanges d'information. Dans un avis référencé 5/2009 du 12 juin 2009, le « G 29 », Groupe de travail de l'article 29 constitué de représentants des CNIL européennes a défini les réseaux sociaux comme des plateformes

[157]Cf. **ASINARI M. V. Pérez**, International aspects of personal data protection quo vadis eu ?, in défis du droit de la protection de la vie privée, éditions Bruylant, 2008, p386.

[158]Cf. **MITCHELL Clyde J.**, "Social Network in Urban Situations", Manchester, Manchester University Press.1969 et voir aussi Guillaume Chanson « Les réseaux sociaux, un objet d'étude ancien », *Vie & sciences de l'entreprise* 2/2011 (N° 188), p. 8-9.

de communication en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des opinions similaires et des intérêts communs ».

Le problème est que les adhérents ne font plus la différence entre ce qui relève de l'ordre privé et ce qui peut être partagé. Les réseaux sociaux sont une variante de l'informatique communicante. Cette forme de communication ayant commencé avec la consommation en ligne et les échanges commerciaux.

Mark Zuckerberg[159] est à l'origine du premier réseau social FACEBOOK. Il est mis en place depuis 1998 mais des conflits financiers retardent sa diffusion au public. Si bien que d'autres réseaux du même type sont proposés au public. C'est notamment le cas de MySpace, qui trouve d'abord une attention particulière auprès des artistes, qui s'en servent pour leurs promotions d'albums, de disques par exemple. Ensuite, ce sont les jeunes publics entre 20 et 30 ans qui s'y intéressent qu'ils soient artistes ou pas. Par la suite, plusieurs autres réseaux apparaissent et épousent diverses options : tandis que certains ne servent que des intérêts divertissants, d'autres sont à visée professionnelle. Facebook, Twitter, Linkedln, Viadeo, MySpace, Copainsdavant sont des exemples. Ces réseaux présentent certes des avantages mais également des inconvénients.

Pour les aspects positifs, les réseaux sociaux relayent les informations et facilitent des échanges.

Sur le plan international, par exemple c'est par le biais des réseaux sociaux que les familles libyennes, tunisiennes installées en Europe parviennent à obtenir des nouvelles de leurs proches au cours de la période dite du printemps arabe en Libye et en Tunisie. C'est aussi grâce à ces canaux que les journalistes, mêmes de presses internationales arrivent à diffuser des informations en temps réel. Ces exemples sont

---

[159] Cf. **MEZRICH Ben**, La revanche d'un solitaire: la véritable histoire du fondateur de Facebook traduit de l'anglais (États-Unis) par **DELPLANQUE Lucie** (titre d'origine The accidental billionnaires), collection Essais-documents. Paris, 2009 : ZUCKERBERG est d'origine allemande, a étudié à l'Université d'Harvard, et se met, dès 2004, avec d'autres étudiants à concevoir le réseau social qui devient en 2009 une plateforme d'échanges : FACEBOOK. Le succès de Facebook et des autres réseaux sociaux a d'ailleurs été relayé dans un film titré « the Social Network », primé en 2011 de la distinction du César du meilleur film étranger. Il a été réalisé par **David FINCHER**. Ben Mezrich, auteur adapté ; Aaron Sorkin, scénario ; Trent Reznor & Atticus Ross, Jesse Eisenberg, Andrew Garfield, Justin Timberlake, Sony pictures home entertainment DL 2011.

notables dans une autre partie du continent africain, en Côte-d'Ivoire notamment. En Afrique de l'Ouest, les médiaux sociaux permettent aux Français d'origine ivoirienne ou même à des personnes ayant des attaches ailleurs de transférer des fonds ou des recharges téléphoniques[160] à leurs familles restées en Côte d'ivoire au moment des troubles post-électorales qui paralysent la vie économique et sociale dans cet Etat.

Pour des aspects négatifs, les réseaux sociaux sont surtout liés à l'absence de contrôle de la part des utilisateurs. Il faut mesurer ici l'importance de ces nouveaux moyens de communication. L'usage démesuré des réseaux de la part des internautes conduit au stockage d'informations qui transitent par leurs bases de données. Ce sont d'importantes mines d'informations. De la sorte, toutes les photos par le biais de *Flickr* ou *Picasa*, le partage de vidéos sur des sites tels Youtube, Dailymotion, qu'elles soient personnelles ou professionnelles se retrouvent sur la toile publique. C'est en cela que les personnes expérimentées pourraient y avoir recours à des moments insoupçonnés.

En témoigne un site internet créé par des américains *USENET* qu'on pourrait qualifier de « fou du net ». Leur projet a pour objectif d'archiver tout ce qui est mis sur internet ; les réseaux sociaux ne sont pas en reste. Cette manière de procéder soulève des questions d'irréversibilité c'est-à-dire l'impossibilité de faire un demi-tour pour des traces indésirables ou des photos ou encore des commentaires dont les internautes seraient peu fiers. La question est de savoir s'il est possible ou non par exemple de supprimer des données injectées sur la toile dans la mesure où les personnes à l'origine de cette diffusion de base (ceux qui les ont mis sur internet) n'en désirent plus la communication publique pour des raisons diverses.

Cette dernière considération quant aux réseaux sociaux soulève la question de l'oubli sur internet : est-ce que les réseaux sociaux (par leurs bases de données, archives) oublient réellement quand nous effaçons ce que nous avions partagé à une date antérieure

[160] Les recharges téléphoniques sont des systèmes permettant de créditer le compte de l'utilisateur d'un téléphone grâce à son numéro et ce, par le biais d'interfaces numériques.

précise ? Aucune donnée supprimée d'un réseau social n'est réellement effacée. Elle est tout simplement archivée dans des bases de conservations des données du site concerné. Cette assertion tient pour preuve l'aisance du réseau à retrouver une personne anciennement membre du réseau concerné, dès l'instant où cette personne requiert une réactivation de sa page qu'elle avait souhaitée supprimer des mois auparavant. Il lui est possible de retrouver l'ensemble des données censées être effacées.

b- L'encadrement légal des réseaux sociaux

Cette remarque renvoie au temps de conservation des données au sein des bases d'archivages des sites internet en général et des réseaux sociaux en particulier. Pendant combien de temps des données sont-elles conservées en archives dans les bases de données des entreprises ?

La conservation des données en droit européen est réglée grâce à la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications[161], et modifiant la directive 2002/58/CE. En son article 6, la directive prescrit une durée minimale de conservation des données de six mois et maximale de deux ans à compter de la communication. Il faut préciser que toutes les données n'ont pas vocation à être conservées. En effet, les contenus ne sont pas visés et l'article 5 de la même directive liste les données susceptibles de faire partie du champ d'application. Il s'agit essentiellement « *des données nécessaires pour retrouver et identifier la source d'une communication (c'est-à-dire le numéro de téléphone de l'appelant, les noms et adresses de l'abonné inscrit) , les données nécessaires pour déterminer la date, l'heure et la durée d'une communication (la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet), les données nécessaires pour déterminer le type de communication(cellulaire, téléphone fixe ou mobile), les données nécessaires pour*

[161] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques

identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel (à savoir le numéro de téléphone de l'appelant et le numéro appelé, qu'il s'agisse d'une téléphone fixe ou mobile), les données nécessaires pour localiser le matériel de communication mobile(…) ».

Ces dispositions de la directive permettent de souligner la précision des informations susceptibles d'être conservées. Elles ne sont certes pas relatives au contenu mais sont d'une extrême importance puisqu'elles permettent de géo-localiser les personnes concernées et de retracer leurs gestes en se servant uniquement de leurs communications téléphoniques. Le contenu ne semble pas ici nécessaire ou plutôt le fait de ne pas conserver le contenu des communications téléphoniques ou électroniques participe, dans une certaine mesure, du respect d'un droit fondamental qu'est celui de la liberté de communication.

Cependant, la directive est invalidée par l'arrêt de la Cour de Justice de l'Union Européenne du 8 avril 2014[162] rendue à la suite des révélations de Snowden sur l'affaire PRISM. Dans quel cadre la Cour de Justice a-t-elle pris cette décision ?

Les faits à l'origine de l'arrêt rendu par la CJUE le 8 avril sont relatifs à deux affaires[163] : la première concerne la Digital Rights Ireland Ltd qui demande d'annuler la septième partie de la loi de 2005 sur la justice pénale (infractions terroristes) Criminal Justice (Terrorist Offences) Act 2005 dans une affaire l'opposant au Minister for Communications, Marine and Natural Resources, au Minister for Justice, Equality and Law Reform, au Commissioner of the Garda Síochána, à l'Irlande ainsi qu'à l'Attorney General ; et la seconde affaire est celle de plusieurs recours dirigés contre de l'article 102

---

accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE publiée au Journal officiel n° L 105 du 13/04/2006 p. 0054 - 0063

[162] Cf. CJUE, 8 avril 2014, n° C-293/12, aff. Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et a.

[163] Elles sont répertoriées respectivement sous les numéros C-293/12 pour la première et C-594/12 pour la seconde.

bis de la loi de 2003 sur les télécommunications[164], ladite loi assurant la transposition de la directive 2006/24 dans le droit interne autrichien.

S'agissant de la première affaire, la Digital Rights prétend être propriétaire d'un téléphone portable qui a été enregistré le 3 juin 2006 et qu'elle utilise depuis cette date. Elle introduit un recours devant la High Court le 11 août 2006 afin de remettre en cause la légalité des mesures législatives et administratives nationales quant à la conservation des données conservation de données relatives à des communications électroniques. Elle réclame à cet effet, la constatation de la nullité de la directive 2006/24.

S'estimant incompétente pour trancher de la validité de la directive, la High court sursoit à statuer et saisit en demande préjudicielle la CJUE. La High Court questionne la CJUE en ces termes : « *La restriction faite aux droits de la partie requérante en matière d'utilisation de téléphonie mobile qui découle des exigences des articles 3, 4 et 6 de la directive 2006/24 est-elle incompatible avec l'article 5, paragraphe 4, TUE, en ce qu'elle est disproportionnée et qu'elle n'est pas nécessaire ou qu'elle est inappropriée pour atteindre les objectifs légitimes (…).* A cet effet, *La High Court demande à la CJUE d'analyser la directive au regard des droits fondamentaux suivants :* Le droit des citoyens à circuler et à résider librement sur le territoire des États membres, consacré à l'article 21 TFUE, le droit au respect de la vie privée contenu dans l'article 7 de la Charte des droits fondamentaux de l'Union européenne et dans l'article 8 de la CEDH, le droit à la liberté d'expression consacré par l'article 11 de la Charte et par l'article 10 de la CEDH.

En réponse à la High Court, la Cour de Justice de l'Union européenne estime que la directive est invalide parce que le législateur européen a dépassé les limites qu'impose le respect du principe de proportionnalité en exigeant de la part des fournisseurs d'accès et des opérateurs assimilés, une conservation trop généralisée. De plus, la Cour ajoute que la directive opère une ingérence dans la vie privée des individus puisqu'aucune limite

[164] Il s'agit de la « Telekommunikationsgesetz 2003 introduit dans cette loi par la loi fédérale modifiant celle-ci (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011).

n'est fixée pour encadrer ladite conservation des données stockées par les fournisseurs d'accès. Par limite, il faut comprendre que tous les usagers quelle que soit leur activité ou leurs antécédents judiciaires sont concernés par cette conservation des échanges téléphoniques ou électroniques. Il n'est pas tenu compte d'une cible en particulier, notamment au regard d'une action en justice en particulier. C'est la généralisation des conservations téléphoniques qui est censurée par la Cour de justice.

Outre les interrogations précédentes, celle de l'utilisation adéquate des systèmes de confidentialité se pose. Comment les internautes y ont recours ? Le fait pour un internaute de cocher des cases relatives aux axes de confidentialité contenus dans les conditions générales de publication est-il un élément suffisant pour que cet internaute contrôle ses publications ? Tout internaute est-il suffisamment prudent dans le partage des éléments de sa vie personnelle et professionnelle sans crainte de se voir « piéger » dans l'avenir ?

La réponse peut tout de suite être négative puisqu'il suffit de sillonner les pages Facebook de plusieurs personnes avec lesquelles on n'est pas forcément amis pour se rendre compte que le système présente trop de failles : le cercle infernal *des amis des amis* crée la possibilité de poster des commentaires sur les informations injectées sur la page Facebook d'individus sans aucun lien. Et pourtant, ces publications sont dans tous les cas des portes d'entrée aux activités des cybercriminels. Si certains recruteurs, chefs d'entreprises ont recours à ces réseaux pour rechercher des informations sur leurs futurs employés ou connaître l'activité de leurs collaborateurs[165], les cybercriminels, qui sont des habitués des réseaux numériques ne sont aucunement exclus de profiter de ces aubaines et des informations divulguées sur ces réseaux. Il faut souligner que la pratique des recruteurs consistant à espionner les pages Facebook des demandeurs d'emplois ou des candidats à des postes est illicite en ce qu'elle porte atteinte à la vie privée de ces candidats. Les pages et échanges transitant par Facebook, étant des communications de l'ordre de la vie privée.

[165]Cf. **FEL C. et SORDET E.**, « l'utilisation des réseaux sociaux par l'entreprise et ses collaborateurs », Semaine juridique Pratique Sociale, pp19-24.

A ce propos, les règles de confidentialité sont fréquemment évoquées et sujettes à discussion. D'ailleurs, l'Agence de Sécurité Nationale américaine (NSA) fait l'objet depuis le début du mois de juin 2013 d'interrogations de la part de plusieurs journalistes sur cette question de la surveillance des réseaux de Facebook et de Google[166] notamment.

A ce sujet, la Commission européenne échange avec les responsables des firmes américaines et surtout de l'Agence de Sécurité Nationale sur les questions de la protection des données notamment en ce qui concerne les écoutes de masse et la surveillance des correspondances des internautes[167]. Sur tous les plans, la balance est à équilibrer quant aux aspects positifs et négatifs. Ce sont des cas d'espèce qui permettent de les mesurer davantage.

Sur un plan international, la publication via internet du film provocateur sur les dangers de l'islamisme intitulé *« l'innocence des musulmans », film de* Nakoula BASSELEY Nakoula[168] a donné lieu à des manifestations violentes dont l'attaque du consulat des Etats-Unis à Benghazi[169], entraînant la mort de l'ambassadeur des Etats-Unis et de plusieurs autres personnes dans le monde. Plusieurs manifestations ont également eu lieu.

---

[166]Cf. **GRALLET G.**, Journal Le point du 10 juin 2013 et pour une version en ligne cf. http://www.lepoint.fr/technologie/zimmermann-faire-confiance-a-google-ou-facebook-c-est-etre-a-poil-sur-internet-10-06-2013-1678994_58.php. D'ailleurs lors du Journal télévisé de France 2 du 11 juin, la question est soulevée et le parallèle est fait entre l'interception des communications de tout genre par l'administration américaine et les surveillances de ces communications en Europe et notamment en France.

[167] L'Union européenne a rencontré les responsables de la NSA pour discuter des questions des écoutes téléphoniques en masse en relation avec le programme PRISM (programme de surveillance des échanges électroniques et des communications téléphoniques) mis en place par l'Agence américaine de Sécurité depuis 2007 selon les informations divulguées par les journaux britannique et américain *The Guardian* et *Washington Post*, cf. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Voir également France 24 du 18 juin 2013 : article de **Sébastian SEIBST**, journaliste de France 24 sur http://www.france24.com/fr/20130607-prism-espionnage-nsa-cybersurveillance-donnees-facebook-google-yahoo-microsoft-scandale-verizon. La publication du programme PRISM a été confirmée par Edward SNOWDEN, ancien consultant de la NSA, au journal allemand *Der Spiegel*.

[168] Voir **GOUZY JP**, la vie politique en Europe et dans le monde, *L'Europe en formation*, 2013, n°3, p.229 - 255.

[169] cf. **SALLON H.,** l'innocence des musulmans, le film qui a mis le feu aux poudres, *Journal Le Monde*, 12 septembre 2012 ; Agence de presse du journal Le Figaro, L'auteur supposé du film anti-islam, arrêté par la police, *Journal Le Figaro international* du 15 septembre 2012.

Sur le plan de la politique interne (française), les élections législatives de 2012, dans la circonscription de la Charente maritime opposent Ségolène ROYAL à Olivier FALORNI. Après plusieurs démarches, Madame ROYAL reçoit un message de la part du Président de la République François HOLLANDE. Celui-ci lui témoigne son appui et son soutien en ces termes « Ségolène ROYAL est l'unique candidate de la majorité qui peut se prévaloir du soutien et de l'appui du Président de la République. » A la suite de la publication de ce message dans la presse, la page Twitter de la première dame, d'alors, compagne du Président François HOLLANDE contenait le tweet suivant : « *Courage à Olivier FALORNI qui n'a pas démérité, qui se bat aux côtés des Rochelais depuis tant d'années dans un engagement désintéressé* »[170]. Ce tweet marque clairement la prise de position adverse de la première dame par rapport au message de soutien envoyé par le Président de la République à la candidate de la majorité. Dans ce cadre, il est possible de souligner la polémique soulevée par le *tweett* de Valérie TRIERWEILER d'un tweet[171] aux élections législatives de 2012.

Au niveau des utilisations électroniques, les consommateurs créent des ouvertures aux cybercriminels notamment avec l'usage régulier des Wireless Fidelity [172]pour « WIFI » et des Bluetooth[173]aussi bien dans les relations professionnelles que

---

[170] Cf. **M. ESCOIFFIER et L. BRETTON**, « *Comment Valérie TRIERWEILER encourage l'adversaire de Ségolène ROYAL* », Journal Libération du 12 juin 2012 ; voir également F. GERSCHEL & E. HACQUEMARD, « *L'histoire secrète de la rivalité TRIERWEILER- ROYALE* », Journal Le parisien du 13 juin 2012.

[171] Tweet est le mot pour désigner le fait pour un membre du réseau social twitter de noter un commentaire ou une observation sur sa page en guise d'avis ou de point de vue. Journal Le monde du 12 juin 2012 : *le tweet de Trierweiler suscite l'embarras à gauche et l'ironie de la droite*. Pour une Version en ligne, consulter : http://www.lemonde.fr/article/2012/06/12/ tweet-de-Trierweiler-suscite-l-embarras-a-gauche-et-l-ironie- de-la-droite_1717193_823448.html .

[172] Le WIFI ou *Wireless fidelity* est une technique d'accès issue d'une norme internationale et qui favorise la connexion au réseau internet sans fil ni câble, cf. Vocabulaire des Nouvelles Technologies de l'Information et de la Communication, Journal officiel du 5 mai 2005.

[173] Le Bluetooth correspond à la norme IEEE 802.15.1 et c'est un standard ouvert à la transmission de la voix et des données entre terminaux mobiles (téléphones, assistants personnels, ordinateurs portables et ordinateurs fixes, mis en place en 1994 par le groupe ERICSON, Cf. *Information technology -- telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements*, IEEE Computer Society. LAN/MAN Standards Committee; International Organization for Standardization; International Electrotechnical Commission.; Institute of Electrical and Electronics Engineers; IEEE Standards Board. New York, N.Y., USA : Institute of Electrical and

personnelles.

En ce qui concerne les WIFI, la connexion d'un ordinateur à un poste sans fil et sans câble requiert un processus de sécurisation grâce à une clé appelée clé WEP[174] ou clé WAP.

Cette clé permet à l'utilisateur de s'identifier et à authentifier son accès. Les cybercriminels parviennent par des techniques[175] à dérober ces codes pourtant secrets.

A la suite de ces illustrations, il est possible d'affirmer que la protection des données personnelles uniquement par les textes législatifs contre les dérives de l'administration mais aussi des particuliers ne suffit plus. D'autres moyens plus efficaces doivent être trouvés.

Les activités de simples vols d'informations, de sabotage informatique ou de vols de données via les réseaux numériques sont une manifestation accrue des usages frauduleux des données laissant des traces sur les réseaux numériques. La ré-exploitation des données des personnes (qu'il s'agisse du nom, des adresses géographiques ou des données bancaires) par des individus peu scrupuleux, qui n'en sont pas les véritables propriétaires est devenue un exercice de base pour ces cybercriminels. C'est dire que les activités sur les réseaux numériques et électroniques de la part de ces malfrats connaissent de véritables mutations du fait de la professionnalisation des acteurs visés.

§ 2- Les mutations des activités cyber-criminelles

Les activités criminelles appartenant à la cybercriminalité sont essentiellement des actes frauduleux commis au moyen des réseaux électroniques et numériques ou encore

---

Electronics Engineers, 1998; et voir également **CONCHON E.**, *« Définition et mise en œuvre d'une émulation de réseaux sans fil »* thèse soutenue en octobre 2006 à l'Institut National Polytechnique de Toulouse sous la direction de Michel DIAZ.

[174] WEP c'est-à-dire Wireless Equivalent Privacy : il s'agit d'un protocole de sécurisation du contrôle d'accès et qui fournit l'authentification, l'intégrité et la confidentialité. cf. **ATELIN P.**, WIFI, solution de sécurisation, collection TechNote, ENI éditions, Saint Herblain, France, octobre 2006.

[175] Ces techniques sont citées par le Lieutenant **GUINIER**, dans sa présentation du 02 février 2011 à l'Université de Strasbourg sur la *cybercriminalité et son contexte géopolitique*. Ils peuvent facilement le faire en téléchargeant des logiciels à cet effet.

des actes visant ces réseaux. Il s'agit entre autres des intrusions informatiques, des altérations ou encore des ventes en ligne en dehors du cadre légal prévu.

Cette forme de criminalité numérique de base dont se saisissent les autorités notamment européennes connaît aujourd'hui une mutation qu'il faut prendre en considération aussi bien dans la prévention que dans la sanction de la cybercriminalité.

Il est possible d'observer que parallèlement à l'amélioration des technologies grâce aux innovations, les cybercriminels en font une nouvelle source d'inspiration (A). De plus, la tendance est à la professionnalisation de ces branches d'activités numériques illégales (B).

A- L'innovation technologique créatrice d'activité cybercriminelle

L'objectif est de relever les difficultés nées de l'évolution technologique. L''innovation technologique est continuelle. En effet, l'augmentation des performances techniques des nouvelles formes de communication, d'échanges ou de partages de données offre aux criminels numériques, de nouveaux supports pour organiser leurs activités criminelles. Il est possible d'en avoir une illustration avec la récupération des données bancaires par des internautes[176], qui n'en sont pas les propriétaires, dès lors qu'elles ne sont pas suffisamment sécurisées.

La publicité des nouvelles formes de technologies est certes une manière de les vendre et de mieux les faire connaître mais, elle est aussi et malheureusement une aubaine donnée aux attaques des cybercriminels. Dans la mesure où elle est une source d'amplification de l'activité cybercriminelle, l'innovation technologique s'analyse en un autre obstacle à la lutte contre la cybercriminalité. Il ne sera cependant pas question de freiner des évolutions sous prétexte qu'elles seront utilisées par des criminels à des fins malsaines.

---

[176] Cf. **ARPAGIAN N**. qui cite l'exemple du FBI qui a fermé, le 16 octobre 2008, une plateforme de marché illicite de récupération et de recel de données des internautes via un site baptisé « *Dark Market*. Ce site rendait disponible des informations de 2500 clients répartis dans le monde entier : cf. page 18, la cybersécurité.

Il faudra fort de ce constat trouver des moyens techniques dépassant les capacités de contournement et imaginatives de ces malfaiteurs.

L'innovation technologique est révélatrice de la rapidité des cybercriminels à réagir puisque ces derniers usent de ces techniques pour narguer les Etats à leurs poursuites. Des clubs, des sites dédiés spécialement à des attaques de structures étatiques et gouvernementales ont ainsi été créés par ces délinquants pour défier les Etats comme par exemple le site des *hacktivistes* dénommé ANONYMOUS. Ce groupe s'est assigné comme rôle de punir le Federal Bureau Investigation (FBI) en attaquant son site internet. Cette attaque a contribué à bloquer pendant un certain temps ledit site. Or bloquer un site institutionnel, le rend défaillant et inopérable même pour un laps de temps relativement court. Ce genre de blocage contribue à déstabiliser des institutions, d'autant plus quand elles sont dans des secteurs de la sécurité comme c'est le cas du FBI.

En outre, une autre illustration est celle du blocage du site du journal l'Express[177]. Ce quotidien a dû faire face à une attaque répressive de la part des hackers d'Anonymous pour avoir critiqué les pratiques de ce groupe. De la sorte, les idéaux défendus par ces délinquants sous prétexte de liberté d'expression se muent en attaques défensives et ciblées, utilisant à leur guise les nouvelles techniques de l'information. Il convient de souligner que toutes les sources utiles et créées pour faciliter la vie des citoyens deviennent une porte ouverte aux cybercriminels. Il faut dès lors s'interroger sur l'impact de « l'open data » quant à ces éventuelles sources. Que recouvre réellement ce terme : est-on en présence de données ouvertes si on transcrit littéralement ?

L'open data est le mouvement créé, en 2000, à la suite de la volonté du gouvernement OBAMA de jouer la transparence quant aux activités administratives. Il s'agit de rapprocher les populations de l'administration via la communication. Le problème est la confusion entre l'*open data* et l'*open Government*. Si l'open data consiste dans la communication des données de manière à en faciliter la lisibilité par les

[177] A la suite d'une critique du directeur du journal L'express, Christophe Barbier, sur la chaîne de télévision i- télé, le groupe Anonymous bloque le site officiel du journal : article de **E. METTOUT** du 23 janvier 2012 et disponible sur le site du journal cf. : http://www.lexpress.fr/actualite/media-people/media/anonymous-ou-anonymes-contre-l-express_1074418.html.

concernés, l'*open government* consiste en une ouverture des modes d'administration des structures. C'est en réalité la transparence dans la manière de gérer les ressources étatiques qui est mise en avant dans l'*open government*.

Les deux théories, *open data et open government* ne sont pas identiques, même si, toutes les deux, elles ont en commun la transparence quant aux données communiquées. Il faut néanmoins souligner que la transparence du service public par rapport aux usagers et aux citoyens ne doit pas être synonyme de non- respect de la vie privée. L'administration d'OBAMA aux Etats-Unis a d'ailleurs eu l'occasion de s'en rendre compte : la publication des budgets par Etat a mis au grand jour les déficits et des interprétations en sont nées. L'objectif de cette publication par l'administration fiscale était de montrer comment l'Etat gère les ressources et l'affectation des impôts qui en est faite. Le but visé n'a pas été compris par les populations dans la mesure où la manière de procéder n'est pas suffisamment pédagogique : les autorités américaines s'étant contenté de présenter les budgets à l'état brut des statistiques. Le résultat est différent si une autre manière de présenter ces budgets votés est utilisée : le canal des statistiques comparant des Etats ayant les mêmes critères démographiques ou présentant les mêmes richesses économiques, ou encore des potentialités de tourisme similaires.

Pour suivre cette dynamique de transparence, le Parlement européen vote courant juin 2012 l'adoption des règles qui ouvrent la réutilisation des données publiques[178] géographiques et de météo aux entreprises. Selon le député bulgare Ivaiola Kalfin[179], cette ouverture aux données publiques facilitera l'acceptation de la part des entreprises du principe de la transparence. Il semble qu'il permette la prospection auprès des clients. Cette méthode remet tout de même en cause l'interdiction de la prospection directe.

---

[178] Il s'agit en réalité de la modification de la directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public, publiée *au* Journal officiel n° L 345 du 31/12/2003 p. 0090 – 0096 ; le texte a été déposé au Sénat le 19 décembre 2011 et examiné par la commission des affaires étrangères et européennes le 07 juin 2012. Cf. site du Sénat : http://www.senat.fr/ue/pac/E6950.html

[179] Voir le détail sur : http://www.europarl.europa.eu/news/fr/headlines/content/20130610STO11409/html/Les-d%C3%A9put%C3%A9s-approuvent-l'acc%C3%A8s-aux-donn%C3%A9es-publiques-pour-stimuler-l'innovation

Lorsqu'un individu « lambda » donne son accord pour ses données géographiques notamment dans un annuaire tenu à l'administration, cet accord répond à un objectif précis. Permettre à des entreprises de réutiliser ces données communiquées dans un but précis, n'est-il pas de nature à forcer cet individu lambda à faire d'autres démarches pour accepter ou refuser les publicités ou autres actions prospectives des entreprises autorisées à réutiliser ces données recensées et mises à jour par l'administration ?

Le texte de la directive européenne sur l'open data a été voté et publié au Journal officiel[180]. Il s'agit de la directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des données détenues par le secteur public.

L'open data devient au regard des données qu'il communique, un autre facteur de commission d'actes cybercriminels. Il est possible de conclure que toute donnée injectée sur les réseaux numériques est une potentielle source exploitable par des réseaux cybercriminels.

C'est d'ailleurs dans cet ordre d'idée qu'on peut faire cas de professionnalisation des branches cybercriminelles.

B- La professionnalisation des cybercriminels

Il est possible de parler de professionnalisation des cybercriminels eu égard à la manière de procéder qui progresse. En effet, par le passé, la subtilité n'était pas de mise et il était plus fréquent pour des personnes de craquer des codes de sécurité afin de pouvoir infiltrer les systèmes informatiques visés. David S. WALL a procédé à une classification de la cybercriminalité en diverses générations dans son ouvrage *Cyber crime : the transformation of the crime in information Age*[181]. Selon cet auteur, il y a trois générations de cybercriminalité :

---

[180] Cf. Directive 2013/37/UE du Parlement européen et du Conseil publié au JOUE L. 175/1 du 27 juin 2013.

[181] Cf. **WALL D. S**., Cybercrime: the transformation of crime in the Information age, P 45-46, op. cit.

Cf. Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.

La première génération de cybercriminalité concerne des opérations de fraude effectuées avec discrétion. Elles sont secrètes et ne visent qu'un système informatique à la fois. Il cite en exemple la fraude du Salami « the Salami Fraud » opérée dans le film Superman III : Gus Gorman, le fraudeur dont il est question, transfère des sommes d'argent via données bancaires par petites coupures sur son moyen de paiement (en l'occurrence il payait par chèque). Dans ce cas, l'outil informatique est un moyen pour commettre l'infraction.

La seconde génération est celle qui utilise le réseau informatique c'est-à-dire il est fait appel à des systèmes informatiques en nombre beaucoup plus important et cette fois il est question de craquer des codes et d'infiltrer des systèmes à la fois téléphoniques et informationnels. Cette génération utilise les réseaux de télécommunication pour déchiffrer des codes numériques.

La troisième génération de cybercriminalité est marquée par sa nature distributive et automatique. C'est l'ère des robots distribuant les virus sans forcément s'intéresser à une cible en particulier. C'est ainsi qu'au XXIème siècle, la pratique est d'infiltrer les systèmes informatiques de sorte à en devenir des administrateurs parallèles. C'est notamment ce qui est arrivé en 2010 pour le système informatique de l'OCDE ou encore pour l'entreprise AREVA[182] et encore plus récemment, en mai 2013 l'infiltration du système informatique de l'Agence Internationale de l'Energie Atomique par les hackers syriens[183].

Cette classification est conforme à la réalité puisque c'est dans cet ordre que les cybercriminels font évoluer leurs activités. Les actions ne se limitent pas aux attaques

---

[182] Cf. France Info du 29 septembre 2011, *AREVA victime d'une attaque informatique, renforce sa sécurité*, disponible en ligne : http://www.franceinfo.fr/france-justice-police-2011-09-30-areva-victime-d-une-attaque-informatique-renforce-sa-securite-565505-9-11.html; lire également V. ARENE, Le monde informatique du 30 septembre 2011, *le réseau informatique d'AREVA piraté* ; l'information figure enfin dans le Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.

[183]Flash d'information diffusée sur les ondes de la radio Europe 1, le 22 octobre 2013 avec pour titre : *Nucléaire: l'AIEA victime d'attaque informatique*, disponible en ligne http://www.europe1.fr/International/Nucleaire-l-AIEA-victime-d-attaque-informatique-1682937/; voir

matérielles. La subtilité utilisée par les cybercriminels dans cette perspective évolutive s'analyse par ailleurs au plan psychologique.

C'est l'influence psychologique qui est exercée par des réseaux de cybercriminels sur des personnes vulnérables ou influençables comme des jeunes à la recherche d'une cause à défendre. C'est l'occasion de sonder la modélisation actuelle des comportements de ces jeunes. L'impact d'internet et des communications électroniques sur le comportement des individus est notable dans le fait que les criminels du cyberespace sont recrutés de plus en plus jeunes. Le fait de commettre des actes via et sur les réseaux informatiques est petit à petit remplacé par l'utilisation de ces réseaux comme des moyens de formation pour transformer ces jeunes personnes en criminels. En d'autres termes, internet sert à véhiculer des messages de nature à influencer le psychique et endoctriner des personnes.

Deux illustrations fondent cette affirmation d'endoctrinement des jeunes via l'Internet. La première est relative à la fabrication d'armes explosives par des étudiants brillants, par l'intermédiaire des sites internet, dans la ville de Boston[184]. Le second événement est le massacre à l'arme blanche d'un jeune soldat londonien par un homme seul, qui se réclame du mouvement islamiste. Ce second événement tragique a eu lieu en pleine rue, le 23 mai 2013[185]. La réponse donnée par le tueur est que le soldat assassiné aurait tué des femmes et des enfants musulmans en Afghanistan et en Iraq compte tenu de l'engagement de l'armée anglaise sur ces territoires. Cette réponse est symptomatique des amalgames qui peuvent être faits à la suite de propagandes sur internet. Amalgame entre l'apologie des crimes via internet et la religion. La religion est mise en avant comme

---

également l'article de M. BAUD, « cyber guerre. En quête d'une stratégie, Focus stratégique, n°44, mai 2013.

[184] Cf. l'information relayée par le journal Le Parisien : http://www.leparisien.fr/faits-divers/attentats-de-boston-le-suspect-est-toujours-a-l-hopital-21-04-2013-2745431.php;
Pour une autre version des événements : http://www.bfmtv.com/international/boston-freres-tsarnaev-prevoyaient-un-attentat-4-juillet-506728.html;

[185]L'actualité a été reprise par différentes presses comme Le journal Le Figaro du 23 mai 2013 et disponible à l'adresse : http://www.lefigaro.fr/international/2013/05/23/01003-20130523ARTFIG00380-la-grande-bretagne-sous-le-choc-apres-le-meurtre-barbare-a-londres.php. En complément, voir le journal Le Monde du 1er juin 2013 faisant état de l'inculpation du jeune homme, pour une version en ligne, voir : http://www.lemonde.fr/europe/article/2013/06/01/soldat-tue-a-londres-le-deuxieme-suspect-inculpe_3422408_3214.html.

vecteur pour véhiculer des messages d'incitation au crime, des idées de vengeance par l'intermédiaire des réseaux de télécommunication et principalement par internet.

L'assassinat d'un ou plusieurs éléments des forces de l'ordre dans des lieux publics est un moyen pour les terroristes de choquer les populations, surtout les politiques et d'attirer l'attention des médias sur leurs causes. La preuve est qu'à chaque acte de cette nature et envergure, des groupes formés comme le BOKO HARAM[186] du Nigéria, le revendiquent. Internet est un canal médiatique très utilisé par ces groupes, qui ont des services de renseignements à la pointe de la technologie.

En analysant ces actions au regard de la surveillance par l'Etat de ces individus, il faut se demander comment expliquer le manque d'anticipation. Est-ce de la négligence dans la mesure où ces personnes qui commettent des exactions, sont pourtant surveillées dans le but d'éviter des dérapages ?

L'affaire du massacre de Londres au mois de mai 2012 rappelle celle du jeune MERAH[187], qui a été suivi pendant plusieurs années par les services de la Direction des renseignements français, en France et à l'étranger. Ce dernier a effectué des voyages en Afghanistan selon les autorités policières et de renseignements généraux. Et malgré cette connaissance des déplacements douteux, les crimes qu'a commis Mohamed MERAH n'ont pas pu être évités.

Un aspect des mutations de la cybercriminalité est celui des actions illicites organisées via le web profond encore appelée « *deep web* ». Il s'agit d'une partie des réseaux

---

[186] Nom de la secte islamiste nigériane, terroriste à l'origine de plusieurs enlèvement notamment de Français au Cameroun et au Nigéria : cf. http://www.pressafrik.com/Boko-Haram-revendique-l-enlevement-des-sept-otages-francais_a98589.html; voir aussi : Le Monde diplomatique avril 2012, article d'Alain Vicky « aux origines de la secte *Boko Haram* », p 8 et 9.

[187]Cf. Agence Française de Presse, *Toulouse : un militaire abattu d'une balle dans la tête*, Journal Libération du 03 mars 2012 ; cf. aussi Gilbert LAVAL, *Des parachutistes pris pour cible à Montauban*, Libération du 16 mars 2012 ; ajouter l'article de Sylvain MOUILLARD, *A Toulouse, la communauté juive sous le choc*, Libération du 19 mars 2012 ; Voir également Caroline POLITI, Toulouse: *le récit de la traque de l'ennemi public n°1* publié au Journal l'Express du 21 mars 2012 et disponible sous le lien :http://www.lexpress.fr/actualite/societe/toulouse-le-recit-de-la-traque-de-l-ennemi-public-n°1_1096271.html#KGddCZZcky3bKTju.99. A compléter avec l'article paru dans le Journal Le Monde du 22 mars 2012 intitulé : un *tueur au scooter*.

numériques à laquelle les moteurs de recherche classiques n'ont pas accès. Cette voie est prisée par les cybercriminels qui y mènent leurs actions illicites de manière quasi- aisée.

Les changements opérés dans le domaine de la criminalité commise sur internet et les réseaux numériques s'apprécient également en termes d'organisation sectorielle.

Il existe plusieurs explications au fait que l'Etat n'arrive pas à mettre la main sur les délinquants. La première explication tient à une bonne maîtrise des outils informatiques par les cybercriminels. La seconde explication relève du fait que ces délinquants réussissent souvent à détourner l'attention de l'Etat et de ses services en faignant d'être intégré, en menant une vie normale au point de faire croire à une repentance, à une réinsertion. Et une fois, la surveillance réduite, les délinquants reprennent leurs activités criminelles. La troisième explication est liée au fait qu'on ne connaît pas jusqu'où l'Etat peut aller dans sa surveillance des grands criminels (terroristes). Les attentats du début du mois de janvier 2015 contre le Journal Charlie Hebdo[188] et du supermarché de Vincennes (en France) permettent de s'interroger sur cet élargissement des écoutes : Ne peut-on pas ordonner des écoutes des membres de la famille du délinquant poursuivi. Selon le Procureur de la République, François MOLINS, les épouses des terroristes ont échangé plusieurs coups de fils (500). Ce qui est important en termes de communication et conduit à se questionner sur la nature de ces communications. Finalement, ces échanges avaient-ils pour but de préparer les attentats ? Les époux de ces dames, les terroristes utilisaient-ils les téléphones comme couverture et échapper ainsi aux écoutes mises en place dans le cadre de leur surveillance ?

Le débat des surveillances par l'Etat s'en trouve relancé quant à l'étendue et aux limites.

En réalité, il n'y a pas que l'activité terroriste qui emprunte de nos jours les voies numériques comme internet. D'autres infractions comme le blanchiment d'argent, la consommation et la vente de drogue s'appuient également sur ces mêmes voies. En considération de ce qui précède, on peut dire que la cybercriminalité prend l'aspect de

[188]Cf. Journal Le Monde du 08 janvier 2015, Attentat contre « Charlie Hebdo » : le récit d'une journée noire ; Journal Libération du 08 janvier 2015, Fusillade meurtrière à Charlie Hebdo, article disponible en ligne sous : http://www.liberation.fr/fusillade-charlie-hebdo,100481.

crime organisé via l'usage des réseaux de communication quels qu'ils soient : il peut s'agir des ordinateurs zombies pour pirater par exemple des serveurs de banque, des téléphones ou des réseaux hydrauliques[189].

Comme le révèlent quelques exemples situés sur la période 2012-2014, les cybercriminels affinent de plus en plus leur modus operandi.

Premièrement, en 2012, le site pétrolier saoudien *Saudi Aramco* a été attaqué : 30.000 ordinateurs ont été infectés, et leurs données ont été effacées *et remplacées par une image du drapeau américain en feu*[190].

Deuxièmement, en 2013, il y a eu l'attaque dénommée *Dark Seoul* qui a visé les interfaces bancaires et les médias de la Corée du Sud ;

Enfin, en décembre 2014, le système informatique de SONY Pictures a été victime d'une attaque. Selon les experts en sécurité informatique de Symantec, cette attaque a été menée, avec les techniques utilisées dans les précédents exemples. L'attaque de SONY a consisté pour les cybercriminels à insérer un logiciel malveillant dans le système informatique de SONY, pour en extraire des données et informations confidentielles de différentes catégories (aussi bien des informations concernant des clients, que des salariés de l'entreprise américaine)[191]. Les auteurs de cette attaque ont par la suite voulu échanger ces données contre des sommes d'argent. Le chantage financier, n'ayant pas abouti, les données ont été divulguées sous la forme de messages sur l'écran des salariés de SONY Pictures.

On le voit, de même que les technologies évoluent, les cybercriminels s'adaptent à ces progrès scientifiques en changeant et variant leurs modes opératoires. Les jeunes

---

[189] Le piratage des réseaux hydrauliques ou des conduits de gaz sont d'autres formes qu'empruntent les actes de cybercriminalité : le mode opératoire répond à l'usage des canaux permettant la circulation de l'information.

[190] Cf. article de **Clément BOHIC**, Journal IT expresso, disponible en ligne sous le lien : http://www.itespresso.fr/piratage-sony-pictures-certitudes-impuissance-fbi-85462.html

[191] Voir : http://www.lenouveleconomiste.fr/financial-times/le-piratage-sans-precedent-des-studios-sony-25533/

cybercriminels s'inspirent des techniques antérieures, déjà utilisées et surtout de processus qui sont très médiatisés: la technique du *Dark Seoul*, en est une illustration, puisque l'attaque informatique dont a été victime le studio américain SONY Pictures en 2014, est similaire à cette technique déjà employée en 2013.

D'autres activités criminelles telles que le trafic de drogue, le blanchiment d'argent se servent des outils numériques[192]. D'ailleurs, le proxénétisme également côtoie ces organisations criminelles. Petit à petit, les pratiques qui consistent à appâter un homme via une webcam par les atouts physiques d'une jeune dame intègrent les actes cybercriminels : c'est ce qu'il est convenu d'appeler la *cyber-prostitution*. Cette technique est exercée dans divers pays (pays d'Afrique, de l'Europe de l'Est). S'agissant de la répression, si elle apparaît comme aisée pour les pays de l'Union européenne à cause de l'existence d'instruments juridiques harmonisés, il n'en va pas de même pour l'Afrique de l'Ouest.

L'identification des sources de la commission des infractions sur internet est un vecteur pour la stratégie européenne de lutte contre la cybercriminalité.

Section 2 : La stratégie européenne de lutte contre la cybercriminalité

Internet ne connaît pas les mêmes frontières territoriales que les autres domaines. C'est toute la question de l'immatérialité du cyberespace et de la fixation de ses limites. Dans ces conditions, il s'avère particulièrement délicat de créer un corpus de règles répressives couvrant des espaces non identifiés. C'est pourquoi la construction des incriminations se veut pointue, méthodique et délicate. (§1)

Cette stratégie est délicate dans la mesure où elle révèle les deux Europe (d'une part l'Europe politique à travers le Conseil de l'Europe et d'autre part l'Union Européenne,

[192] Cf. Article de C. GUILLEMIN sur le journal ZDNET : http://www.zdnet.fr/actualites/blanchiment-des-capitaux-nouvelle-tendance-de-la-cybercriminalite-en-2006-39366347.htm; compléter avec le livre blanc de McAfee sur le blanchiment numérique, Analyse des monnaies virtuelles et de leur utilisation à des fins criminelles, rédigé par Raj SAMAN, François PAGET et Matthew HART, 2014.

beaucoup plus économique). Dans ce contexte, le Conseil de l'Europe a régulièrement émis des recommandations à l'endroit des Etats membres[193]. L'une des plus importantes est la Recommandation R(89) 9 du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur. Elle a été adoptée par le Comité des Ministres le 13 septembre 1989, lors de la 428e réunion des Délégués des Ministres[194].

Dans un premier point, la recommandation R(89) 9 demande aux Etats membres du Conseil de l'Europe, de prendre en considération le rapport sur la criminalité en relation avec l'ordinateur, élaboré par le Comité européen pour les problèmes criminels, et, précisément, des principes directeurs pour les législateurs nationaux, et ce, lors des révisions de leurs législations, ou lors de l'élaboration de nouvelles lois. Le second point de la recommandation exige aux mêmes Etats d'établir un rapport au Secrétaire Général du Conseil de l'Europe en 1993 sur toute évolution de leur législation, de leur pratique judiciaire, et de leurs expériences en matière de coopération juridique internationale relative à la criminalité informatique[195].

Cette double exigence qui ressort de la recommandation R(89) 9 démontre la volonté d'harmonisation des législations dans le domaine de la criminalité informatique. D'ailleurs, la coopération judiciaire internationale en dépend dans la mesure où les textes législatifs sur le plan international, se trouveront ainsi harmonisés. C'est pourquoi la recommandation est un pilier de la lutte contre la cybercriminalité dans le monde. S'y ajoute la Recommandation n° R(95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information[196].

---

[193] Le conseil de l'Europe compte 47 pays dont les 27 Etats de l'Union européenne cf. le site officiel du Conseil de l'Europe : http://hub.coe.int/fr/

[194] Cf. Annuaire européen, 1989, vol. XXXVII, Martinus NIJHOFF PUBLISHERS.

[195] Recommandation n° R (89) 9 du comité des ministres aux états membres sur la criminalité en relation avec l'ordinateur (adoptée par le comité des ministres le 13 septembre 1989, lors de la 428e réunion des délégués des ministres).

[196] Cf. Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information (adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres).

Ces recommandations concernent donc également les Etats tiers à l'Union Européenne, membres du Conseil de l'Europe. C'est le cas par exemple de la Turquie, qui a adhéré au Conseil de l'Europe depuis le 9 août 1949[197]. Ces pays souhaitent avoir un niveau de protection suffisamment élevé[198] afin de correspondre aux normes de sécurité établies pour échanger avec les pays de l'Union européenne notamment. Ils entendent, par conséquent, être plus actifs dans la lutte contre la criminalité technologique. Dès 1998, dans les périodes expansives de l'internet, la stratégie de lutte contre la criminalité contre la haute technologie est élaborée grâce à des décisions cadre. Ces décisions sont des actes pris en application du Traité de l'Union Européenne et elles s'adressent aux Etats-membres directement. La prise en compte des enjeux liés à la sécurité du numérique en Europe s'accentue en 2000 avec l'adoption de la stratégie de Lisbonne[199] des 23 et 24 mars 2000.

L'objectif de cette stratégie est le renforcement de la société d'information en une société de connaissance. Cette volonté d'étendre la connaissance s'accompagne de la mise en place d'une sécurisation des systèmes d'information. C'est pourquoi, les 19 et 2 juin 2000, le Conseil européen de Feira[200] a approuvé un plan global d'action sur

---

[197] La Turquie est même un des pays fondateurs du Conseil de l'Europe : cf. le point 1 de la résolution 1380 de 2004, qui elle-même renvoie à la recommandation 1662 de la même année.

Les deux documents étant relatifs aux obligations et engagements de la Turquie en tant que membre du Conseil de l'Europe. Cf. également pour une citation de la date : http://hub.coe.int/web/coeportal/country/turkey?dynLink=true&layoutId=171&dlgroupId=10226&fromArticleId. La recommandation et la résolution précitées peuvent être consultées en ligne sous ces liens : http://assembly.coe.int/Documents/AdoptedText/ta04/FREC1662.htm et http://assembly.coe.int/Documents/AdoptedText/ta04/FRES1380.htm.

[198] Niveau de protection exigé par la directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données publiée au Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050, article 56 qui exige « *un niveau de sécurité adéquat.*»

[199]Cf. : http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/fr/ec/00100-r1.f0.htm, et voir également étude sur la cyberdéfense et la cybersécurité au sein des institutions européennes, réalisée par ESTERAL CONSULTING sur demande des affaires stratégiques du ministère de la défense française.

[200] Cf. le point 22 des conclusions de la présidence à l'issue de la tenue des débats précise qu'il faut : « *préparer des perspectives à plus long terme pour une économie fondée sur la connaissance, qui favorise l'intégration par les technologies de l'information et comble la fracture numérique. Il convient, en tant que mesure prioritaire à court terme, de prendre les dispositions nécessaires pour faire baisser le coût d'accès à l'Internet grâce au dégroupage de la boucle locale* ».

l'initiative *eEurope* et a demandé sa mise en œuvre avant la fin 2002. Ce plan d'action souligne l'importance que revêtent la sécurité des réseaux et la lutte contre la cybercriminalité.

Le 26 janvier 2001 la Commission au conseil, au Parlement européen, au Comité économique et social et au comité des régions présente la communication 2000/890 intitulée *créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité* [201].

Pour mettre en pratique cette lutte, la Convention de lutte contre la cybercriminalité est élaborée sur la base du rapport établi par le Comité européen pour les problèmes criminels. Ce rapport est en réalité en grande partie le projet de la convention dite de Budapest de 2001.

En effet, les pouvoirs publics européens ont pour objectif d'harmoniser les textes législatifs nationaux concernant les incriminations relevant de la Convention sur la cybercriminalité du 23 novembre 2001 dite également Convention de Budapest.[202]

En réalité, la Convention définit les grandes lignes des incriminations liées à la cybercriminalité et laisse le soin aux Etats signataires de préciser davantage ces incriminations. Toutes les infractions nécessitent des précisions notamment dans les applications pratiques. Les explicitations sont laissées à l'appréciation des Etats parce que cette compétence relève des prérogatives liées à la souveraineté étatique.

A la Convention, s'ajoute le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques[203] et date du 28 janvier 2003. Il a été établi 2 ans après la Convention de Budapest. Il est requis cinq ratifications pour donner force

---

Cf. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/fr/ec/00200-r1.f0.htm

[201]Pour la version PDF : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:FR:PDF

[202] Cf. Convention sur la cybercriminalité, 23. XI. 2001, publiée à la Série des Traités Européens STE n° 185, et compléter avec l'article de **CHOPIN F**., *les politiques publiques de lutte contre la cybercriminalité*, Actualité Juridique pénal 2009, p. 101

[203] Pour une version en ligne : http://conventions.coe.int/treaty/fr/Treaties/Html/189.htm

contraignante à ce protocole. C'est depuis 2006 que les 5 ratifications ont été obtenues. C'est pourquoi, depuis le 1er mars 2006, ce protocole est entré en vigueur[204].

Outre, la Convention de lutte contre la cybercriminalité, d'autres textes comportant des dispositions liées au champ d'application de la cybercriminalité s'ajoutent.

A ce titre, la protection des données à caractère personnel est envisagée grâce à la Convention 108 du 28 janvier 1981 du Conseil de l`Europe sur la protection des personnes à l`égard du traitement automatisé des données à caractère personnel[205]. A cette Convention, est affilié le protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données signée en 28 novembre 1981[206].

C'est en appui d'un nombre aussi important de normes souvent peu claires que les juges devront intervenir tant au niveau communautaire que national. (§2)

§1- La construction normative de la répression de la cybercriminalité : les incriminations

La construction normative de la répression concerne les incriminations des actes relatifs à la cybercriminalité au sein des pays de l'Union européenne. Il s'agit spécifiquement de comparer les incriminations contenues dans l'ensemble des législations de chacun des Etats membres de l'Union européenne.

Sous l'égide de l'Union européenne, il n'y a pas réellement de Convention relative à la cybercriminalité propre aux Etats de l'Union. Mais de manière indirecte, les

---

[204] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG

[205] Convention du 28 janvier 1981 parue à la Série des Traités Européens (STE) 108.

[206]Ce protocole additif de la convention précitée est en lien direct avec la cybercriminalité puisqu'il est question de protection des données personnelles et surtout de leur traitement. Il est publié à la STE sous le numéro 181. Protocole dont la ratification a été autorisée en France par la loi n° 2007-301 du 5 mars 2007 autorisant l'approbation du protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données publiée au Journal Officiel du 7 mars 2007 page 4323 (texte n° 5).

Etats de l'Union Européenne ont signé des conventions gravitant autour de la cybercriminalité c'est-à-dire des conventions qui traitent des questions directement liées à la cybercriminalité. C'est le cas par exemple de la protection des données, de l'organisation des transferts de données, des questions de contrôle des flux transfrontières.

Au titre de la classification des incriminations cybercriminelles, il est fréquent de voir que les atteintes sont regroupées selon qu'elles concernent les biens, les personnes ou encore les systèmes informatiques en eux-mêmes[207].

La Convention dite de Budapest du 23 novembre 2001[208] sur la cybercriminalité contient quatre catégories d'infractions qui sont :

- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques ;

- les infractions informatiques ;

- les infractions se rapportant au contenu et

- les infractions liées aux atteintes à la propriété intellectuelle et les droits annexes.

Qu'il soit permis de les aborder autrement. L'ordinateur est certes un outil très utilisé mais le développement de nouvelles applications notamment sur les outils mobiles comme le téléphone oblige à prendre en considération les infractions liées aux données transitant par ce canal. En plus des appareils mobiles, les données peuvent enfin emprunter d'autres chemins comme des réseaux et serveurs. C'est pourquoi les textes de loi réprimant la cybercriminalité doivent également couvrir ces espaces particuliers. Ainsi, les incriminations peuvent être classées selon qu'elles concernent l'ordinateur (A), le téléphone mobile ou autres terminaux assimilés (B) et enfin les réseaux et serveurs (C).

A- Les incriminations liées à l'ordinateur et aux systèmes informatiques

[207] Cette classification est adoptée notamment par Mme **QUEMENER Myriam** dans son ouvrage « cybercriminalité et droit pénal appliqué » paru aux éditions ECONOMICA, en 2010.

[208] cf. Série des Traités Européens STE n° 185 – Convention sur la cybercriminalité, 23.XI.2001.

Ces incriminations liées à l'ordinateur sont celles qui traitent des infractions relatives aux attaques directes des ordinateurs ou des systèmes informatiques. En quoi consiste une attaque de ce genre ? Ce comportement intrusif ou de maintien dans un système sans y avoir été autorisé, encore appelé *hacking* selon le terme anglo-saxon, peut être défini de manière générale comme une intrusion illicite dans un système informatique. Il s'agit des cas dans lesquels un utilisateur[209]: « *Sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient. Avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique*».

Il y a 3 types d'intrusion frauduleuse:

- Les *black hat* dont le but est de nuire, de saccager un système informatique purement et simplement. Ce sont en général des personnes infiltrées dans des organismes de toute envergure et qui agissent dans l'ombre. Ce qui leur vaut leur intégration dans le groupe « Anonymous » par exemple.
- Les *white hat* viennent pour procéder à des intrusions professionnelles sans rien entreprendre jusqu'à ce qu'ils se fassent appréhender : cas de l'anglais Gary McKinnon qui a procédé à la plus importante des intrusions informatiques sur le site du Pentagone en 2002 et condamné à dix (10 ans de prison) [210].
- Les *grey hat* : se situent entre les 2 premiers blocs précédents.

Dans le cadre des intrusions frauduleuses, l'objet de l'atteinte est l'ordinateur ou plutôt le système informatique. Le système informatique est défini par l'article 1 du chapitre 1 de la Convention de lutte contre la cybercriminalité comme « *tout dispositif isolé ou*

---

[209] L'article 550 bis du code pénal a été inséré par la loi sur la criminalité informatique 2000-11-28/34 et a été publié au moniteur Belge du 03 janvier 2001, voir également http://www.polfed-fedpol.be/crim/crim_fccu_ict_fr.php

[210] Information publiée dans le journal l'express su 17 octobre 2012: « Grande-Bretagne: autiste, le hacker du Pentagone ne sera pas extradé, voir : http://www.lexpress.fr/actualite/monde/europe/grande-bretagne-autiste-le-hacker-du-pentagone-ne-sera-pas-extrade_1175569.html#6UDix917EW38PMpR.99.
Compléter avec l'article de James Sturcke and agencies " *Hacker Gary McKinnon loses appeal against extradition to US" disponible sur le site du journal* theguardian.com, du 28 August 2008, http://www.theguardian.com/technology/2008/aug/28/hacking.security.

ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données »[211].

Le but étant de détruire un système informatique grâce à un accès frauduleux au système encore appelé intrusion informatique ou de rendre le système concerné défectueux pour parvenir à dérober des informations qui y sont stockées. Il existe plusieurs infractions qui revêtent soit la forme d'intrusion soit d'autres formes de hacking.

a- Les intrusions frauduleuses et leurs dérivés

L'incrimination d'intrusion frauduleuse nécessite de définir ses termes et son contenu. S'agit-il uniquement de l'accès illégal aux informations ou les infractions qui découlent de cet accès ou enfin des deux actes à la fois[212] ? De manière plus explicite, en quoi consiste une infraction d'intrusion frauduleuse ? Le fait d'accéder de manière frauduleuse à un système de traitement de données à lui seul, est-il sanctionné ou faut-il nécessairement un acte illégal en plus de l'accès sans autorisation ?

A la lumière de la Convention de Budapest, deux grandes catégories sont concernées. Il est question de la série des infractions relatives à la confidentialité, l'intégrité et la disponibilité d'une part et des infractions informatiques d'autre part.

La première catégorie concerne les données et les systèmes informatiques et correspond au titre 1 de la convention. Plusieurs infractions sont définies : l'accès frauduleux, l'interception frauduleuse, l'atteinte à l'intégrité des données et l'atteinte à l'intégrité du système informatique. L'article 1 de la convention précise que l'accès illégal suppose un accès intentionnel et sans droit à tout ou partie d'un système informatique.

La seconde catégorie est de l'interception illégale. Elle implique « *une intention et aucun droit,* et surtout il faut qu'elle soit effectuée *par des moyens techniques, de*

---

[211] Cf. article 1 chapitre1 de la Convention sur la cybercriminalité, 23.XI.2001 STE n° 185.

[212] Comprendre LA CYBERCRIMINALITE, guide pour les pays en développement, International Telecommunications Union.

données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques ». A titre d'exemple, le fait d'insérer une clé USB dans un système informatique pour l'infecter de virus sans nécessairement une destruction ou la disparition de données. C'est le cas d'une affaire en 2010 relative à la transmission de virus dans le système informatique de l'OCDE en 2010[213].

En troisième position, la Convention traite de l'atteinte à l'intégrité des données en ces termes : l'incrimination concerne « *le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques* ».

En quatrième lieu, c'est l'atteinte à l'intégrité du système informatique qui est mentionnée et sanctionnée à condition qu'il y ait *eu intention et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.*

La Convention de Budapest a bien déterminé les contours de l'incrimination. Il convient de se demander dans cette mesure ce qui est incriminé et ce qui est sanctionné selon les Etats.

En effet, soit l'accès à un système de données est illégal et l'infraction est commise dès cet acte non permis ; soit l'accès est légal mais le maintien quant à lui, non autorisé et ce maintien constitue une infraction puisque non voulu ou non consenti par les propriétaires du système concerné. Le maintien illégal pourrait dès lors justifier de sanctionner de tels actes étant entendu que sera puni le fait d'avoir violé l'intimité des concernés en utilisant à leur insu leurs données personnelles, des informations propres à leur personne.

---

[213] L'information n'a pas été relayée par plusieurs journaux dans la mesure où les employés de l'OCDE ont été discrets de peur de créer la panique. Mais lors de la réunion ministérielle, le 05 novembre 2010, le journal Under news, a posté un article en ligne à la suite de la communication des ministres sur cette attaque informatique. Pour lire l'article cf. https://www.undernews.fr/hacking-hacktivisme/le-reseau-de-locde-pirate.html.

Le hacking, dans son ensemble, est incriminé par la loi belge du 28 novembre 2000 sur la criminalité informatique [214] et codifié à l'article 550 bis du code pénal belge. Ce texte pénal dispose que : « *Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.* »

En application de la législation belge, la jurisprudence différencie le hacking interne du hacking externe. Cette distinction repose sur le fait que dans le hacking interne, il faut en plus des actes, une intention frauduleuse. En ce qui concerne le hacking externe le dol général suffit, le dol spécial constituant une circonstance aggravante[215]. Tandis que le dol général est défini ici comme la conscience et la volonté d'enfreindre la loi pénale, le dol spécial s'entend de la connaissance par l'agent de l'absence de droit à accéder au système informatique concerné[216].

On peut citer ici l'arrêt de la Cour d'appel de Paris en date du 5 février 2014 rendu par la chambre 10. Les faits opposent Monsieur Olivier L. au Ministère public. Plus précisément, à la suite de recherches expertes via le moteur de recherches Google, Monsieur Olivier L. a eu accès à l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), a téléchargé des documents contenus sur cet extranet et les a utilisés pour écrire un article. Il publie cet écrit sur internet en utilisant un pseudonyme et y adjoint les pièces téléchargées sur l'extranet de l'ANSES. La publication fait l'objet d'enquête et les contrôleurs des pages de l'ANSES se rendent compte d'un accès frauduleux à l'extranet. Après avoir reconnu les différentes manœuvres entreprises sur cet extranet, sans y avoir été autorisé, Monsieur L. a reconnu s'y être maintenu et avoir communiqué une partie des informations à une autre personne. Le juge du Tribunal de Grande instance de Créteil est saisi pour mettre fin à cette

---

[214] Cf. Loi du 28 novembre 2000 relative à la criminalité informatique, publiée au Moniteur belge, 3 février 2001, p. 2909

[215] Revue de droit des technologies de l'information belge, p.17

[216] Cf. **Jean PRADEL** définit clairement ces deux aspects du dol dans son article sur les infractions relatives à l'informatique paru à la Revue Internationale de Droit Comparé, Vol. 42 N°2. Avril-juin. Etudes de droit contemporain. pp. 824.

pratique. Il relaxe Monsieur Olivier L. Le ministère public interjette alors appel de la décision. La Cour d'appel infirme le jugement du tribunal en ce qu'il a relaxé Monsieur Olivier L. Le juge d'appel condamne Monsieur L. à une amende de 3000 euros pour s'être rendu coupable d'accès et de maintien frauduleux dans un système informatique. Le dol général consiste dans la conscience qu'avait Monsieur L. de se trouver en possession d'informations, de données et de documents réservés à l'usage strictement interne de l'ANSES. Le dol spécial est le fait pour Monsieur L. de savoir qu'il n'était pas autorisé à accéder à cet extranet, qui se définit comme une extension des pages internes de l'organisme et par conséquent réservée exclusivement au personnel ayant reçu à cet effet un identifiant et un mot de passe pour l'accès. En l'espèce, il n'est pas besoin de dol spécial, c'est-à-dire que le dol général suffit. L'intention de nuire n'est pas recherchée. Seul, le fait d'avoir eu accès de manière frauduleuse, sans droit, occasionne l'infraction.

L'incrimination du hacking a également connu une évolution en Allemagne[217]. Dans cet Etat, avant 2007, seul l'accès illégal au système de données était sanctionné. La possession d'outils de hacking n'est pas encore une infraction en droit Allemand[218]. Cette disposition est à l'image du droit Danois où le simple fait de posséder des outils favorisant des intrusions dans les systèmes informatiques n'est pas une infraction en soi[219]. En d'autres termes, cette possession ne constitue pas une preuve de l'intention de commettre des intrusions informatiques illégales.

Le droit Danois va plus loin dans la mesure où le fait d'avoir eu accès à des sites de manière illégale, n'est réprimé qu'à la condition de représenter des atteintes graves comme par exemple le non-respect de règles comme la loi protégeant les droits d'auteurs.

---

[217] Cf. Comprendre LA CYBERCRIMINALITE, guide des pays en développement, Division applications TIC et cybersécurité, Département des politiques et stratégies, Secteur du développement des télécommunications de l'Union Internationale des Télécommunications, avril 2009.

[218] Article 202 a. du Strafgesetzbung (StGB: Code pénal allemand), Cf. **KOOPS BERT- JAPP** and **BRENNER Susan**, Cybercrime and jurisdiction : a global survey, the Hage TMC, Asser Press, 2006, Pays-Bas, p. 184.

[219] Cf. Article §21 du code pénal danois et Cybercrime and Jurisdiction, p. 161.

En ce qui concerne l'Angleterre, c'est l'accès intentionnel sans autorisation qui est incriminé mais il est exigé d'autres conditions nécessaires à la sanction. On peut en trouver trace dans le Computer Misuse Act[220] de 1990 encore applicable à ce jour[221] bien que le gouvernement britannique ait décidé de le reformer dans le but de l'adapter aux nouvelles formes de criminalité informatique en 2003[222]. Le Computer Misuse Act définit trois catégories d'accès frauduleux : il s'agit de l'accès non autorisé au matériel informatique , à la section 1 ; de l'accès non-autorisé avec l'intention de commettre ou de faciliter la commission d'autres infractions (c'est-à-dire des infractions pour lesquelles la loi prévoit des peines d'emprisonnement pour meurtre ou pour lesquelles la peine de prison est de 5 ans ou plus pour le délinquant récidiviste de 21 ans ou plus) à la section 2 ; et à l'accès non autorisé modifiant le matériel informatique à la section 3.

Chacune des sections citées est conditionnée : pour ce qui est de la section 1, il faut que celui qui commet l'infraction soit sur le territoire de la Grande Bretagne lors de la commission de l'accès non autorisé sur l'ordinateur attaqué ou que les données ou les programmes du matériel informatique considéré soient endommagés du fait de l'individu contrevenant à la loi. Ce sont les sections 4 et 5 qui apportent ces précisions. Pour la section 2, c'est-à-dire l'accès non autorisé avec l'intention de commettre ou de faciliter d'autres infractions, le Computer Misuse Act précise que l'exigence d'un lien significatif est écartée dès lors que l'acte relève de la compétence législative anglaise. Si dans sa nature, l'infraction est extraterritoriale, elle est possible sans aucun lien avec la Grande Bretagne[223].

---

[220] Le texte est disponible en ligne sur http://www.legislation.gov.uk/ukpga/1990/18/contents voir également Jurisdiction and the ambit of criminal law, p. 193-197. Ce texte est initialement plus une charte privée qu'une proposition gouvernementale de loi. Le besoin d'encadrement légal d'actes comme les intrusions informatique frauduleux était pressant en 1980 notamment à la suite de la décision *Gold et Schifren de 1988 :* R v Gold, Schifren [1988] 2 All ER 186, cf. p.295, Cybercrime and Jurisdiction, op. cit.

[221] Etude rédigée par **OLINET M**., l'Harmonisation des sanctions pénales en Europe, extrait d'actes du colloque de l'unité mixte de Recherche de droit comparé de Paris 5, société de législation comparée dirigée par Mme Delmas-Marty, DL 2003.

[222] cf. **BRENNER S**., Cybercrime and Jurisdiction p. 297, qui renvoie au meeting de CAROLINE FLINT, MP, Parliamentary Under Secretary, Home Officer Minister in speech made a EURIM meeting, 14 July 2003.

[223] cf. **HIRST**, Jurisdiction and the Ambit of the Criminal Law (Oxford University Press 2003), p. 194.

Le lien significatif dans le cas de la section 3 est la simple présence de l'accusé au lieu de commission de l'accès interdit ou le fait que la modification sur le système informatique ait lieu au Royaume Uni. Et cette précision ressort de la section 5. Alors que les deux premières catégories d'accès non autorisés nécessitent des modifications actuelles sur l'ordinateur, la troisième catégorie concerne la modification des contenus de l'outil informatique du type logiciels malveillants ou virus qui endommagent notamment l'ordinateur de manière temporaire ou permanente et pas spécialement sur le champ[224].

Il ressort de ce texte de loi anglais une remarque quant au contenu : le Computer Misuse Act réprime à la fois les intrusions frauduleuses ainsi que l'intention de l'accès non autorisé et il sanctionne les modifications intervenues, qui, elles, relèvent de la falsification et de la fraude ; les personnes qui s'adonnent à ces modifications de contenus n'étant pas celles habilitées à le faire. La Convention de Budapest aborde les fraudes et falsifications dans une seconde catégorie distincte des intrusions frauduleuses.

La seconde catégorie d'infractions cybercriminelles est relative à la falsification et la fraude informatiques. La falsification prend en compte plusieurs actes et est complexe dans sa définition. Il s'agit d'actes d'introduction, d'altération, d'effacement ou de suppression intentionnels et sans droit des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles[225]. Cette définition de la falsification informatique est complète dans la mesure où tous les actes susceptibles d'altérer la version originale des données y sont décrits. Elle peut être également qualifiée de complexe puisqu'elle envisage non seulement les actes mais également la nature, le contexte et les conséquences voulues par ces modifications engendrées.

La fraude informatique quant à elle répond à un contexte légèrement différent : il est question de *fait intentionnel et sans droit de causer un préjudice patrimonial à*

---

[224] C'est le cas des actes de cyber vandalismes par exemple cité par HIRST, idem.

[225] Cf. Article 7 titre 2 de la Convention sur la cybercriminalité du 23 novembre 2001.

autrui[226]. La notion de préjudice apparaît en plus des précédents critères que sont l'intention et le caractère sans droit de l'acte. Et il ne s'agit pas de n'importe quel préjudice. Il faut qu'il revête un caractère patrimonial. A titre illustratif, Monsieur PIRATE s'introduit dans le système informatique de la préfecture de police et réussit à modifier ses informations relatives à l'immatriculation de son véhicule en insérant les coordonnées de monsieur RIENFAIT. A la suite de ces modifications, monsieur PIRATE commet un excès de vitesse et son véhicule est flashé par les radars. Une contravention est envoyée mais c'est Monsieur RIENFAIT qui la reçoit. C'est dire qu'aux vues des changements, il apparaît que c'est l'adresse de Monsieur RIENFAIT qui est répertoriée et non celle du réel coupable de la contravention. Au moment de la contravention, par le biais d'un système informatique, une personne choisit les données (les informations) relatives à l'immatriculation d'un véhicule, et les change de sorte à induire en erreur les autorités compétentes pour sanctionner les contrevenants au code de la route. Le caractère patrimonial peut s'apprécier au regard du fait que la falsification entraîne le paiement d'une amende liée à l'excès de vitesse.

En droit français, la Cour de cassation a élaboré une étude sur la caractérisation du préjudice. Cette étude publiée au rapport de la Cour de cassation[227], différencie les préjudices extrapatrimoniaux des préjudices patrimoniaux surtout dans le domaine de la santé. De sorte que revêtent le caractère patrimonial, les préjudices liés au patrimoine ou aux biens de l'individu, et les dommages qui portent atteinte directement à la personne sont de l'ordre extrapatrimonial.

Que signifie le préjudice patrimonial dans cette qualification de la fraude informatique ?

S'il est pris sous l'angle de la possibilité de lui attribuer une valeur pécuniaire, le préjudice peut être qualifié de patrimonial. Dans ce cas, il faudrait envisager le préjudice

---

[226] Cf. Article 8, titre 2 de la Convention sur la cybercriminalité du 23 novembre 2001

[227] cf. Bulletin de la Cour de Cassation, rapport annuel 2007, troisième partie, « *étude sur la caractérisation du préjudice* ».

patrimonial comme l'atteinte portée à son image par le biais de la détérioration ou de la falsification des données à caractère personnel.

Peut-on dès lors considérer les données à caractère personnel comme un bien ou un élément du patrimoine des personnes ? Partant de cette qualification, quelle est la nature du préjudice de l'utilisation frauduleuse des données à caractère personnel ?

La réponse à cette question dépend de la nature ou de la qualification d'une donnée à caractère personnel. Certes, les données à caractère personnel constituent des éléments permettant d'identifier ou rendant identifiable une personne, mais quel est le sort qui leur est réservé ? S'agit-il de bien personnel ? Ou de bien au sens d'élément du patrimoine ? Si la donnée à caractère personnel est considérée comme directement liée à la personne, le préjudice qui découle de son utilisation frauduleuse sera certes évaluable en argent et par ricochet donnera droit à indemnisations, mais il s'agira d'un préjudice personnel. A l'inverse, si l'on considère que la donnée à caractère personnel est un bien au sens des biens du patrimoine de chaque individu, le préjudice sera patrimonial. Dans un article paru à l'édition générale du juris-classeur, Michel VIVANT traite des biens informationnels[228]. Quant à Pierre CATALA, il cite le précédent auteur dans son article sur la propriété de l'information dans les Mélanges Raynaud[229] en précisant que « *l'information prend une valeur particulière, une valeur qui se trouve être matérialisée dans un support faisant considérer alors cet objet nouveau aussi bien comme valeur, comme bien que comme valeur d'information* ».

S'agissant de la fraude informatique, en droit français notamment, c'est la loi n° 88-19 dite loi GODFRAIN du 5 janvier 1988 relative à la fraude informatique[230] qui répond à l'interrogation. Cette loi a été insérée dans le code pénal français et traite des dispositions relatives à l'intrusion et au maintien frauduleux dans un système informatique. Elle a d'abord été abrogée par la loi n° 32-1336 du 16 décembre 1992

---

[228] cf. **VIVANT Michel**, les biens informationnels, JCP 1984, I, 3132.

[229] cf. **CATALA Pierre**, Mélanges Raynaud, Paris, Dalloz 1985, p 97.

[230] Cf. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique publiée au JORF du 6 janvier 1988 page 231.

relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur[231] puis insérée dans le code pénal. Les articles 323-1 et suivants correspondent aujourd'hui à cette loi et ont quant à eux été modifiés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[232].

L'article 323-1 du code pénal constitue donc l'incrimination fondamentale sur laquelle repose l'essentiel de la loi du 5 janvier 1988 et répond à une revendication ancienne de la pratique et de la doctrine. Il dispose que : « *le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de 2 ans d'emprisonnement et de 30 000 euros d'amende ; lorsqu'il en est résulté soit la suppression ou la modification de données contenue dans le système, soit une altération du fonctionnement de ce système, la peine est de 3 ans d'emprisonnement et de 45 000 euros d'amende.*

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à soixante-quinze mille (75000) euros d'amende et à cinq (5) ans d'emprisonnement.

En application de cet article, la Chambre criminelle de la Cour de cassation a rendu un arrêt de cassation partielle en date du 3 octobre 2007[233]. La haute Cour a cassé la décision de la Cour d'appel de Lyon, qui n'a pas censuré une personne s'étant maintenue dans un système de traitement de données sans autorisation. Des faits de l'espèce, il ressort qu'en vertu d'un contrat qui la lie à une société, une personne employée par ladite entreprisse bénéficie d'un code d'accès à la base de données de l'entreprise. Ce code a été remis pour la durée du contrat de travail. Or, le contrat a par la

[231] Cf. Loi n° 32-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur parue au JORF n° 0298 du 23 décembre 1992 page 17568.

[232] Loi n° 2004-575 du 21 juin 2004, Journal Officiel de la République Française n°143 du 22 juin 2004 page 11168 texte n° 2.

[233] Cf. Cour de Cassation chambre Criminelle, 3 octobre 2007, Bulletin criminel 2007, n° 236.

suite été rompu. La bénéficiaire des codes d'accès les a conservées et les a utilisées pendant deux ans sans aucune autorisation ultérieure à la fin de son contrat. L'entreprise anciennement employeur s'est plaint de cette utilisation. La Cour d'appel saisie a estimé que l'accès était régulier et n'a dès lors pas condamné l'employé. La Cour de cassation casse cet arrêt et le renvoie devant une autre chambre. Cette décision qui casse et renvoie est importante dans la mesure où elle montre que malgré un accès régulier, les modifications ou les manipulations d'un système de traitement de données nécessitent également les autorisations pour les effectuer.

C'est à ce stade qu'il faut souligner que l'accès mais également le maintien dans une base de données sont encadrés. Le caractère régulier n'efface pas l'utilisation sans droit qui a par la suite eu lieu.

A l'instar du droit français, le droit Luxembourgeois dispose de l'article 509-1 inséré dans le code pénal de 1993 et modifié en 2000. Cette disposition prévoit une incrimination quant à la fraude informatique : « *quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.*

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1250 euros à 25.000 euros ».

En clair, la suppression ou l'altération des données s'analyse en une circonstance aggravante de l'infraction. Alors que le droit français est plus sévère en prévoyant des sommes jusqu'à quarante-cinq mille (45000) euros d'amende, le droit luxembourgeois se limite à vingt-cinq mille (25000) euros.

Il faut en outre observer que la peine privative de liberté maximale prévue est de 2 ans, au Luxembourg, en opposition au droit français qui punit jusqu'à 3 ans de prison celui qui aura commis une fraude informatique.

Au titre des catégories prévues par la Convention de Budapest, est cité *in fine* l'abus de dispositif, spécifié en plusieurs composantes à l'article 6. Il se dégage une

classification majeure de cette énumération : il faut qu'il y a ait eu *intention* et que la personne ait agi *sans droit*. En droit pénal français, l'intention n'est pas définie mais certains auteurs ont étudié cette notion en considérant l'intention comme *acte intentionnel, un acte conscient, voulu et accompli en vue d'un résultat précisément par son auteur*[234]. D'autres juristes comme Stéphanie BERTE, définissent l'intention comme « *la volonté tendue vers un but dont l'auteur connaît le caractère illicite et constitue en principe une des composantes de la majorité des infractions* [235]».

Sur la question, le professeur PRADEL est précis dans son article sur *les infractions relatives à l'informatique* en écrivant que l'intention suppose à la fois *un dol général et un dol spécial. Le dol général consistant dans la conscience de la volonté d'enfreindre la loi pénale. Le dol spécial quant à lui est la fraude elle-même c'est-à-dire la connaissance par l'agent de l'absence de droit à accéder à un système ou à s'y maintenir*[236].

Une autre classification ressort de ces incriminations générales mais elle est de moindre envergure puisqu'elle se contente de différencier l'intégrité des données de celle du système informatique. Sur ce point, la Convention de Budapest entend par « donnée informatique » *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction*[237].

Quant au système informatique, la Convention de Budapest l'a défini comme *« tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure*

---

[234] Cf. Recueil Dalloz 1993, p. 222, note de PORTHAIS et PRADEL sous le jugement rendu par la 16ème Chambre correctionnelle du Tribunal de Grande Instance de Paris en date du 23 octobre 1992 dans l'affaire du sang contaminé. Dans cette affaire, le tribunal a jugé que la contamination d'hémophile par le virus du SIDA lors de transfusions sanguines ne constitue pas un empoisonnement mais le délit de tromperie sur les qualités de la marchandise.

[235] Cf. **BERTE S.**, l'intention en droit pénal, Thèse sous la direction de **Pierrette PONCELLA**, Université de Paris 10, 2005. Voir aussi **PAGEAUD**, La notion d'intention en droit pénal, JCP 1950, I, n°876.

[236] Cf. **PRADEL**, les infractions relatives à l'informatique, revue internationale de droit comparé, 1990, volume 2, n°2, p815-828.

[237] Cf. alinéa 2 de l'article 1 titre 1 de la convention de Budapest du 23 novembre 2001.

ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données[238].

Cette différenciation au niveau de l'atteinte résulte du fait que chacune des deux composantes de l'ensemble donnée-système informatique peut être atteinte séparément. Les rédacteurs de la Convention ont de la sorte, réglé la question du cumul ou non des atteintes en cas d'infractions contre l'intégrité de l'un ou de l'autre.

Si un délinquant porte atteinte à l'intégrité d'une base de données sans pour autant s'en prendre au système informatique en lui-même, il sera possible pour le juge de le sanctionner uniquement du fait de cette infraction. Cette qualification permet de sanctionner des faits comme le *skimminig*, une variante du hacking, subtile en ce qu'il associe plusieurs infractions.

1- Une variante de fraude informatique : le skimming[239]

C'est la combinaison de la fraude informatique, du faux en informatique et du hacking. Il est question en effet d'une copie illégale de données de la piste magnétique d'une carte de paiement[240]. Les juges belges [241] ont été saisis pour connaître de tels faits dans les arrêts du tribunal correctionnel de Dendermonde respectivement de janvier et juin 2004. Le skimming est un faux en informatique dans la mesure où la création de fausses cartes bancaires ou la copie de celle-ci est mentionnée explicitement dans les travaux préparatoires de la loi sur la criminalité informatique comme exemple de ce type.

Il s'agit d'une fraude puisque le délinquant cherche à se procurer avec une intention frauduleuse, un avantage économique illégal, en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique

---

[238] Cf. l'alinéa 1 de l'article 1 de la convention de Budapest

[239] Cf. Lieutenant **FRESSINET Eric**, Le cybercriminel, portrait d'un profil type ? In Cybercriminalité, Cybermenaces et *cyberfraudes*, sous la direction d'Irène BOUHADANA et de Williams GILLES, IMODEV, p 39- 41, DL. Mars 2012.

[240] Revue du droit des technologies de l'information, n° 39/2010

[241]Corr. Bruxelles, 6 janvier 2004 ; Corr. Dendermonde, 7 juin 2004, *in* Aspects juridiques du paiement électronique, Kluwer, 2004, pp. 239 et 244

l'utilisation normale des données dans un système informatique (article 504 quater du Code pénal).

Enfin, le skimming est un hacking car à la suite de la fausse carte, les personnes poursuivies accèdent à un système informatique et s'y maintiennent, sachant pertinemment qu'elles n'y sont pas autorisées (article 550 bis du code pénal)[242].

Le skimming peut, outre la falsification des cartes, consister dans la falsification même du distributeur de billets de banque afin qu'il puisse bloquer les cartes. Ces dernières sont par la suite récupérées par les personnes à l'origine de la falsification du guichet. La police belge connaît ce type de pratiques le 8 juin 2010 et arrête deux bulgares avec leur matériel c'est-à-dire le lecteur de bandes magnétiques[243].

En janvier 2013, dans le cadre d'opérations contre les vols de codes secrets du type skimming, le bureau régional de la Securities Exchange Commission (SEC), autorité américaine de contrôle des marchés financiers met fin aux activités d'un trader escroc : Firas Hamdan, qui avait réussi à lever six (6) millions de dollars au sein de la communauté liba*naise de Houston entre 2007 et 2012. Firas Hamdan promettait à ses coreligionnaires libanais et druzes de mirifiques retours sur investissements de l'ordre de 30 % grâce, prétendait-il, a son programme de trading algorithmique de haute fréquence, spéculant sur la dette grecque. Il fera perdre en tout 1,5 million de dollars à trente-trois (33) investisseurs naïfs*[244].

Le Hacking peut servir de préliminaire à plusieurs autres infractions comme le piratage informatique, le spamming, l'usurpation d'identité numérique, le phishing pour ne citer que ces infractions. Ces comportements tout aussi répréhensibles les uns que les autres ont fait l'objet d'incrimination dans les lois européennes.

---

[242] Idem.

[243] Cf. Communiqué de presse de la police belge disponible en ligne : http://www.polfed-fedpol.be/presse/presse_detail_fr.php?recordID2=1944; compléter avec **BAESELEN Xavier,** la réponse écrite du ministre de l'intérieur belge sur le phénomène du skimming en Belgique : cf. Chambre des représentants de la Belgique, 4e session de la 52e Législature, question écrite n° 0477, du 22 février 2010.

2- Le piratage informatique

Qu'est-ce que le piratage informatique ? Est-ce l'utilisation des données ? Est-ce uniquement la dénaturation des informations dérobées dans un système informatique ? S'agit-il des actes modifiant ou altérant les contenus de systèmes informatiques auxquels les auteurs auraient eu frauduleusement accès ? Est-ce enfin la suppression des informations contenus dans les systèmes informatiques ?

Le dictionnaire Le Robert définit le pirate comme *un aventurier qui court les mers pour piller les navires*[245]. De manière générale, il s'agit *d'un individu sans scrupule qui s'enrichit aux dépens d'autrui*. Pirater de manière générale, c'est reproduire (une œuvre) illégalement et le même dictionnaire donne l'exemple d'un logiciel piraté.

S'agissant du piratage informatique, il consiste par analogie dans le fait de reproduire illégalement une œuvre numérique. Le piratage informatique renvoie à la contrefaçon liée à l'informatique mais pas seulement. Le piratage comprend à la fois des manœuvres frauduleuses sur le système informatique lui-même notamment (des logiciels) mais également le fait de dérober les œuvres et les données informatiques.

A titre d'illustration, le 25 novembre 2012, des hackers s'introduisent dans le système informatique de l'Agence Internationale de l'Energie Atomique pour dérober des informations confidentielles. Cette opération est un piratage informatique.

Les données dérobées étant stockées sur le serveur de l'agence[246] avec un accès autorisé uniquement à des personnes habilitées et par conséquent fermé à l'accès du public.

Le piratage informatique n'est pas un terme prévu par la Convention dite de Budapest. Compte tenu de la définition de cette pratique, elle fait partie de plusieurs infractions : le piratage en lui-même n'est pas isolé, il est le commencement d'exécution des actes

---

[244] Cf. Journal Bloomberg news du 30 janvier 2013. Compléter avec **J-F. GAYRAUD**, Le Nouveau Capitalisme criminel: Crises financières, narcobanques, trading de haute fréquence, éditions Odile Jacob, 2014.

[245] Le Robert, Dictionnaire pratique de la langue française, édition France Loisirs, Paris 2005, p 1277.

[246] Les faits remontent au 25 novembre 2012, l'information est diffusée par la Radio France International, cf. : http://www.rfi.fr/europe/20121127-exclusivite-rfi-scientifiques-aiea-danger-piratage-informatique-internet-nucleaire-israel-iran.

comme l'interception illégale, il est intégré à la falsification informatique, infraction de laquelle il est le plus proche en termes d'actes constitutifs.

S'agissant des piratages informatiques contre les œuvres protégées par la propriété intellectuelle par exemple, la Convention de Budapest, leur réserve la dernière catégorie[247] : il s'agit de la catégorie des infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Les droits connexes comprennent les droits reconnus aux artistes interprètes, chanteurs ou d'autres œuvres quant à leurs prestations. Il s'agit également de droits reconnus aux producteurs d'enregistrements sonores, aux organismes de radio - diffusion et de télévision. Ces droits sont assimilés au droit d'auteur mais ont la particularité d'être limités dans le temps ou dans leur portée[248].

Le piratage informatique englobe les différents actes allant à l'encontre des obligations contenues dans plusieurs conventions propres au respect de la propriété industrielle et aux droits voisins comme par exemple le droit d'auteur.

Dans cette catégorie les références sont faites aux Conventions et accords suivants :

- l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques[249]

- l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI)[250] sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de

---

[247] Cette catégorie correspond à l'article 10 de la convention et il revient aux termes des dispositions de l'article à chaque Etat de prendre les mesures législatives nécessaires (…).

[248] Voir le site de l'office européen du droit d'auteur : http://www.eucopyright.com/fr/quentend-on-par-droits-connexes ; détails de la différence entre droits d'auteur et droits connexes, cf. l'ABC du droit d'auteur, rédigé sous la supervision de **PETYA TOTCHAROVA** et **EMILE GLELE**, Section de la Diversité des expressions culturelles, UNESCO, Paris, 2010.

[249] L'acte de Paris apporte des ajouts à la convention de Berne, c'est pourquoi il est rattaché à cette convention. Il figure dans la base de données de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI).

[250] L'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce **(**ADPIC) constitue l'Annexe 1C de l'Accord de Marrakech instituant l'Organisation mondiale du commerce. Il est entré en vigueur depuis le 1er janvier 1995, et disponible sur le site de l'OMC : http://www.wto.org/french/docs_f/legal_f/27-trips.pdf

tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

Cet accord est un acte multilatéral autour de trois grands axes : le premier axe concerne les normes c'est-à-dire les différentes protections et de leur durée pour chacune des composantes de la propriété intellectuelle ; le second axe est relatif aux moyens de faire respecter les droits c'est-à-dire les mesures et les procédures pour corriger les atteintes portées ; et enfin comme troisième axe les modes de règlements de conflits.

- la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome)[251]

- le Traité de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. Peut ainsi être qualifié de piratage informatique, le fait pour un individu de détourner via les réseaux informatiques, des œuvres d'art vendues en ligne et de se les approprier pour les revendre à des prix dérisoires.

Autre exemple de piratage, le fait pour des individus de copier de manière illégale[252] des logiciels commercialisés par des éditeurs de logiciels et de les utiliser ou de les revendre via des réseaux informatiques. Compte tenu de l'ensemble des normes impliquées dans ce type d'infraction, il apparaît cohérent de répertorier les actes par catégories. C'est ce choix qu'a opéré le législateur français lorsqu'il classifie et intègre à chaque catégorie les actes qualifiables de contrefaisant en fonction d'un droit de propriété intellectuelle précis.

Si d'une manière générale, la contrefaçon consiste dans le fait d'imiter une œuvre déjà existante et de la vendre à une valeur moindre par rapport à celle qui lui est attribuée

---

[251] Convention publiée à la STE n° 153.

[252]La copie est illégale parce qu'ils n'ont aucun droit de copie dans la mesure où ils ne paient rien. Seul l'utilisateur qui paie des droits aux éditeurs de logiciels acquiert une licence pour profiter du logiciel acheté.

sur le marché, il peut également s'agir de modifier une œuvre, qu'elle soit musicale ou de toute autre forme, sans pour autant avoir le droit qu'a le créateur ou le concepteur ou encore l'auteur de l'œuvre. Le but de la contrefaçon est de tromper et de tirer profit d'une chose dont on n'est pas le concepteur. En ce qui concerne la contrefaçon en ligne, elle est surtout pratiquée sur les œuvres d'art, les marques, les logiciels, les œuvres musicales. Elle peut également être pratiquée à l'encontre de sites internet déjà existants.

Outre cette évolution législative, il faut mentionner la création d'un délit de contrefaçon en ligne. Cette nouvelle incrimination permet de s'arrêter sur les œuvres contrefaites par le biais du réseau numérique. En quoi consiste la contrefaçon en ligne?

3- La contrefaçon en ligne

La contrefaçon en ligne rejoint les techniques de piratage de logiciels susvisées mais surtout soulève les questions relatives à l'utilisation des sites internet pour écouler des marchandises contrefaites et ce, dans le but de tromper plus aisément les potentiels acheteurs. En effet, derrière leurs écrans, il est difficile pour les consommateurs de vérifier la véracité ou l'authenticité des qualités de la marchandise proposée. Or, il se trouve de manière générale que ces qualités sont fausses ou mensongères puisque les vendeurs ont copié des marques existantes sur le marché, pour les revendre moins chère que les marchandises produites par les vraies marques. Ainsi, hormis la falsification ou l'imitation de logiciels pour tromper les consommateurs, des personnes s'adonnent à des actes de contrefaçons par l'intermédiaire des outils informatiques. Il s'agit réellement de l'ensemble des atteintes à la propriété intellectuelle.

Cet ensemble d'infractions est sanctionné en droit français par le décret 2006-1763 du 23 décembre 2006[253]. Ce décret contient des dispositions relatives à la répression pénale de certaines atteintes portées au droit d'auteur et aux droits voisins.

[253] Décret n° 2006-1763 du 23 décembre 2006 relatif à la répression pénale de certaines atteintes portées au droit d'auteur et aux droits voisins paru au JORF n° 302 du 30 décembre 2006 page 20161 texte n° 118.

Ainsi l'article 1 du décret précise « dans le chapitre V du titre III du livre III du code de la propriété intellectuelle, il est ajouté, après l'article R. 335-2, deux articles R. 335-3 et R. 335-4 ainsi rédigés : « Art. R. 335-3. - Est puni de l'amende prévue pour les contraventions de la quatrième classe le fait de:

1° *détenir en vue d'un usage personnel ou d'utiliser une application technologique, un dispositif ou un composant conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace mentionnée à l'article L. 331-5 du présent code qui protège une œuvre, une interprétation, un phonogramme, un vidéogramme, un programme ou une base de données* ;

« 2° *recourir à un service conçu ou spécialement adapté pour porter l'atteinte visée* à l'alinéa précédent. Ces dispositions ne s'appliquent pas aux actes qui ne portent pas préjudice aux titulaires de droits et qui sont réalisés à des fins de sécurité informatique ou à des fins de recherche scientifique en cryptographie.

Selon l'article R. 335-4, *est puni de l'amende prévue pour les contraventions de la quatrième classe le fait* de :

1° « *détenir en vue d'un usage personnel ou d'utiliser une application technologique, un dispositif ou un composant conçus ou spécialement adaptés pour supprimer ou modifier un élément d'information visé à l'article L. 331-22 et qui ont pour but de porter atteinte à un droit d'auteur, à un droit voisin ou à un droit de producteur de base de données, de dissimuler ou de faciliter une telle atteinte »* ;

2° « *recourir à un service conçu ou spécialement adapté pour porter, dans les mêmes conditions, l'atteinte visée à l'alinéa précédent. Ces dispositions ne s'appliquent pas aux actes qui ne portent pas préjudice aux titulaires de droits et qui sont réalisés à des fins de sécurité informatique ou à des fins de recherche scientifique en cryptographie.* ». En clair, les amendes prévues au titre des sanctions dans ces articles sont des peines de l'ordre des contraventions, uniquement prises pour des infractions. Il faut donc isoler les intrusions effectuées en vue de desceller des failles des systèmes de sécurité pour informer l'entreprise de celles qui ont pour objectif de commettre l'infraction consistant à diffuser des informations censées être confidentielles.

C'est dans cette dernière optique que s'inscrit l'arrêt de la chambre criminelle de la Cour de cassation du 27 octobre 2009[254]. Des faits de l'espèce, il ressort que Monsieur X, gérant de la société XX Consulting, spécialisée dans le conseil en sécurité informatique a diffusé sur le portail de la société, des écrits directement visibles sur le site et accessibles à tous. Ces écrits permettaient d'exploiter des failles de sécurité informatique. Monsieur X a été condamné par les juges du fond à une amende de 1000 euros. S'estimant lésé, il se pourvoit en cassation en arguant d'un motif légitime tiré de la volonté d'information. La Cour de cassation enseigne dans cet arrêt que la volonté d'information ne saurait légitimer la violation d'un système contenant des informations censées être confidentielles.

En effet, les juges de la Haute Cour ont décidé que : « *qu'il ne peut valablement arguer d'un motif légitime tiré de la volonté d'information, dès lors que, du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ; attendu qu'en l'état de ces énonciations, abstraction faite du motif surabondant relatif aux antécédents judiciaires du prévenu, et dès lors que la constatation de la violation, sans motif légitime et en connaissance de cause, de l'une des interdictions prévues par l'article 323-3-1 du code pénal implique de la part de son auteur l'intention coupable exigée par l'article 121-3 du même code (…)* ».

Dans cette décision de justice, l'accent est mis sur le motif légitime pour diffuser des informations professionnelles confidentielles. Cette décision pourrait être perçue par certains auteurs comme une interdiction de révéler des failles de sécurité[255]. La notification des failles de sécurité devenue depuis 2009 une obligation encadrée par le législateur mais avec certaines réserves et dans des conditions précises.

---

[254] Cf. Chambre criminelle de la Cour de cassation 27 octobre 2009, n° 09-82.346, bulletin n° 177.

[255]Certains auteurs comme CANEVET (S), l'ont perçu comme tel, pour voir son commentaire http://www.canevet.org/spip/dist/spip.php?article184&lang=en

Un reproche pourrait être fait à la loi puisqu'elle semble accorder des cas de diffusion de ce genre d'informations susceptibles de faciliter le piratage de données. Quels sont les cas justifiant un contournement de la règle ? Quel motif légitime peut-on brandir pour diffuser des informations confidentielles ? Le recours à cette notion peut intriguer. Et pourtant, pour des raisons de santé, de sécurité ou de défense des intérêts et de la sûreté de l'Etat, des informations confidentielles personnelles sont parfois communiquées. Il pourrait donc s'agir d'intérêt supérieur à la protection de l'intimité d'une personne. A titre illustratif, l'imminence d'un risque de contagion ou de propagation d'une maladie meurtrière ou d'une bactérie est de nature à justifier la divulgation de données personnelles contenues dans un système de données par exemple.

Dans le cadre d'un échange à la suite d'une mission ministérielle sur la cyber-contrefaçon entre la France et la Chine, les professeurs Pierre SIRINELLI et Bertrand BROCHANT ont clairement pu démontrer l'orientation que doit prendre la lutte contre la contrefaçon en ligne ; ils ont de ce fait identifié les défis qu'implique de relever cette autre forme de cybercriminalité. Selon eux, **«** *la lutte conte la cyber-contrefaçon exige plusieurs défis dont trois principaux d'ordre technique, méthodologique et idéologique. Le premier consiste à maîtriser et comprendre parfaitement le fonctionnement d'internet et les business models mis en place.*

Le second défi est méthodologique (…) et tient à l'intégration d'autres utilisateurs d'internet tels les prestataires techniques d'internet, les transporteurs express ou encore des spécialistes de la veille sur internet. Le troisième défi est d'ordre idéologique et ce n'est pas le moindre quand l'irrationnel rejoint le virtuel ! Dès lors qu'on avance dans la volonté de réguler les flux illicites sur la toile, on se fait au mieux considérer comme rétrograde et passéiste, au pire accuser de menées liberticides. »[256]

L'accord en matière de protection des droits de propriété intellectuelle a été signé à Pékin le 7 juillet 2009 entre le Comité national anti-contrefaçon français (Cnac) et

[256] http://www.bernard-brochand.fr/9-JUILLET-2009-Accord-franco.html

l'Administration chinoise pour l'Industrie et le Commerce[257]. Depuis 2007, une équipe d'experts essaie de mettre en place une législation contre la contrefaçon numérique. Durant plusieurs années cet acte en construction a été gardé secret et a fait l'objet de nombreuses critiques notamment du fait de l'ambiance secrète de son élaboration.

L'acte a finalement été dévoilé par la Commission européenne dans une version consolidée publiée par la Commission européenne[258]. Le traité est dénommé Anti - Counterfeiting Trade Agreement (ACTA) et a pour objectif de protéger les emplois perdus du fait de la contrefaçon des produits[259].

Il faut souligner les nombreuses critiques portées par les défenseurs de la liberté d'expression notamment en Pologne où s'est tenue une grande manifestation contre la signature dudit traité. Les incertitudes qui planent sur la compatibilité de cet accord avec le Traité UE, conduisent la Commission européenne à le soumettre à la Cour de Justice. En attendant le verdict de la Cour, les députés ont travaillé et quatre commissions à savoir la commission des affaires juridiques, la commission de l'industrie, des libertés civiles et du développement ont voté pour le rejet de l'ACTA. Quant à la commission du commerce international, compétente sur la question, elle tient compte de ces différents avis pour trancher. Le rapporteur, Monsieur David Martin a formulé la recommandation de rejeter l'accord. Selon cet eurodéputé, le traité ACTA n'est pas suffisamment précis sur les questions relatives à la protection des droits sur la propriété intellectuelle et les sanctions que prévoit cet accord ne sont pas suffisamment claires pour éviter les *interprétations intempestives*[260].

---

[257] Voir le site officiel du Comité national anti-contrefaçon français : http://www.contrefacon-danger.com/publication/content/ART_3_236.php

[258] Version consolidée du Traité ACTA, consulté sur http://www.international.gc.ca

[259] Déclaration du commissaire européen **KAREL DE GUCHT**, en charge du commerce, lors d'un communiqué de presse

[260] Cf. Projet de recommandation sur le projet de décision du Conseil relative à la conclusion de l'accord commercial anti-contrefaçon entre l'Union européenne et ses États membres, l'Australie, le Canada, la République de Corée, les États-Unis d'Amérique, le Japon, le Royaume du Maroc, les États-Unis mexicains, la Nouvelle-Zélande, la République de Singapour et la Confédération suisse (12195/2011 – C7-0027/2012 – 2011/0167(NLE)) et pour une version en ligne cf. : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-

Le 22 février 2012, la Cour de Justice a été saisie de la question de la compatibilité de l'accord ACTA. C'est sur le fondement des articles 207 et 208 du Traité UE que le Parlement européen est saisi pour statuer sur l'entrée en vigueur des accords internationaux. Le 4 juillet 2012, le Parlement européen a tranché sur la question du rejet de la signature de cet acte anti-contrefaçon[261] sans attendre la réponse de la Cour de justice. Par conséquent, l'Union Européenne et ses Etats membres, sont écartés pour la signature de cet accord. Seuls les signataires d'origine que sont l'Australie, le Canada, les Etats- Unis, le Japon, le Mexique, le Maroc, Singapour, la Nouvelle – Zélande et la Corée du Sud y sont parties contractantes.

L'importance des intrusions frauduleuses montre que ces infractions méritent d'être encadrées par les législateurs. Elles ne sont pas les seules pratiques qui méritent l'attention.

La consultation fréquente ou pas de sa messagerie internet (boîte mail) permet de se rendre compte d'interlocuteurs généralement inconnus adressant des messages, pour la plupart, non sollicités, d'où leurs appellations de courriers indésirables. C'est l'invasion des messageries électroniques par des messages non sollicités. Quel est l'encadrement légal prévu face à ces pratiques ?

b- Le spamming : l'invasion des messageries électroniques

Le spamming consiste dans le fait d'inonder les boîtes mails de courriers indésirables. Cette infraction existe depuis 1978 aux Etats - Unis grâce à l'américain Gray THUREK qui a récupéré l'ensemble des adresses de 600 utilisateurs du réseau ARPANET[262] pour leur envoyer un mail identique[263].

486.174%2B02%2BDOC%2BPDF%2BV0//FR

[261] Le parlement a rejeté l'Accord Commercial Anti-contrefaçon par 478 voix pour son rejet, 39 voix contre et 165 abstentions : cf.http://www.europarl.europa.eu/news/fr/pressroom/content/20120217BKG38488/html/L'ACTA-examin%C3%A9-au-Parlement-europ%C3%A9en

[262] ARPANET est le premier réseau numérique mis en place dans le courant des années 70.

[263] Journal Libération du 10 août 2007, deuxième édition, n° 8167.

Alors que les Etats- Unis se sont dotés d'une législation contre les spams avec la loi Can-Spam act[264] (Controlling the assault of non-solicited pornography and marketing act) entrée en vigueur le 1er Janvier 2004, la France n'a pas de texte spécial contre les spams.

Sur la question, la Direction Française du Développement des Médias a réalisé une étude sur le spam et le courrier électronique[265]. Il n'y a pas de législation qui réprime explicitement le spamming.

Par contre qu'il s'agisse du niveau international, européen ou de la loi française, plusieurs dispositions pénales sont contenues dans divers textes et sanctionnent cette pratique de manière indirecte. Quant à la Convention sur la cybercriminalité signée par les Etats membres à Budapest en 2001, elle ne fait pas de mention explicite du spam. C'est par référence à d'autres délits contenus dans cette Convention que le spamming est sanctionné. Il faut chercher ailleurs la répression du spamming. Le spamming est considéré comme un envoi massif de courrier non sollicité. Il est donc réprimé sous l'angle du manque de consentement pour la diffusion et l'utilisation des données des individus.

C'est pourquoi, la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données contient des dispositions précises sur le consentement donné par les particuliers pour l'utilisation de leurs données notamment dans le but de recevoir des messages publicitaires. L'article 7 de la directive prévoit que : « *le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement* », le consentement étant défini par l'article 2 du texte comme « *la manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement* ». L'accent est clairement mis sur le caractère du consentement donné : « indubitablement ». Il ne doit subsister aucun doute. Or, dans la pratique du spamming,

---

[264] Cf. S. 877, Controlling The assault of non solicited pornography and marketing Act of 2003, 15 USC 7701-03 and 18 USC 1307

[265] La législation française du spam consultée sur http://www.ddm.gouv.fr

en règle générale, le destinataire n'a jamais sollicité les messages qu'il reçoit. En cela, il y a violation à son droit de ne pas recevoir des messages et surtout, il y a une violation à son consentement.

En complément de la directive sur la protection des données des personnes, la directive européenne n°2002/58 du 12 juillet 2002 relative à la vie privée et aux communications[266] contient des dispositions, transposées en droit français grâce à la Loi sur la Confiance en l'Economie Numérique dite LCEN du 21 juin 2004[267] , permet de réprimer le spamming. Cette loi fait une référence aux sanctions prises contre la criminalité informatique.

Il est toutefois dommage que la loi LCEN précise en son article 22 que *les sanctions pénales soient fixées par le Conseil d'Etat*. Ce détail aurait tout simplement dû figurer dans l'article concerné et faciliter ainsi le caractère coercitif de cette disposition pénale.

C'est la raison pour laquelle, il est fait recours à d'autres textes pour punir les auteurs de spam. Il s'agit entre autres du code de la consommation dans lequel il est possible de lire : « *l'usage abusif de courrier électronique est interdit à plusieurs titres selon la nature et les conditions de l'envoi. Est notamment interdit en France tout courrier électronique envoyé à des fins de publicité mensongère : la sanction est de 2 ans d'emprisonnement, et/ou 37500 euros d'amende*[268] ». Cette disposition légale interprétée a contrario signifie qu'il est possible d'abuser de courrier électronique à condition que l'envoi massif n'ait pas pour objectif de tromper les destinataires. Il est préférable, à notre sens, de s'interroger sur le nombre d'envois de courriers électroniques à partir duquel on peut conclure à un envoi abusif. La notion du caractère abusif doit être comprise dans le

---

[266] Directive européenne n° 2002/58 du 12 juillet 2002 parue au Journal Officiel des Communautés Européenne n° L 201 du 31/07/2002 p. 0037 – 0047 modifiée par la Directive n° 2009/136/CE du 25 novembre 2009 publiée au JOUE du 18 décembre 2009, L337/11.

[267]Loi n° 2004-575 du 21 Juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004 page 11168 texte n° 2.

[268] Article L 121-1 du code de la consommation français

sens de la contravention à la règle légale selon laquelle, il faut au préalable obtenir le consentement du destinataire du message avant de lui faire parvenir des publicités.

Au Royaume uni, la directive 2002/58 a été transposée dans le dispositif législatif par la loi de 2003 entrée en vigueur le 11 décembre 2003 appelée « Privacy Regulations and Electronic Communications ». Elle contient des dispositions restrictives quant au spam, aux appels téléphoniques indésirables, à l'envoi des fax non sollicités à la fois à des entreprises ou des personnes privées[269].

D'une manière générale est caractérisé d'abusif, le fait d'user de manière excessive ou immodérée d'une chose ou d'un bien. C'est aussi l'usage mauvais d'une chose, d'un droit, d'une autorité.

En doctrine française, Emmanuelle LAJUS-THIZON a essayé de définir l'abus dans sa thèse « l'abus en droit pénal » en faisant plusieurs références de la notion. Elle a considéré l'abus en tant que *composante d'un délit, dont la définition, par exemple, mentionne un abus de pouvoir, un abus d'autorité ou l'abus d'une qualité vraie*, mais également, en tant qu'*élément constitutif à la qualification même du comportement considéré (abus de confiance, abus de faiblesse et, en dehors du code pénal, abus de biens sociaux, abus de position dominante, abus de dépendance économique ' sans oublier, l'abus de blanc-seing.*[270] En s'appuyant sur les approches de l'abus développées par Madame LAJUS-THIZON, le fait d'outrepasser le consentement du destinataire des messages publicitaires, que ce dernier n'aurait pas sollicité, constitue un abus entraînant les sanctions édictées par la loi.

Les peines encourues au titre du spamming sont des peines de prison et une amende pécuniaire. Compte tenu de la gravité, ces peines sont considérables et devraient parvenir à dissuader les « spammeurs ». D'autant plus que la tenue des fichiers d'adresses est également soumise à déclarations sous peine de sanctions. En effet, la loi Informatique et

---

[269] Cf. The Privacy and Electronic Communications (EC Directive) Regulations 2003 et pour une version en ligne: http://www.ppsi.gov.uk/si/si2003/uksi_20032426_en.pdf.

[270] cf. **LAJUS-THIZON E**., L'abus en droit pénal, thèse de droit, volume 105, Collection Nouvelles bibliothèques de thèses, Dalloz, avril 2011.

Libertés sanctionne le défaut de déclaration des fichiers d'adresses de messagerie. L'article 23 de ladite loi punit de *cinq ans d'emprisonnement et de trois cent mille (300000) euros* d'amende tout défaut d'accomplissement des formalités préalables au traitement automatisé d'informations nominatives. Cette sanction est contenue dans le code pénal à l'article L 226-18. A ce titre, la Chambre Criminelle de la Cour de cassation a sanctionné la société Alliance Bureautique Service (ABS) pour l'envoi de spam à des clients, qui n'avaient aucunement sollicité ces courriels[271]. Il ressort de l'espèce que, la société ABS avait eu recours à un robot mail pour collecter des adresses mail de particuliers en vue de leur envoyer des courriels publicitaires à l'aide du logiciel Free prospect. Or, ces destinataires n'avaient pas sollicité ces messages et n'avaient à aucun moment donné leur consentement pour l'usage de leurs adresses. La Cour d'appel saisie a condamné la société pour envoi de messages non sollicités sur le fondement de l'article 226-18 du code pénal. La société s'est pourvue en cassation au motif qu'il n'avait été procédé à aucun enregistrement. La Cour de cassation a rejeté le pourvoi en cassation. Pour ce faire, elle a considéré que : « *constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques d'une part et d'autre part, est déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition.* ». L'enseignement de cet arrêt est celui de l'importance du consentement des particuliers, peu importe l'enregistrement ou non dans un fichier. Le support n'est pas le critère caractéristique de l'infraction. Il suffit qu'il y ait eu collecte frauduleuse, et absence de sollicitation des courriers de la part des destinataires pour que l'infraction soit constituée.

Il apparaît que le spamming est sanctionné sous l'angle du non-respect des modalités de traitement des données. Il est question de punir un manquement aux obligations de

---

[271] Cf. Cour de cassation, Chambre criminelle, 14 mars 2006, n° de pourvoi 05-83423, Bulletin criminel 2006,

n ° 69 p. 267.

recueil de consentement des personnes avant la collecte de leurs données. C'est la collecte frauduleuse, c'est-à-dire en marge des règles qui est punie.

En effet, le spam est considéré comme tel dans la mesure où la personne qui le (le courrier indésirable) reçoit n'a pas donné son autorisation pour que son adresse mail (qui est une donnée personnelle) fasse partie de la liste des destinataires. Il faut souligner à ce sujet que les spammeurs utilisent des moyens comme des spamware[272] ou des aspirateurs d'adresses mail pour obtenir les adresses des destinataires de leurs messages non sollicités. C'est pourquoi, le spammeur est puni sur le fondement d'une collecte frauduleuse.

Les sanctions encourues pour le spamming sont l'amende pécuniaire et la peine de prison. Le montant de l'amende varie en fonction de l'Etat de l'Union considéré. Ainsi, en Roumanie, la condamnation maximale est de cinq cents (500) euros, en Espagne elle s'élève à trois cent mille (300 000) euros, en Italie, un juge a sanctionné un spammeur à verser cinq cent soixante-dix mille (570 000) euros d'indemnités et enfin aux Pays-Bas, l'amende peut atteindre 1 million d'euros. En France, la peine de prison peut aller jusqu'à cinq (5) ans avec une amende pouvant atteindre trois cents mille (300 000) euros.

Ce sont les plaintes des internautes qui sont à l'origine de la mise en place des sanctions contre le spam. Ces plaintes ont permis aux juges de trancher des cas de spamming et des associations de prévention et d'analyse de ces spam ont vu le jour. En l'occurrence Signal spam en France, Eco Verband en Allemagne favorise le signalement des spam par les internautes.

Le spamming est une variante des infractions liés à l'ordinateur tout comme le phishing et ses dérivés.

c- Le *phishing* et l'usurpation d'identité

[272]Le spamware est un logiciel permettant d'envoyer des spam mais également d'aspirer des adresses de messagerie électroniques de manière à générer une liste d'adresses de destinataires de spam.

Le phishing et l'usurpation d'identité numérique sont deux infractions qui se combinent facilement en ce que la première permet dans certains cas d'aboutir à la seconde.

1- Le phishnig

Le phishing ou hameçonnage est issu d'une contraction de fishing (pêcher) et phreaking (piratage des centraux téléphoniques). Le phishing nécessite plusieurs étapes à savoir la constitution d'une base de données à partir de création de forums de discussion[273]. Ces forums vont permettre de récupérer plusieurs adresses mails. Cette opération est réalisée en parallèle de l'achat de kits (c'est-à-dire des pièces détachées, des équipements nécessaires ou encore des outils) de phishing usurpant l'identité de grandes enseignes et spécifiquement des banques. Ces kits sont acquis sur des espaces illégaux et imitent parfaitement l'interface graphique de l'entité visée. Les sites sont par la suite installés sur des espaces d'hébergement gratuits à l'étranger[274].

Il s'agit d'une technique de fraude largement révélée en France lors de la grande tentative d'escroquerie du 7 mars 2006 réalisée envers les clients de la banque LCL[275]. A cet exemple, s'ajoutent les opérations de phishing contre les clients EDF[276] en janvier 2013,

---

[273] Les forums de discussion sont des plateformes mises en ligne et qui permettent aux internautes d'échanger sur des thèmes précis, ou encore sur des difficultés rencontrées dans un domaine de leur quotidien.

[274] Etude rédigée par le Centre d'Etudes Informatiques et Stratégiques (CEIS)

[275] Précis Dalloz, C. Feral-Schuhl, page 841.

[276]Cf. Journal l'Expansion.com avec l'Agence Française de Presse (AFP) « *les clients d'EDF cibles d'une arnaque de phishing géante* »publié le 31/01/2013 et voir pour une version en ligne : http://lexpansion.lexpress.fr/entreprises/les-clients-d-edf-cibles-d-une-attaque-de-phishing-geante_1412291.html.
Voir également Journal Le Figaro du 31 janvier 2013 « *de faux courriels EDF par centaines de milliers* » publié en ligne : http://www.lefigaro.fr/conso/2013/01/31/05007-20130131ARTFIG00438-des-faux-courriels-edf-par-centaines-de-milliers.php: les clients EDF recevaient de faux courriels comportant le logo d'Edf Bleu Ciel, leur demandant de remplir des formulaires en ligne afin de régler via internet le défaut de paiement de leur facture à la suite d'un refus de paiement opposé par leur banque.

et d'autres actes du même type dirigés contre des utilisateurs du système de paiement en ligne *Paypal*[277] en France en janvier 2014, sur le site de vente en ligne le Bon Coin.

La technique de *phishing* consiste pour le délinquant à adresser un mail à un ou plusieurs internautes (comme c'était le cas des clients de LCL) l'invitant à se connecter à un site, qui est en réalité la parfaite copie du site connu de l'internaute (en général sa banque) et à lui réclamer sous divers prétextes (vérification des clients) des informations confidentielles (coordonnées bancaires)[278]. En termes plus précis, le vocabulaire des techniques de l'information et de communication définit le phishing comme *une technique de fraude visant à obtenir des informations telles que des mots de passe ou de numéros de cartes de crédit au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales*[279].

Le phishing est réprimé en France mais cette répression n'empêche pas les délinquants d'en commettre davantage. Dès lors comment rendre dissuasives les sanctions édictées par la loi ? Cette question peut paraître curieuse si l'on émet des hypothèses relatives aux difficultés pour identifier ces délinquants. Serait-ce une justification à la commission grandissante de cette forme de crime ? En guise de réponse, il faut souligner qu'il est possible d'identifier une personne connectée grâce à ses adresses IP. Le réel problème qui se pose est de savoir si le fait que l'hébergeur ou le fournisseur d'accès communique les identités des personnes connectées suffit à les identifier réellement. Il est possible, et cela arrive de plus en plus, que le délinquant utilise de fausses identités.

Il existe d'ailleurs des systèmes rendant impossibles (même pour le fournisseur d'accès) les identifications personnelles. Il est dans ce cadre fait appel aux procédés

---

[277] Cf. V. **NICOLAS**, Phishing : l'arnaque Paypal qui se propage sur le Bon Coin, article du 15 janvier 2014 disponible en ligne sur http://rue89.nouvelobs.com/2014/01/15/phishing-larnaque-paypal-propage-bon-coin-249056.

[278] Idem

[279] Définition parue au JO du 12 février 2006.

d'anonymisation[280] des identifiants internet utilisés ou encore de techniques de cryptage qui masquent les composantes permettant de retracer les moments de connexion ou les personnes connectées.

Dans le cadre des opérations de *phishing*, le Tribunal de grande instance de Strasbourg punit dans son jugement[281] du 26 mai 2009 Monsieur S. pour plusieurs opérations frauduleuses : l'utilisation des marques Footlocker, Uknow, Boncoup, sans aucune autorisation de leur propriétaire d'une part , des vols des données bancaires de diverses personnes par l'intermédiaire de faux sites en ligne d'autre part et enfin d'utilisation des données confidentielles de cartes bancaires pour le paiement en ligne de diverses commandes sur internet après l'obtention de ces données par des moyens frauduleux. Les sanctions vont de la peine de prison à la publication du jugement sur les sites des enseignes concernées. Il s'agit *d'une peine de prison de dix-huit (18) mois d'emprisonnement avec sursis , d'une amende délictuelle de trois mille euros (3000 €) pour les infractions d'imitation des marques sans autorisation du paiement de plusieurs sommes (2000 euros à titre de dommages-intérêts et 800 euros au titre des dépens) pour chacune des sociétés auxquelles monsieur Fabien S. a porté préjudice et de la publication de la décisions dans les journaux : les Dernières Nouvelles d'Alsace et Libération et de la publication du jugement sur le site internet footlocker.fr.*

Il ressort de cette décision qu'en plus des peines ou des sanctions traditionnelles prononcées, c'est-à-dire la prison et les amendes, la publication de la décision dans des quotidiens de journaux et sur le site internet des sociétés lésées s'ajoute.

Le fait de publier la décision de justice, condamnant en l'espèce Monsieur S, l'imitateur de sites ayant pignon sur rue, sans autorisation de la part des marque, est un moyen à la fois dissuasif (pour des internautes qui seraient tentés d'agir de manière

---

[280] L'anonymisation recouvre plusieurs techniques pour masquer les données ou rendre impossible l'identification des personnes concernées, cf. Fiche n°16 de la Commission Nationale Informatique et Libertés (CNIL) sur l'anonymisation.

[281] Cf. Tribunal de grande instance de Strasbourg 7ème chambre correctionnelle Jugement du 26 mai 2009 : FL Europe Holding, Foot Locker France / Fabien S, consultable sur www.legalis.net.

comparable) et préventif (pour informer les clients de ces enseignes ou toute personne de l'existence de tels agissements.

Au titre des innovations textuelles adaptées à la technologie, la loi d'orientation et de programmation pour la performance de la sécurité intérieure (dite loi LOPPSI)[282] a été votée.

Elle vise à renforcer la sécurité au sein de l'Etat Français notamment quant à la criminalité organisée. Elle fait partie d'un tome 2 avec la loi LOPPSI II. Ce second acte a pour objectif de créer des infractions spécifiques ou du moins un arsenal répressif plus spécifique à la cybercriminalité. Cette disposition légale introduite par la Ministre Michel Alliot-Marie, est à l'image de ce qui existait déjà dans des Etats voisins, et membres de l'Union européenne comme le Danemark et le Royaume Uni ou encore la Belgique.

C'est dans le cadre d'un système de renforcement législatif qu'a été créée une nouvelle incrimination : l'usurpation d'identité numérique pour pallier le vide juridique qui existait.

2- L'usurpation d'identité numérique

L'usurpation d'identité numérique est une infraction crée par la loi n° 2011-267 du 14 mars 2011 dite Loi LOPPSI. Cette infraction n'était pas spécifiquement prise en compte par le code pénal français jusqu'en 2011 et désormais l'article L 434-23 du code pénal français incrimine l'usurpation d'identité numérique. Cette disposition précise que : « le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75000 € d'amende ».

Nonobstant les dispositions des articles 132-2 du code pénal et suivants, les peines prononcées pour ce délit se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise. Est punie des peines prévues par le premier alinéa la fausse déclaration relative à l'état civil

[282] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure parue au Journal officiel n° 62 du 15 mars 2011 page 4582.

d'une personne, qui a déterminé ou aurait pu déterminer des poursuites pénales contre un tiers ». Il serait intéressant de s'interroger sur la clarté de cette disposition légale : que signifie « *dans des circonstances qui auraient pu déterminer contre celui-ci des poursuites pénales* » ?

Il pourrait s'agir d'une référence faite aux infractions consistant dans l'utilisation du nom d'un tiers sans son consentement. En d'autres termes, il s'agit de l'infraction déjà connue d'usurpation simple de l'identité d'un tiers (c'est le fait pour une personne de se faire passer pour une autre qu'elle n'est pas, en réalité). Cette disposition concerne le fait d'usurper l'identité d'une personne et punit la fausse déclaration d'état civil. Il faut y adjoindre l'incrimination de l'article L 226-4-1 du code pénal français qui, sanctionne *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération*. La peine encourue est d'un an d'emprisonnement et de 15000 euros d'amende. La précision apportée sur l'utilisation de « données de toute nature permettant d'identifier » la personne concernée renvoie à une donnée à caractère personnel et spécifie ainsi l'incrimination en l'étendant aussi bien à l'état civil mais également à toute donnée, qui, d'une manière générale permet de reconnaître un individu.

Ainsi, le 18 décembre 2014, le Tribunal de grande instance de Paris a rendu une condamnation relative à l'usurpation d'identité numérique sur le fondement de l'article 226-4-1 du code pénal. Les faits sont les suivants : un informaticien a créé un faux site officiel de la maire du septième arrondissement de Paris grâce à son nom, et sa photo (sans son autorisation) et faisant croire qu'il s'agissait de la maire, elle-même en ce qu'il a permis d'y laisser des commentaires[283]. S'estimant lésée, la maire a saisi le tribunal afin de faire cesser cette activité numérique indésirable. Le tribunal a sanctionné au principal, l'informaticien à l'origine de cette usurpation d'identité numérique à une peine d'amende

[283] Cf. décision du TGI du 18 décembre 2014, consultable sur www.legalis.net

de trois mille (3000) euros et à cinq cents (500) euros, le complice, qui avait mis à disposition, son serveur pour le faux site officiel.

En plus de l'usurpation d'identité numérique que cette loi vient incriminer et punir, elle insère dans le code pénal des dispositions visant à régir la technique du filtrage. Le filtrage est un mode de contrôle des contenus qui consiste à trier les messages et à refuser ceux qui sont jugés contraires à l'ordre public ou encore à écarter les messages ou images qui portent atteinte aux droits des citoyens d'une manière générale. Ce sont surtout les contenus illicites qui sont visés. Ainsi, des images à caractère pornographique seront écartées et ne seront pas diffusées sur un site ayant vocation à l'éducation notamment. Les dispositions pénales insérées dans le cadre de la règlementation du filtrage pour ce qui est de l'usurpation d'identité sont celles relatives à l'encadrement des filtres anti-hameçonnage pour se protéger des attaques informatiques.

C'est d'ailleurs dans ce cadre que la protection des œuvres littéraires ou musicales par le droit d'auteur ou les droits voisins s'avère utile et efficace.

Parallèlement au phishing, existent les techniques d'escroquerie en ligne auxquelles, il faut ajouter les techniques d'escroqueries liées aux jeux en lignes et d'autres abus de faiblesse. Toutes autres formes de la cybercriminalité dont les incriminations méritent d'être étudiées.

d- L'escroquerie en ligne et les autres abus de faiblesse

La publication sur les sites d'annonces de vente de produits ou de biens est une source de commission des infractions d'escroquerie en ligne et d'abus de faiblesse

1- Les cas d'escroquerie en ligne

Certains cas sont généraux et d'autres comme l'escroquerie liée aux jeux en ligne sont spéciaux ?

α. Les cas généraux d'escroquerie en ligne

Les annonces de vente ou d'achats de biens sont souvent présentées par des délinquants sur des sites de vente en ligne avec des offres alléchantes défiant toute concurrence. A titre illustratif, les tablettes numériques proposées à des prix en dessous des prix pratiqués sur le marché. Ces annonces sont mises en lignes par des particuliers

(ils se présentent ainsi auprès des éventuels acheteurs) parfois sans aucune photo. L'offre prend la forme d'une arnaque dès lors que le vendeur exige de la part de l'acheteur potentiel, que ce dernier effectue le paiement du bien concerné afin de pouvoir le recevoir. C'est le cas de plusieurs internautes victimes d'un arnaqueur reconnu pour ses actes : il s'agit de Christophe BOUDOT. Ce jeune homme agit à visage découvert puisqu'il ose communiquer via un fax sa pièce d'identité pour mieux exiger de ses victimes le versement de la somme correspondante au prix d'achat du bien vendu sur un compte[284].

Ainsi, les chiffres pour 2011 sont révélateurs du nombre de victimes de ce genre de pratique : en ce qui concerne BOUDOT Christophe, il aurait 90 victimes à son actif. Pour compléter la liste des chiffres, il y a eu 60 000 cas d'escroquerie en ligne en France, en 2011. Ce nombre est important et face à de tels comportements, aucune réponse concrète n'est encore donnée. C'est pourquoi les victimes s'érigent en justiciers. Elles portent certes plainte auprès de la gendarmerie et des services de police mais en plus, les victimes opèrent des enquêtes privées, passent des coups de fil, remontent les chaînes d'opérateur de téléphonie, s'il le faut, pour retrouver les traces de leurs *bourreaux numériques*.

En outre, elles recherchent en parallèle d'autres victimes dans le même cas ou ayant connu des circonstances identiques afin de former des collectifs de victimes et mettre fin à ces pratiques d'escroquerie.

Un autre aspect de cette escroquerie en ligne est celui dans lequel l'acheteur devient l'arnaqueur. En effet, il utilise le même processus mais réclame au vendeur le paiement via *Paypal*[285]. La manœuvre est la suivante : une personne (vendeur d'un bien) met en ligne une annonce sur un site de vente en ligne. Cette annonce est consultée par plusieurs acheteurs potentiels dont certains contactent le vendeur. La vente est conclue. Les acheteurs (qui dans ce cas agissent en groupe) précisent au vendeur qu'ils sont des

[284] Emission télévisée sur tf1 : sept à huit du 4 novembre 2012.

[285] Qui est pourtant un site de paiement sécurisé, créé expressément pour garantir le paiement sécurisé et les transactions sans risques de piratage pour les consommateurs qui achètent en ligne.

français mais résidant dans un pays donné de l'Afrique de l'Ouest[286]. Ils précisent par ailleurs que les fonds ont bien été transmis sur le compte de la personne qui propose le bien à vendre. Et la fraude commence avec l'exigence du paiement d'une taxe de transfert des fonds.

En d'autres termes, pour que le vendeur puisse recevoir les fonds transférés, il lui est demandé de payer une somme qui correspond en général à la moitié du prix de vente du bien en vente. Le vendeur reçoit un mail lui indiquant le transfert des fonds, qui ne seront touchés qu'une fois la taxe de transfert réglée. Il faut préciser que le compte Paypal utilisé, est un faux compte, créé avec un logo imité (qui en apparence est le même que l'original) et en plus, le site à partir duquel le mail de confirmation de transfert des fonds par *Paypal,* est un faux mail, créé pour l'occasion[287].

A la suite de ce cas, un test a été effectué par les équipes[288] de l'émission sept à huit pour remonter l'information transmise quant à l'acheteur potentiel. L'équipe a mis en vente via un site de vente en ligne une tablette numérique. Des acheteurs dits intéressés ont proposé un prix et la vente a été conclue. C'est un numéro particulier qui répond avec des interlocuteurs différents bien qu'il s'agit du même numéro. Dans ce cas, il était exigé que le bien proposé (en l'occurrence une tablette tactile) soit envoyé via la poste afin que le transfert opéré sur le compte soit effectif. C'est dire dans ce cas de figure que les personnes agissent en réseau pour multiplier les chances de commettre leurs délits. Quelle est l'incrimination qui correspond à ce cas de figure dans la mesure où le conflit est international ? Il fait intervenir des victimes en France et des délinquants en Côte-D'ivoire ? Quelle sanction est prévue ?

L'escroquerie en ligne est-elle suffisamment définie pour punir cette forme de cybercriminalité ? L'escroquerie est punie par l'article L 313-1 du code pénal français. Cet article dispose que : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres*

[286] Ce pays est en l'occurrence, la Côte-d'Ivoire.

[287] Les cyber-escrocs cf. Emission télévisée sur tf1 : sept à huit du 4 novembre 2012.

[288]Les équipes de journalistes dont Harry ROSELMACK de TF1 pour l'émission Sept à huit.

frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende». Pour que l'infraction puisse être sanctionnée, il faut que la victime dépose une plainte auprès des services de police ou de gendarmerie. Le problème avec les escroqueries en ligne, c'est le nombre important de documents à fournir de la part des victimes.

En effet, elles doivent se munir de tous les éléments pouvant permettre de retrouver l'escroc. Une communication[289] de la Brigade d'Enquêtes Financières et des Technologies de l'Information (BEFTI) permet de lister ces pièces. Il s'agit de donner:

- les références du ou des transferts d'argent effectués,

- les références de la ou des personnes contactées : adresse de messagerie ou postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ainsi que les courriers échangés…,

- tout autre renseignement pouvant aider à l'identification de l'escroc.

Ces documents sont nécessaires à l'identification mais servent surtout de preuves contre les personnes ayant commis ces actes d'escroquerie en ligne.

Dans ce contexte, la Chambre Criminelle de la Cour de cassation a rendu un arrêt le 21 mars 2012[290]. Les faits ayant donné suite à cet arrêt sont relatifs à la mise en place de faux sites de ventes aux enchères par Monsieur Y suivie d'escroquerie en bande organisée.

En effet, Monsieur Sorin Y recrute plusieurs personnes d'origine roumaine, leur fournit des faux passeports et paie leurs frais de voyage afin qu'ils perçoivent pour lui des

---

[289] La communication sous la forme de dépliant sur les escroqueries est disponible sur www.internet-signalement.gouv.fr

[290] Cf. Crim. 21 mars 2012, pourvoi n° 11-84437.

mandats cash en provenance de différents pays. Ces sommes sont le produit de fausses ventes aux enchères organisées par Monsieur Sorin Y, sur des sites internet. Monsieur Y a été condamné par la Cour de cassation à six (6) ans de prison.

Lescroquerie en ligne s'adresse aussi bien de manière générale aux individus qui achètent et vendent sur les sites en ligne. Elle touche également ceux qui s'y distraient au moyen des jeux en ligne. Ces derniers connaissent également un encadrement.

β. L'escroquerie spécifique des jeux en ligne

C'est grâce à la loi du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne [291] que le législateur français opère un toilettage des textes et une adaptation aux évolutions technologiques.

A cet effet, l'Autorité de Régulation des Jeux En Ligne (ARJEL) a été créée en tant que structure de régulation des jeux en ligne en France.

La loi du 12 mai 2010 sur la régulation des jeux en ligne est une occasion pour le législateur français d'intervenir dans un domaine où le gain semble facile. Dès lors, le risque est grand pour que des cybercriminels via l'usage de ces canaux (les jeux) essaient de pirater des comptes bancaires et commettre des vols. A ce propos, ce ne sont pas uniquement les comptes de particuliers qui seraient piratés mais la possibilité de contrefaire des comptes d'entreprises en vue de détourner des fonds est envisageable.

Il convient à ce stade de mentionner que les groupes de cybercriminels créent des sites de jeux en ligne qui sous-tendent leurs activités dans la mesure où ces sites sont co-hébergés avec des sites à contenus pornographiques[292]. Ces associations facilitent de la sorte les techniques de blanchiment d'argent.

La France fait partie des Etats dans lesquels le secteur des jeux en ligne est très règlementé. Ce n'est pas le cas dans d'autres Etats comme la Bulgarie, Chypre, pourtant

---

[291] Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne parue au Journal Officiel de la République Française n°0110 du 13 mai 2010 page 8881.

[292] Etude sur la cybercriminalité des jeux en ligne réalisée en 2006 par CERT-LEXSI, laboratoire d'expertise en Sécurité Informatique.

pays membres de l'Union européenne et pour des Etats non membres les Antilles Néerlandaises, Antigua et les Bahamas. Ce n'est pas seulement le défaut de législation dans ces pays qui facilite l'activité des cybercriminels.

Il faut préciser que les français ou les résidents français sont visés par les cybercriminels qui n'hésitent pas à leur envoyer via des mails, des spam ou autres techniques du genre pour attirer les joueurs en ligne qui sont établis en France. Ces derniers sont incités via de grands événements comme récemment la coupe du monde de football.

Le fait que la loi française incrimine la proposition de telles prestations aux résidents français, n'inquiète pas réellement ces sociétés étrangères. En témoigne la décision de la Cour d'appel de Paris[293]de laquelle il faut retenir les faits suivants : la société NEUSTAR, sans y avoir été autorisée par l'ARJEL et sans aucune déclaration dans ce sens propose via son site internet des paris hippiques. Elle a été assignée en référé devant le juge face à la mise en demeure de l'ARJEL, de se mettre en conformité quant aux déclarations prévues par la loi. L'accès à ce site renvoie vers d'autres services qui transitent par les opérateurs de téléphonie et fournisseurs d'accès agréés que sont Orange France Telecom, Free, Bouygues et Auchan.

Il convient de se rendre compte du niveau quasi nul de dissuasion que suscite le paiement des amendes par les sociétés concernées. Il faudrait certainement élaborer des sanctions plus conséquentes comme par exemple le blocage de ces sites en particulier.

Le blocage des sites n'est pas encore tout à fait accepté de la part des autorités. Il est considéré comme une sanction rigide notamment de la part de la Cour de Justice de l'Union européenne.

Malgré l'encadrement des jeux en ligne, il arrive des cas d'escroquerie des comptes des joueurs. C'est ainsi un moyen pour les cybercriminels de profiter de la faiblesse de certains internautes. Dans le cadre de faiblesse, les joueurs ne sont pas les seuls concernés. En dehors des jeux en ligne, d'autres personnes sont vulnérables et sont de potentielles victimes d'abus. Dès lors, qu'en est-il des abus de faiblesse, non plus en

[293] Cf. Cour d'appel de Paris Pôle 1 - Chambre 3, arrêt du 28 juin 2011, RG n° 11/10112.

ligne mais liées à l'incapacité de certaines personnes pour toute manipulation informatique de leurs données. Par incapacité, il faut comprendre le fait pour ces personnes de ne pas savoir manipuler les outils informatiques d'une part et d'autre part les troubles de la vue des personnes âgées qui les empêchent de lire les informations présentées par les écrans des ordinateurs ou de tout appareil informatique.

2- Les abus de faiblesse

Les abus de faiblesse sont une nouvelle forme d'actes de la part des délinquants informatiques. En effet, cette pratique consiste à dérober des données confiées par une personne qui éprouve des difficultés à utiliser les moyens de paiement (comme les distributeurs de billets de banque) ou des difficultés de lecture ou tout autre souci similaire (analphabétisme, impossibilité de se servir des outils informatiques, handicap...).

Faut-il classer ces comportements en particulière hausse dans la catégorie des abus de faiblesse classiques ou leur conférer une nouvelle place dans les textes répressifs ?

Il s'agit de personnes profitant de la faiblesse de leurs interlocuteurs pour s'introduire frauduleusement sur leurs comptes bancaires grâce aux informations subtilement dérobées, à l'insu des propriétaires.

Récemment, le quotidien Direct Matin, paru le 06 décembre 2012 a fait état de l'augmentation de ce genre de pratiques de manière considérable. Pour l'heure aucune incrimination n'existe en France et pour réprimer ces infractions, c'est l'abus de faiblesse traditionnel qui est le texte de référence qui s'applique. Le fait de censurer ces comportements par l'incrimination de l'abus de faiblesse classique ne suffit pas. Il va certainement falloir pour les juges compléter avec des circonstances aggravantes ou d'autres infractions commises à savoir la sanction de l'abus de faiblesse à laquelle viendra s'ajouter une introduction frauduleuse ou un vol de données, si la preuve est rapportée que celui qui abuse de la faiblesse a commis ces actes.

Les incriminations relatives aux infractions commises via ou sur les systèmes informatiques sont nombreuses. Le téléphone mobile et les accessoires de communication mobiles ainsi que les diverses applications sans cesse développées sont de nouveaux

terrain de chasse pour les cybercriminels. Comment ces infractions qui touchent les moyens de communication mobiles et les réseaux sont-elles traitées ?

B- Les incriminations relatives aux moyens de communication mobiles

Ces incriminations concernent d'une part les appareils mobiles de communication et d'autre part les réseaux de communication. Force est de reconnaître qu'avec l'usage des appareils de téléphonie, de Smartphone et autres tablettes capables de transférer, de transmettre ou d'échanger les données, les services de télécommunication et les opérateurs effectuent des tarifications particulières. Ces dernières sont souvent incompréhensibles pour les consommateurs en l'absence de détails de la part des opérateurs. C'est en cela que sous couverts de facturations non précises, des frais sont décomptés aux consommateurs.

Sous cet angle, facturer de manière arbitraire des services, censés être compris dans le *package* des télécommunications de base pourrait s'apparenter à une sorte de frein à la liberté des consommateurs. Il ne s'agit pas en tant que tel d'actes cybercriminels mais ils doivent être analysés dans les incriminations relatives aux mobiles puisqu'ils font référence à des obligations légales de la part des opérateurs quant aux prix de l'itinérance et des services de données. Ils permettent ainsi de soulever l'importance des accords notamment relatifs à la politique européenne de régulation des médias et autres moyens de communication comme le téléphone ou les nouveaux arrivants telles les tablettes tactiles.

a- Les actes cybercriminels contre les téléphones mobiles et assimilés

Il est question des incriminations sanctionnant les infractions qui portent atteinte aux téléphones mobiles encore appelés téléphones portables ou cellulaires. Ces supports de communication sont également visés par les cybercriminels. En témoignent les attaques contre les Smartphones[294].

[294]Voir sur ce point l'émission radio du 13 décembre 2011 diffusée par France Info au sujet de la protection des données personnelles qui, selon la CNIL n'est pas encore totalement réussie : Ecoutez l'émission sur France Info et lire également l'article sous le lien

1- Les attaques contre les mobiles

En Novembre 2012, le Tribunal correctionnel d'Amiens a condamné à six mois de prison ferme un jeune hacker pour le piratage de forfait de téléphone mobile. L'instruction a permis de comprendre comment ce jeune homme crée un code malveillant pour infecter des téléphones mobiles d'abonnés ayant souscrit à des contrats de communication sous la forme de *forfait mobile*[295] avec des opérateurs de téléphonie. La seconde étape de son acte est de s'introduire dans le système d'exploitation de l'appareil visé, d'atteindre le répertoire des contacts téléphoniques qui y figurent puis d'envoyer des messages écrits à ces contacts. Le but est d'utiliser à distance les abonnements téléphoniques de ces destinataires pour gagner des sommes aux jeux de loterie[296]. En lieu et place de la sanction d'enfermement total de 12 mois, le tribunal a condamné le jeune hacker à 6 mois ferme et au port de bracelet électronique pendant 6 mois.

Il faut souligner que les téléphones visés sont du type Androïdes, ce sont des Smartphones dotés de multiples applications. Or ces téléphones sont munis d'internet. Certes, c'est l'internet qui est la source d'une éventuelle infraction (s'il y a un vol de données par exemple) mais le cas soumis au tribunal correctionnel d'Amiens montre qu'internet n'est pas la seule source de commission des actes de piratage liés au le téléphone mobile. Les forfaits mobiles souscrits s'analysent désormais en de nouveaux supports de l'infraction. Outre les forfaits, les applications du téléphone sont de la sorte perçues comme des occasions notamment de voler les données stockées sur la mémoire

---

suivant :http://cybercriminalite.wordpress.com/2011/12/13/les-donnees-personnelles-pas-assez-protegees-sur-les-smartphones-cnil/

[295] Les forfaits mobiles sont des formules grâce auxquelles les abonnés adhèrent à un contrat de téléphonie qui leur permet d'avoir des créneaux de communication limité à des horaires précises ou illimité en fonction du montant choisi. Par exemple, le forfait limité aux communications vers la France métropolitaine peut comprendre une heure décomptée de la formule, des envois de messages et une connexion internet, elle aussi limitée à un certaine nombre d'heures ou à une capacité définie comme par exemple 500 Go (Giga octets).

[296] Cf. le Journal Le Figaro du 8 novembre 2012 « *Six mois ferme sous bracelet électronique pour un hacker* », article disponible en ligne : http://www.lefigaro.fr/hightech/2012/11/08/01007-20121108ARTFIG00744-six-mois-ferme-sous-bracelet-electronique-pour-un-hacker.php; Il est également disponible sur le site du journal le télégramme : http://www.letelegramme.com/ig/loisirs/multimedia/virus-sur-smartphones-bracelet-electronique-pour-le-jeune-hacker-08-11-2012-1900129.php

du téléphone. D'autres contenus notamment les images dont les photos ou documents enregistrés sur le téléphone sont ainsi susceptibles d'être volées. C'est le cas des données stockées sur des Smartphones[297].

D'autres appareils comme les BlackBerry font l'objet de méfiance de la part des entreprises depuis la mise au grand jour des programmes des écoutes généralisées mis en place par les autorités américaines[298]. Le BlackBerry est une catégorie de téléphone prisé par les responsables des entreprises en général, dans la mesure où, l'une de ses fonctionnalités facilite l'accès à la boîte de messagerie en ligne de manière instantanée et en temps réel. Le problème c'est que ces appareils utilisent de réseaux de communication grâce auxquels ils transfèrent les informations par le truchement du système d'interception ECHELON. Tous les téléphones sont équipés de système d'écoutes discrètes qu'il est possible d'activer par un code informatique.

ECHELON, est un accord basé sur un système d'écoute généralisée et de filtrage des données. Cet accord est signé à l'origine entre les Etats-Unis et la Grande Bretagne[299]. Ce réseau d'écoute généralisée pose de sérieux problèmes de respect de la vie privée des individus mais soulève la question de la possibilité d'interception qui existe.

A ce propos, même les dirigeants politiques n'échappent pas à cet espionnage de masse. Il faut prendre pour illustration la récente découverte de la diplomatie allemande :

Voir encore sur BFM TV : http://www.bfmtv.com/societe/jeune-hacker-damiens-condamne-a-6-mois-ferme-bracelet-electronique-378254.html

[297] Cf. **FILIPPONE D**., un SMS pirate rend fou les Windows Phone : Une attaque par SMS ciblant les Smartphones embarquant la dernière version de l'OS de Microsoft a été identifiée. L'accès au flux de messagerie sur son terminal devient impossible, Journal du Net du 14 décembre 2011sur http://www.journaldunet.com

[298] cf. **FILIOL E.**, le business de la cybercriminalité, éditions DUNOD, Paris, 2006, p. 96.

[299]Voir sur ce point **WARUFSFEL B**., Le renseignement français contemporain, aspects politiques et juridiques, éditions L'harmattan, 2003, p. 55. Et compléter avec le mémoire de DESS de **JANOT Philippe** sur Le réseau Echelon, outil d'intelligence économique, mémoire de DEA sous la direction de Serge SUR, 2000/2001 et le Rapport d'information n° 2623 sur les systèmes de surveillance et d'interception électroniques de M**. Arthur PAECHT,** déposé à la commission de la défense le 11octobre 2000. Ajouter le **Rapport Schmidt**, rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON 2001/2098 (INI), recommandations n°16, 15 et 12.

la chancelière Angela MERKEL serait sur écoute depuis plus de dix ans à son insu[300]. C'est en réalité en 1999 que ECHELON pose de véritables questions liées à son contexte notamment à la suite de la publication du rapport rédigé par Duncan CAMPBELL[301] intitulé *Interception Capabilities*[302] pour une étude à la demande du Parlement européen.

La Convention de Budapest traite des incriminations liées aux mobiles dans les dispositions relatives aux interceptions des communications.

En effet, c'est la possibilité de transiter des données par les ondes et les réseaux de communication mobiles qui les rendent accessibles et par conséquent susceptibles d'être détournées de manière frauduleuse notamment.

La Convention en son article 3 punit ces agissements relatifs à l'interception illégale en disposant que : « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. »*

Et pourtant il faut souligner les interceptions déguisées des États dans la vie des citoyens au moyen des systèmes comme Échelon. Comment qualifier ces actes d'écoutes de masse? L'Etat, pourtant garant de la liberté des citoyens et par ailleurs de la protection des données de ces derniers n'est-il pas, dans ce cas de figure précis d'écoute généralisée

---

[300] Cf. **DELMAS Aurélie**, *Angela MERKEL, cible économique*, article paru dans le Journal Direct Matin du 28 octobre 2013, le commentaire laissé par la chancelière est : « l'espionnage entre amis, ça ne va pas du tout ».

[301] **DUNCAN CAMPBELL** est un journaliste d'investigation britannique, à l'origine de la révélation du réseau Echelon.

[302] Cf. **DUNCAN CAMPBELL**, Interception Capabilities, Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programmed Office) on the development of surveillance technology and risk of abuse of economic information, IPTV Ltd, Edinburgh, Scotland: April, 1999.

et d'interceptions, en infraction au regard des dispositions de la Convention de lutte contre la cybercriminalité ? L'interrogation est large et les réponses sont discutables.

Les écoutes de masse sont un frein à la liberté des citoyens et elles épousent souvent d'autres formes puisqu'elles concernent d'autres données non pas audibles mais écrites. C'est l'hypothèse de l'espionnage des données.

2- L'espionnage de données

La cybercriminalité n'est pas uniquement perpétrée sur les ordinateurs, d'autres supports comme les téléphones mobiles sont visés. Aujourd'hui la plupart de ces appareils de communication sont dotés de fonctionnalités permettant des connexions internet à distance, par wifi ou via des réseaux numériques ou même des communautés de blogs. Ils sont de la sorte de nouveaux supports, outils ou cibles pour les cybercriminels pour la commission de leurs actes malveillants.

C'est pourquoi plusieurs articles ont mis en lumière le développement d'outils, de logiciels d'espionnage pouvant être installés sur les téléphones portables. Des sanctions contenues dans le code pénal Français permettent de punir toute activité de ce genre : il s'agit des articles L226-1, L226-15 et L226-3. Il faut savoir que l'ensemble de ces données contenues dans les appareils mobile ou même les tablettes sont stockées et quand bien même elles seraient retirées du site concerné par les propriétaires, elles existent toujours quelque part dans les archives en ligne.

Les techniques d'espionnages sont nombreuses et intègrent la plupart des moyens de télécommunication. Or, ces outils utilisent des réseaux qui sont eux-mêmes victimes exactions dans le cadre d'activités cybercriminelles.

C'est en cela qu'il est possible de mentionner les processus de blocages de réseaux de télécommunication.

b- Le blocage de service de réseaux de télécommunication

Le blocage de services de réseaux de télécommunication passe par des connexions téléphoniques ou de communication. C'est donc une infraction qu'il convient d'analyser dans le cadre des incriminations liées aux mobiles et supports téléphoniques de communication. Cette infraction concerne également les réseaux. C'est dans ce cadre

que, le 18 novembre 1992, le juge de la cour d'appel de Paris a qualifié un radiotéléphone de système de traitement automatisé de données, et dont le blocage constitue une infraction puisqu'il porte atteinte aux systèmes d'exploitation d'un réseau de télécommunications[303]. La radiotéléphonie est définie par le dictionnaire des médias comme un système de téléphonie mobile dans lequel la liaison entre les terminaux reliés est assurée, totalement ou partiellement, par un réseau hertzien et non par un réseau câblé, dit parfois réseau filaire[304].

Dans une décision de 2012, à la suite des enquêtes menées par la Brigade des Enquêtes Financières et sur les Technologies de l'Information, le Tribunal de Grande Instance de Paris a connu des manœuvres en bande organisée s'agissant des contournements des lignes de téléphonie pour des gains faciles. Cette technique consiste soit dans la création de lignes téléphoniques inexistantes à partir de réseaux de communication d'entreprise (notamment des lignes destinées au service après-vente auprès des consommateurs de l'entreprise concernées), soit dans le contournement des appels vers des postes fixes en vue d'en récupérer les consommations et de créer des flux de communication.

Cette pratique a permis à un employé de télécom de se faire des sommes d'argent en marge de ses revenus. Il s'agit de ce point de vue d'une source de gains faciles. L'arnaque consistant à détourner les lignes téléphoniques en vue de créer des flux. Les flux générés par ces appels vers des destinations lointaines permettent au final toucher des sommes d'argent. Ce genre de pratiques frauduleuses a fait l'objet d'une décision de justice dans laquelle les agents de la BEFTI ont dû intervenir. Ces agissements s'analysent en une forme de cybercriminalité dans la mesure où les lignes téléphoniques fictives génèrent des flux de communication, elles créent des débits et permettent par des techniques de facturation, de générer des sommes versées sur des comptes expressément

[303] Cour d'appel de Paris, 9e chambre, 18 novembre 1992, JCP éd. Entreprise, 1994, I, n° 359.

[304]Cf. Dictionnaire des médias, sous la direction de **Francis BALLE**, p.209, éditions Larousse, Paris, 1998.

créés à cet effet. Ce type d'arnaque a été mentionné dans le Rapport VARENNE relatif aux services à la valeur ajoutée, publié en 2008 par le ministère de l'Economie[305].

Dans l'ordre des infractions caractérisées de mobile, il faut inclure les infractions issues des communications des salariés notamment. En clair, il s'agit de la possibilité aujourd'hui répandue pour les chefs d'entreprises privées de permettre à leurs salariés de travailler à distance via des connexions en réseau. C'est la technique du *Mobile Device Management* ou de la gestion de dispositif mobile (en français). Cette technique permet aux salariés d'une entreprise dont les Directeurs de systèmes d'information le permettent, de travailler en dehors de leur lieu de travail, sur des supports électroniques divers et surtout mobiles comme des téléphones ou des tablettes numériques, à condition d'avoir un accès contrôlé au réseau de l'entreprise[306]. Ces supports créent des risques d'infractions de la part des cybercriminels comme par exemple les interceptions des données. C'est dans ce cadre que s'inscrit la technologie Bluetooth[307], très prisée dans la volonté de communication rapide notamment des salariés en dehors de leur entreprise. Le Bluetooth permet en effet via les ondes de fréquences de partager des cartes de visite, dès lors que les personnes sont connectées ou encore dès l'instant où il est activé sur un appareil qu'il s'agisse d'un téléphone ou de tout autre support. Et il existe plusieurs techniques de piratage facile des données via le Bluetooth : que ce soient les fonctions ou l'appareil qui l'utilise ou encore le carnet d'adresses, le Bluetooth peut faire l'objet d'intrusion et on parle de *bluejacking*, de *bluebugging* ou enfin de *bluesnarfing*[308]. Ces

---

[305] Cf. Rapport sur les services à la valeur ajoutée : tarification de détail et déontologie présenté par **Dominique VARENNE**, contrôleur économique et financier.

[306]Cf. **LE GUYADER Patrick** qui évoque la technique dans son ouvrage sur l'usurpation d'identité, à la page 78. Il explique le concept et en souligne les dangers d'un point de vue juridique de la protection des flux de données. Par accès contrôlé par l'entreprise, il faut comprendre l'attribution de Login ou identifiant du salarié ainsi qu'un mot de passe associé pour favoriser la connexion en sécurité sur le réseau de l'entreprise.

[307]Le Bluetooth signifie littéralement les dents bleues mais est une technologie ou un périphérique de réseau sans fil qui permet de connecter des appareils mobiles par exemple des téléphones.

[308]Cf. **BECKER Andreas,** Bluetooth Security & Hacks, étude publiée le 16 août 2007, Chair for Communication Security et citée par **Patrick LE GUYANDER** au sujet des risques d'interceptions de données via le Bluetooth dans son ouvrage *Usurpation d'identité*, 2012.

infractions dont sont susceptibles d'être victimes les propriétaires des supports à Bluetooth sont-elles incriminées ?

L'incrimination des vols de données est source de difficultés d'un point de vue de la qualification juridique. Elle soulève la question de la source du vol : est-ce via le traitement des données concernées que ces dernières auraient été frauduleusement soustraites ou les données sont-elles détournées en l'absence du consentement du titulaire ?

Il s'agit en fait de copie des données[309]. Dans ce cas, les juges sont intervenus notamment dans un arrêt de la 10ème chambre de la Cour d'appel de Paris du 05 février 2014[310] pour condamner un bloggeur à trois mille euros d'amende (3000 euros) pour s'être maintenu dans un système informatique de données (celui de l'ANSES, opérateur d'informations vitales) et d'avoir volé des données par copie de ces informations. Des faits, il ressort que par une recherche experte et grâce à son système Virtual Private Network, le titulaire du blog *Bluetoff* a eu accès aux codes de connexion de l'intranet de l'ANSES. Il connaissait la confidentialité des données auxquelles il avait eu accès et les a copiées. Ces copies sont qualifiées de vol par la Cour d'appel.

En droit français, la Loi Godfrain réprimait les infractions relatives aux intrusions frauduleuses sans davantage de précisions quant au vol. Désormais, et grâce à la loi du 13 novembre 2014[311], le vol de données est encadré. Il est désormais clairement sanctionné. L'article 16 de la loi modifie l'article 323-3 du code pénal en ce qu'il dispose que « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.* » Le fait d'extraire est l'innovation majeure qui vient

---

[309] Comme le souligne **Fabrice MATTATIA**, dans son analyse sur le vol de données, Vers la reconnaissance juridique du vol de données, publiée dans le magazine *01 Business* du 26 novembre 2014.

[310] Cour d'appel de Paris, Pôle 4, Chambre 10 des appels correctionnels, 05 février 2014, Olivier L. / Ministère Public, n° RG 13/04833.

[311] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme publiée au JORF n°0263 du 14 novembre 2014 page 19162, texte 5.

sanctionner le vol de données notamment par copie (non autorisée, et en cela le fait de copier sans droit des données d'autrui s'analysent en une soustraction frauduleuse, or, c'est la définition (en droit français) du vol.

Les blocages de services de télécommunication s'analysent en des actes cybercriminels et d'autres comportements comme les usurpations d'identité empruntent les canaux téléphoniques. Dès lors, comment sont traitées ces usurpations qu'on peut différencier des précédentes qui, elles, sont numériques exclusivement?

c- L'usurpation d'identité par intimidation téléphonique

L'affaire du canular mis en place par des individus pour obtenir des informations relatives au Système de Traitement des Infractions Constatées (STIC) attire l'attention sur l'usurpation d'identité par intimidation téléphonique. Les faits datent de décembre 2012[312].

Par le biais de coups de fil à différents secteurs de la police et de la gendarmerie, des personnes ont usurpé l'identité de policiers et ont fait croire à des appels de collègues de ces derniers. Ces actes visaient à obtenir des informations contenues dans le Système de Traitement des Infractions Constatées (le STIC) géré par les services de police et de gendarmerie. La question est de savoir quels détails ont été utilisés pour parvenir à détourner les identités des policiers et surtout quelles informations ont été divulguées au point d'atteindre les agents de police floués par ce canular. C'est certes la question de la protection des données dérobées (puisqu'il y a eu à la suite des appels des diffusions des parties des fichiers du STIC sur internet) qui se pose mais encore plus celle de la gestion des informations reçues par les polices et gendarmeries.

Par ailleurs, il convient de s'interroger sur la fiabilité des informations véhiculées via le téléphone. Dans quelle mesure un agent de police ou un gendarme peut désormais être certain qu'il a bien comme interlocuteur un collègue et non une personne qui usurpe

[312] Information diffusée sur la radio RTL le 04 janvier 2013 à 07h54 : « *Les fichiers Stic de certains rappeurs français diffusées sur Internet* ». Voir en ligne cf. http://www.rtl.fr/info/article/les-fichiers-stic-de-certains-rappeurs-francais-diffusees-sur-internet-7756551571

l'identité de son collègue. Quelle incrimination correspond à cette pratique, si elle est prévue par la loi française, ou dans d'autres Etats européens, quelles sont les peines encourues ?

L'enquête est certes ouverte auprès de la Brigade en charge des Enquêtes sur les Fraudes aux technologies de l'Information pour retrouver les individus ayant fait ce canular, mais cela n'empêche pas de s'interroger sur la gestion des données contenues dans le STIC, la procédure de consultation et surtout les modalités de communication de ces informations confidentielles.

D'une manière générale, en France par exemple, le code pénal punit l'usurpation d'identité à l'article 434-23 d'une peine de prison de cinq ans et de soixante-quinze mille (75000) euros d'amende. Il s'agit en l'espèce d'une usurpation classique empruntant les canaux téléphoniques, et distincte de l'usurpation numérique. On peut valablement en déduire que les peines prévues par les dispositions de l'article précité trouvent à s'appliquer.

L'usurpation d'identité par téléphone lance le débat des vérifications d'identité entre agents de gendarmerie ou de tout autre service en charge de la gestion de fichiers sensibles comme le STIC.

En dehors des fichiers sensibles, d'autres secteurs des télécommunications sont règlementés et exigent de la part des opérateurs des actes contrôlés comme la facturation justifiée de certains services comme l'itinérance.

d- Les facturations anarchiques de l'itinérance et des services de données

L'itinérance peut être définie comme le fait de se déplacer dans l'exercice de ses fonctions[313]. Elle est plus connue sous le nom de « *Roaming* » et consiste pour l'utilisateur d'un réseau de téléphonie de conserver son opérateur d'un pays à l'autre sans changer de téléphone. Le souci c'est que la tarification qui fluctue ne respecte pas nécessairement toujours l'encadrement prévu de la part des opérateurs.

[313] cf. Définition du dictionnaire Le Robert, p 941.

De ce fait, téléphoner à l'étranger ou envoyer un message est coûteux. C'est pourquoi, la question de la tarification a été abordée par les députés au sein de l'Union européenne. En effet, au mois de mai 2012, elle a donné lieu à un accord en vue de la réduction des prix liés à l'utilisation du téléphone à l'étranger[314] et le règlement est publié[315]. L'objectif de l'action des parlementaires européens est de mettre des limites aux prix fixés par les opérateurs de téléphonie et surtout d'encadrer les factures et éviter des facturations indues et inattendues de la part des consommateurs.

Au titre de cette réduction des prix, les opérateurs ont désormais l'obligation de fournir le détail des prestations facturées et surtout, ils doivent alerter les consommateurs dès lors que les factures avoisinent certaines sommes. L'alerte ayant pour but de permettre au consommateur d'être averti de sa consommation et de mieux la réguler ou la contrôler.

En cas de non- respect de ces obligations désormais légales, les opérateurs encourent des sanctions. Ces sanctions sont essentiellement pécuniaires.

Les incriminations liées aux mobile et téléphones sont spécifiques en ce qu'elles utilisent les moyens de communication téléphoniques comme des outils ou des intermédiaires de commission d'actes cybercriminels.

A ces moyens mobiles, s'ajoutent les réseaux et les serveurs qui ont la particularité de ne pas être localisés dans des espaces géographiques connus. En d'autres termes, les réseaux relèvent plus de la combinaison de plusieurs espaces de communication et semblent de la sorte relevés de l'irréel. Quelles sont les incriminations liées à ces réseaux et serveurs en ce qui concerne la cybercriminalité ?

C- Les incriminations liées aux réseaux et serveurs

---

[314] cf. Actualité du Parlement européen : « *Nouvel accord pour réduire les prix de l'itinérance et des services de données* », Session plénière, société de l'Information du 10 Mai 2012, sur www.europarl.europa.eu

[315] Règlement (UE) n°531/2012 du Parlement Européen et du Conseil du 13 juin 2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, publié au JOUE du 30 juin 2012, L 172/10.

Les réseaux et les serveurs permettent d'aborder l'informatique en nuage ou *cloud computing* et les botnets, c'est à dire les *machines zombies* utilisées pour lancer des attaques contre des systèmes informatiques. Dans ce cadre seront envisagées les problématiques de sécurité du *Cloud computing* ainsi que les infractions en direction de serveurs ou par ces serveurs. A ces questions, s'ajoutent celles des contenus illicites et les téléchargements illégaux.

a- La pratique des botnets

Les botnets ou *ordinateurs zombie* sont souvent utilisés pour lancer des attaques de détournements (déni) de service partagés contre les systèmes informatiques. L'Agence Nationale de la Sécurité des Systèmes d'Information française (ANSSI) définit le botnet ou Réseaux de machines zombies (un réseau de bots, contraction de réseau de robots) comme un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise[316].

Le botnet facilite la commission de plusieurs infractions en réseaux. Le déni de service ou Denial of Service (DOS) est un dysfonctionnement de service créé par un virus ou un pirate qui attaque un système visé.

Le déni de service résulte des agissements des *black hat* ou *chapeaux noirs* (en français) dans le but de créer un dysfonctionnement de service de manière à nuire à la continuité du service concerné. Exemple dans le cadre du serveur appelé *Dynamic Host Configuration Protocol*, il s'agit de s'attaquer au serveur de manière à ce qu'il ne puisse plus communiquer les informations aux postes de travail de l'entreprise ciblée[317]. De la sorte, il y a un arrêt de travail des salariés. Si l'entreprise fournit des services ou des prestations particulières rentables, elle se trouve paralysée ; elle ne produit pas mais paie

[316] Voir pour la définition, les fiches techniques sur le portail de la sécurité informatique : http://www.securite-informatique.gouv.fr et plus précisément sous le lien : http://www.securite-informatique.gouv.fr/gp_rubrique33_lettre_R.html

[317] Certains termes spécifiques ont nécessité le recours à des spécialistes comme M. Lionel ALLA, architecte en système d'informations, pour leur expertise en la matière.

ses salariés. L'entreprise réalise ainsi une perte au niveau de son chiffre d'affaires. C'est une pratique qui peut être employée par un concurrent notamment.

A titre illustratif, le concurrent a pour cible, le système de GOOGLE. A la suite de l'attaque effectuée, le système entier est affecté, et provoque un dysfonctionnement dont les utilisateurs des services fournis par GOOGLE vont être affectés. De la sorte, des boîtes de messageries électroniques GOOGLE, donc ayant pour nom de domaine Gmail vont être affectées[318]. La cible, dans ce cas, est le système de base et ce genre d'attaque diffère de l'attaque indirecte qui consiste dans le procédé inverse.

En effet, le processus inverse, appelé Denial Distributed of Service est le fait pour un hacker ou autre délinquant d'utiliser les systèmes annexes ou dérivés d'un ensemble informatique pour au final atteindre le système principal. Pour réutiliser les éléments de l'exemple précédent, le délinquant utilise les services annexes à Google notamment les boîtes mails ou les bases de données fournies par Google[319] pour atteindre le système central de gestion des interfaces de Google.

Un autre processus employé par les *hackers* pour favoriser le déni de service est d'insérer un script dans le DHCP visé, de manière à l'entraîner à générer jusqu'à saturation des adresses IP[320]. L'adresse *Internet Protocol* (l'adresse IP) est le protocole universel de transmission. Or, si le DHCP fournit des adresses IP à saturation, il n'en disposera plus et les accès aux postes de travail se trouvent bloqués et par conséquent inopérants.

---

[318]Cf. les liens qui suivent : http://searchsoftwarequality.techtarget.com/definition/denial-of-service et http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

[319] Définition sur http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm.

[320]Cf. **GRENIER Jean-Guy**, Dictionnaire d'informatique et d'internet anglais-français, la maison du dictionnaire, Paris, 2000.

C'est cette technique qui est employée dans l'attaque informatique perpétrée contre les services publics de l'Estonie en Mai 2007[321]. Comment les lois des Etats de l'Union européenne sanctionnent-elles ces attaques en réseaux qui se multiplient de plus en plus?

Jusqu'en 2013, il n'existait pas de législation claire sur les sanctions légales contre l'utilisation des botnets ou un recours à cette pratique.

Néanmoins, le Conseil de l'Europe, et spécialement la division en charge de la législation c'est-à-dire le Comité de la Convention sur la Cybercriminalité établit des notes explicatives et des guides sur certains aspects répressifs de la Convention de lutte contre la cybercriminalité. Ce comité a précisé dans son guide intitulé « T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets», rédigé lors de sa 9ème rencontre en juin 2013 à Strasbourg[322], que les pratiques *de botnets relèvent de plusieurs articles de la Convention de Budapest : il s'agit de l'article 2 qui traite de l'accès illégal au sens des intrusions frauduleuses, de l'article 3 en ce que les botnets peuvent constituer des interceptions illégales, l'article 4 parce que les botnets facilitent des interférences de données c'est-à-dire la modification, l'endommagement ou la falsification des données ; l'article 5 pour la faculté qu'ont les botnets de falsifier des données dans un système informatique dans son intégralité. L'article 6 quant à lui définit l'ensemble de toutes les possibilités de dénis de service : or c'est bien à cet ensemble qu'est destinée la pratique des botnets*. Les articles 8 à 11 sont également constitutifs des incriminations de botnets.

Les botnets sont un moyen de commettre tous les types d'infractions répertoriés et incriminés par la Convention de Budapest de lutte contre la cybercriminalité. C'est pourquoi, les attaques opérées par ces machines zombies sont toutes punies par les différentes incriminations de la convention, de l'intrusion frauduleuse à la fraude informatique en passant par l'accès illégal et aux interceptions illégales.

---

[321] Cf. **LANDER Mark** and **MARKOFF John**, Digital Fears emerge after data siege in Estonia, New York Times (May 29, 2007); voir également **BRENNER Susan**, Cyber threats : The emerging fault lines of the nation State, Oxford university press, 2009.

[322] Pour une version des différents articles et du guide sur la cybercriminalité et les botnets, cf. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_6REV_GN2_botnets_V7adopted.pdf

La sanction contenue dans chacun de ces articles qu'elles soient des peines privatives, de liberté ou des sanctions financières s'appliquent aux personnes ayant eu recours aux botnets avec des circonstances aggravantes pour les cas dans lesquels les pertes sont considérables et les préjudicies subis de la part des victimes, colossaux.

Et c'est au regard de l'article 13 de la Convention de Budapest que les Etats doivent légiférer quant aux sanctions à prendre contre les botnets. Cette disposition de la Convention fait référence à la proportion des sanctions édictées compte tenu du fait que les botnets peuvent causer des préjudices aussi bien aux institutions publiques ou privées qu'aux personnes.

Dans ce cadre, la police espagnole a récemment démantelé un réseau de botnets se faisant appelé « *Mariposa* »[323]. Ce groupe constitué principalement de trois individus, utilisait le réseau de botnets pour dérober des données informatiques des banques et des entreprises d'une manière générale.

D'une manière générale, il faut mentionner les différentes décisions-cadre prises au sein de l'Union par la Commission européenne. En effet, la première qui permet de faire un point sur l'ensemble des législations de l'UE est la décision cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États[324].

Mais celle qui nous semble plus intéressante est celle de 2005 relative aux attaques visant les systèmes d'informations[325]. Ce texte prône clairement un rapprochement des législations pénales en la matière afin d'assurer une lutte efficace. Et pour y parvenir, la décision cadre entend harmoniser la définition des infractions, autrement dit, il est question de trouver des terrains d'entente au plan des incriminations.

---

[323] Ce terme signifie papillon en espagnol ; cf. article « *Coup de filet en Espagne pour démanteler Mariposa, un botnets géant* » dans le MAGIT sous le lien http://beta.lemagit.fr/article/securite-espagne-police-hackers-conficker-botnet/5750/1/coup-filet-espagne-pour-demanteler-mariposa-botnet-geant/

[324] Cf. Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États - membre parue au JOCE L 190, 18.7.2002. Une décision cadre étant un acte pris en application d'un Traité, ici il s'agit du Traité UE.

Elle cite à titre illustratif l'accès illicite à un système d'information, l'atteinte à l'intégrité d'un système et l'atteinte à l'intégrité des données[326]. La décision cadre a été modifiée en 2008[327] et ce sont les points relatifs au terrorisme qui ont été abordés[328].

Malgré le lien étroit qui existe entre la cybercriminalité et le terrorisme, ce thème ne fera pas l'objet de développements poussés et sera par conséquent occulté de manière volontaire à certains niveaux.

Sur la question des attaques contre les systèmes d'information, la décision - cadre 2005/222/JAI relative aux attaques des systèmes d'information a été à nouveau modifiée en juillet 2013 grâce à la Résolution législative du Parlement européen du 4 juillet 2013 sur la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information[329] et abrogeant la décision-cadre 2005/222/JAI du Conseil.

Cette résolution adoptée en première lecture par l'Assemblée du Parlement est l'occasion de réitérer les objectifs d'harmonisations légales des infractions cybercriminelles et du droit procédural qui en découle. Elle donne naissance à la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil[330].

---

[325] Décision-cadre 2005/222/JAI du conseil du 24 février 2005 relative aux attaques visant les systèmes d'information publiée au JOUE L 69/67 du 16.03.2005.

[326] Point 11 de la décision cadre de 2005, précitée : « *il est nécessaire d'adopter une approche commune pour les éléments constitutifs des infractions pénales*(…).

[327] Cf. Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale parue au JOUE L 350/60, du 30.12.2008.

[328] Cf. Décision-cadre 2008/919/JAI du conseil du 28 novembre 2008 modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme publiée au JOUE L330/21 du 9. 12. 2008.

[329] Cf. 2010/0273(COD) - 04/07/2013 Texte adopté du Parlement, 1ère lecture/lecture unique disponible sur le site du Parlement européen.

[330] Cf. DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil publiée au JOUE L 218/8 du 14. 08. 2013.

En juin 2013, le Parlement européen a initié un projet de directive en phase de réprimer plus sévèrement ces actes trop longtemps restés sans sanction. Ce projet de directive est conclu entre les députés et les négociateurs du Conseil et de la Commission en 2012. Il a été adopté par la Commission des libertés civiles le jeudi 06 juin 2013. Les nouvelles règles visent également à faciliter la prévention et à renforcer la coopération policière et judiciaire en la matière. Le délai de réponse aux demandes d'aide urgentes sera fixé à huit heures. Il est surtout intéressant en ce qu'il introduit *également une peine d'au moins trois ans d'emprisonnement pour l'utilisation de "réseaux zombies", visant à établir un contrôle à distance d'un nombre significatif d'ordinateurs en les infectant de malicieux par le biais de cyber-attaques ciblées*[331]. L'assemblée plénière du Parlement européen a examiné le texte au mois de juillet 2013 pour son adoption. Cette adoption, marque le début de la répression des infractions notamment en réseaux et principalement une sanction au niveau de l'Union européenne s'agissant des botnets.

Avec la directive 2013/40 du 04 juillet 2013, il existe désormais un encadrement pénal des botnets au niveau de l'Union Européenne. La directive définit cette infraction « *la création de réseaux zombies, c'est-à-dire l'acte d'établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyber-attaques ciblées. Une fois créé, le réseau d'ordinateurs contaminés qui constitue le réseau zombie peut être activé à l'insu des utilisateurs des ordinateurs dans le but de lancer une cyber-attaque à grande échelle.*

D'autres problèmes sont issus des nouveaux usages des technologies de l'information comme la dématérialisation de l'hébergement des données ailleurs que sur son poste de travail ou son serveur local : c'est dans cette catégorie que se place la technique du cloud computing ou l'informatique en nuage.

b- Les problématiques du Cloud computing

---

[331] Pour une version du projet cf. Communiqué de presse du 06 juin 2013 de la Commission Libertés civiles, justice et affaires intérieures sur le site du Parlement Européen : *Des règles communes pour lutter contre les cyberattaques, sous la présidence de Juan Fernando López Aguilar (S&D, ES), REF.: 20130603IPR11005.*

Avec le Cloud *computing* qui est un nouvel arrivant dans le secteur des Technologies de l'Information et de la Communication, quelles incriminations pourront être créées à l'encontre des délinquants et cybercriminels qui vont forcément et inévitablement trouver des moyens de pénétrer ce nouvel environnement, ce nuage informatique par le biais duquel des informations et des données pourront être échangées ?

Le *Cloud computing* est une technologie dite de nuage informatique qui consiste en la création d'un réseau permettant un partage de données entre les ordinateurs de ce réseau. La National Institute of Standards and Technology (NIST) le définit comme « *a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources* (e. g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[332].

Le *Cloud computing* est né dans les années 2000 pour répondre aux besoins de mobilité des utilisateurs des réseaux et d'Internet. Si l'informatique dans les nuages est présentée comme une opportunité pour les entreprises[333], il n'en demeure pas moins qu'elle soulève des difficultés quant à l'externalisation des données à travers leur transfert et la sécurité qui y est liée.

Compte tenu du stockage des informations sur des serveurs en général à l'étranger (principalement des serveurs américains) la question de la loi applicable en cas de problème notamment d'un point de vue contractuel, se pose. Sur ce point, les principaux amateurs de *Cloud* à l'heure actuelle sont Amazon, Google. Or ces prestataires ont leurs serveurs aux Etats-Unis. Ils seront enclins systématiquement à imposer l'application de la loi américaine. Or c'est un dispositif mal connu des entreprises européennes. Il faut

---

[332] P. MELL, T. GRANCE, NIST, the NIST Definition of Cloud computing (Draft), Special Publication 800-145 (Draft), janv. 2011, et pour une version en ligne: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf cité par J-P MOINY in RLDI n°78 de Janvier 2012 dans son article « *Cloud computing : validité du recours à l'arbitrage ? Droit de l'homme et clauses abusives*. L e document a été mis à jour sous le lien suivant: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[333] **BERNAULT C**., Informatique en nuage et données personnelles : quand l'informatique est dans les nuages, les données personnelles s'envolent », Revue Lamy Droit de l'Immatériel, Janvier 2012, n° 78.

remarquer que s'agissant des Etats-Unis, les problèmes sérieux se posent quant à l'hébergement des données mais également des questions d'application de lois et des questions de compétence juridictionnelle.

c- Les incriminations liées aux contenus de messages

Dans la Convention de Budapest, ces incriminations correspondent à la troisième catégorie d'infractions. Cette catégorie est relative aux contenus et regroupe en son sein les infractions liées à la pornographie enfantine, à la prostitution des enfants, à, l'exploitation sexuelle ou encore tout stockage ou téléchargement exercé dans cet objectif[334]. Certaines portent atteinte aux mœurs (1) et d'autres sont attentatoires à la confidentialité de l'information (2).

1- Les contenus illicites portant atteinte aux mœurs

C'est en vue de la transposition de la directive du Parlement européen du 8 juin 2000[335]que la France a introduit la loi du 21 juin 2004 pour la confiance dans l'économie numérique[336]. Parmi les mesures qu'elle apporte au droit français, cette législation a permis d'introduire le dispositif de lutte contre les contenus illicites sur internet notamment en ce qu'elle exige qu'il il faudrait de plus que le caractère illicite de l'information dénoncée soit manifeste ou qu'un juge en ait ordonné le retrait ».

Ce dispositif est renforcé par la loi du 5 mars 2007 relative à la prévention de la délinquance[337]. Il s'agit principalement de contenus portant atteinte aux jeunes publics. Et dans cette catégorie sont insérés les contenus montrant des enfants nus ou les attirant dans

---

[334] Le Rapport explicatif de la convention sur la cybercriminalité est très clair sur la question.cf. STE 185.

[335] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») publiée au Journal officiel n° L 178 du 17/07/2000 p. 0001 – 0016.

[336]Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique parue au JORF n°143 du 22 juin 2004 page 11168 texte n° 2.

[337]Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance publiée au JORF n°0056 du 7 mars 2007 page 4297, texte 1.

les pièges des pédophiles ou encore des sites pornographiques adressés à des mineurs. En définitive, il s'agit de contenus portant atteinte aux mœurs et surtout aux mineurs.

Les contenus illicites peuvent également concerner l'apologie des pratiques racistes, ou fascisme ou encore du nazisme. C'est dans ce cadre qu'avait été rendu l'arrêt Yahoo du 22 mai 2000 qui mettait en cause la publication d'un site d'apologie du nazisme en France. Les juifs de France avaient saisi le Tribunal de grande Instance de Paris pour faire cesser cette atteinte. Le Tribunal de Grande Instance de Paris a donc rendu l'ordonnance en référé du 22 mai 2000 en exigeant des tenants du site Yahoo Inc. le retrait des enchères sur des objets nazis ou antisémites, informations publiés sur le site Yahoo en France[338].

2- La divulgation d'informations confidentielles

Le code pénal français sanctionne à l'article L 411-6, le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation de dix ans d'emprisonnement et de 150 000 € d'amende. Cet article du code pénal français définit les catégories de divulgations d'informations confidentielles uniquement à destination de l'étranger.

Ce qui laisse sous-entendre que la fourniture de renseignement par des nationaux à des entités étrangères est une infraction internationale. D'ailleurs, l'infraction fait partie de la section des crimes et délits contre la Nation. Cette distinction territoriale est cohérente puisque la protection des secrets confidentiels au niveau de l'Etat et notamment en ce qui concerne les entreprises est couverte par les clauses de confidentialité contenues dans les contrats de travail ainsi que les clauses de non-concurrence.

[338] Ordonnance des référés du TGI de Paris, 22 mai 2000, puis ordonnance du Tribunal de Grande Instance de Nanterre 1ère chambre, Section A Jugement du 24 mai 2000.

Sur ce fondement, et d'un point de vue territorial, l'espionnage de données s'assimile à la violation de la confidentialité liée à son emploi et sous cet angle, il peut être défini comme le fait pour un salarié notamment de dérober des informations censées restées confidentielles, pour les communiquer en contrepartie d'une rémunération et donc à des fins commerciales.

Pour ce qui est du droit pénal, l'article 311-1 du code pénal punit l'abus de confiance dans les relations contractuelles par l'article 314-1 d'une part et d'autre part, grâce à l'article 445-1 et 2 du même code. C'est le délit de corruption qui est employé pour sanctionner les actes relatifs à l'espionnage de données par les salariés dans une entreprise. A ce propos, la Chambre Criminelle de la Cour de cassation précise dans sa décision du 22 septembre 2004 que « Constitue un abus de confiance le fait pour un salarié chargé de mettre au point un projet de *borne informatique*, d'en disposer comme d'un bien propre au profit d'un tiers, alors que, dès sa réalisation, le projet était propriété de l'employeur et qu'il n'en était que détenteur »[339].

En appui de cet arsenal législatif, les juges du tribunal de Clermont Ferrand ont le 21 juin 2010, condamné un ancien salarié de la société Michelin[340] pour tentative de divulgation de secrets d'affaires. Il ressort des faits du jugement qu'un salarié de la société de vente de pneumatiques MICHELIN est poursuivi par son ex-employeur, la société MICHELIN pour avoir tenté de vendre des informations liées à la fabrique des produits à une société concurrente, la société BRIGESTONE, une société japonaise. Cette dernière a averti sa concurrente et le salarié a été poursuivi devant les tribunaux pour espionnage industriel.

La société MICHELIN avait été classée en établissement à régime restrictif du fait de son centre de recherches et sur décision interministérielle, l'instruction interministérielle

---

[339] Cour de Cassation, chambre criminelle du 22 septembre 2004, n° du pourvoi : 04-80285, arrêt publié au bulletin criminel 2004 n° 218 p. 777.

[340] Tribunal correctionnel de Clermont Ferrand, 21 juin 2010, l'affaire est reprise par des organismes de presse comme le journal Le monde qui titre dans un article du 22 juin 2010 de Manuel Armand « *L'accusation d'espionnage contre un ex-cadre de Michelin n'a pas été retenue » ;* décision du tribunal commentée par M. VERON dans la revue Droit pénal 2010, commentaire 116 ; voir également la revue Communication Commerce électronique n° 3, mars 2011, commentaire 31, E. A. CAPPRIOLI.

n° 486 du 1er mars 1993 sur la protection du patrimoine scientifique et technique dans les échanges internationaux[341] est intervenue. Le tribunal de Clermont Ferrand a conclu à un simple abus de confiance et non à un espionnage industriel. Le salarié a été condamné à deux ans d'emprisonnement avec sursis et au versement d'une amende de 5000 euros.

Cette affaire MICHELIN révèle que la cybercriminalité peut être facilitée par les salariés sur le lieu de travail. Dès lors, pose la question de la contribution de ces salariés aux attaques informatiques dont sont victimes les équipements de travail c'est-à-dire les systèmes informatiques des entreprises et les outils de communication (téléphones fixes et portables).

A cet effet, la CNIL a établi un guide[342] offrant aux employeurs et aux salariés les outils nécessaires à une information suffisante et adéquate quant à leur utilisation d'internet, afin d'éviter d'une part la violation des libertés fondamentales par l'employeur et d'autre part garantir la confidentialité de certaines informations capitales et confidentielles de l'entreprise.

Les attaques du système informatique peuvent être dues à des actes extérieurs tels les vols de données ou encore l'espionnage industriel provenant de l'extérieur de l'entité ciblée. C'est le cas avec l'affaire du piratage d'AREVA[343]: pendant deux ans, des pirates chinois se sont introduit le site d'AREVA. C'est au moyen de virus Stuxnet que cet espionnage a pu avoir lieu.

C'est en 2010 que le programme malveillant Stuxnet est découvert avec les attaques informatiques contre le programme d'armement nucléaire iranien : ce programme a saboté le processus d'enrichissement de l'uranium[344]. C'est d'ailleurs le

---

[341] Rapport de l'Assemblée nationale n° 4159 du 11 janvier 2012 fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur la proposition de loi (n° 3985) DE M. BERNARD CARAYON visant à sanctionner la violation du secret des affaires.

[342] Cf. : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf

[343] Des hackers complotistes ou des espions industriels? Cf. : http://lexpansion.lexpress.fr/entreprise/areva-victime-d-une-attaque-informatique-de-grande-ampleur_263462.html

[344] Cf. Note d'analyse Mars 2013 n°324 du centre d'analyse stratégique auprès du cabinet du Premier ministre français, voir en ligne également sur www.strategie.gouv.fr

même processus développé par un autre ver deux ans plus tard : le ver FLAME découvert en 2012, qui excelle encore plus que le précédent puisqu'il a la capacité de copier plusieurs fichiers, de mémoriser les frappes de clavier et de déclencher le micro et l'émetteur Bluetooth et peut s'autodétruire à tout moment[345].

Toutes ces attaques ont désormais des objectifs stratégiques puisqu'ils sont en direction d'infrastructures énergétiques des Etats. Elles donnent l'impression d'une guerre froide sous une forme déguisée. Une autre forme d'espionnage est celle mise en place par les drones.

3-L'espionnage par les drones

Les drones sont des machines téléguidées comprenant des données et avec pour objectif de capter des informations militaires spécifiquement. Ces outils pilotés à distance sont utilisés par des chérifs américains aux Etats-Unis pour l'heure mais vont peu à peu intervenir sur les territoires européens et par la suite africains[346]. Ces engins posent problème compte tenu du manque d'encadrement légal à l'heure actuelle.

Les contenus des messages font aussi intervenir les œuvres littéraires. C'est pourquoi, elles sont étudiées dans les incriminations liées aux réseaux et serveurs.

4- Les infractions contre les œuvres littéraires

Il convient de souligner que l'activité législative en matière d'infractions contre les œuvres littéraires notamment – autre pan de la cybercriminalité essaie de respecter l'équilibre entre les sanctions des comportements illicites et cybercriminels et les libertés individuelles telles les libertés d'expression et de communication. Pour illustration, la loi du 28 octobre 2009[347] pour la protection pénale des œuvres littéraires et artistiques sur Internet crée une peine complémentaire de suspension de service de communication en

[345] Idem.

[346] Les drones ont été utilisés par l'armée américaine dans les interventions en Afghanistan. Ces drones font leur apparition dans les milieux militaires européens, les armées européennes étant la plupart du temps, appelées à la rescousse par les pays africains comme ça été le cas récent du Mali pour la gestion de la crise liée à l'islamisation de cet Etat par l'Al Qaida.

[347] Loi n°2009-1311, 28 octobre 2009 : JORF du 29 oct.2009, p. 18290

ligne[348]. Cette sanction est le lien permettant de souligner l'important dispositif mis en place pour lutter contre les téléchargements illicites, autres facteurs favorisant des activités cybercriminelles.

d- Les téléchargements illicites

En informatique, le téléchargement (en anglais *download*) est l'opération de transmission d'informations - programmes, données, images, sons, vidéos - d'un ordinateur à un autre via un canal de transmission, en général[349]. Il peut se faire soit à partir d'un ordinateur distant et dans ce cas, on parle de téléchargement descendant ou *download* vers un ordinateur. Le téléchargement se fait également vers un autre ordinateur et dans ce cas, il s'agit d'un *upload*. Quel que soit le sens du téléchargement (*upload* ou *download*), le mécanisme approprie des données par le biais des moyens techniques.

Parmi ces techniques de téléchargements illicites des œuvres littéraires protégées par le droit d'auteur, se trouvent les partages dits de Peer-to-Peer c'est-à-dire partage de fichiers à fichiers. Cette technique n'est pas illégale en soi. Elle le devient lorsque les pratiquants l'utilisent pour partager des œuvres dont, en principe, l'utilisation nécessite de verser des droits à leurs auteurs et que ces droits ne sont pas versés. En d'autres termes, les utilisateurs se servent du Peer-to-Peer pour échapper au versement de redevances aux titulaires de droits sur les œuvres concernées. C'est souvent le cas dans le monde musical mais également en matière d'œuvres littéraires. Cette expression se traduit en français « pair à pair » et correspond au mode d'utilisation d'un réseau dans lequel chaque utilisateur est en mesure de mettre certaines ressources de son ordinateur à la disposition des autres[350].

---

[348] Droit Pénal, Revue Mensuelle Lexisnexis Jurisclasseur, décembre 2009.

[349] Définition figurant dans le vocabulaire de l'internet paru Journal officiel du 1er septembre 2000, p.215.

[350] Définition tirée du Journal officiel de la République Française n° 11 du 13 mai 2006, p. 7072

Par Peer to Peer, est désigné tout logiciel permettant des échanges et communications de pair à pair, c'est-à-dire d'ordinateur à ordinateur[351].

Le peer-to-peer est assimilable soit à la copie privée soit la contrefaçon en ligne. S'agissant de la copie privée, elle suppose qu'une seule et même personne télécharge une œuvre et l'utilise. Or dans le cas du peer-to-peer, celui qui télécharge et celui qui utilise l'œuvre téléchargée sont souvent différent et dès lors, la manœuvre est une contrefaçon en ligne. En quoi consiste le Peer-to-Peer ? Pour envisager une sanction, quelle peine est imputée à celui qui s'adonne de façon continuelle à une telle pratique de partage ? Est-ce sa responsabilité qu'il engage ? S'expose-t-il à verser des frais de consommation aux titulaires de droits d'auteurs, notamment au titre de la copie privée illicite ?

En France, la recherche de solutions contre ces téléchargements illégaux et notamment des peer-to-peer conduit à analyser les questions relatives aux licences globales. En quoi consistent ces solutions ? Les licences globales sont la possibilité offerte aux internautes moyennant paiement d'une somme forfaitaire d'échanger des œuvres via les réseaux peer-to-peer sans prendre le risque de se voir condamner pour contrefaçon. Et dans ce cas l'acte de téléchargement est considéré comme une copie privée[352]. Cette solution au problème de contrôle des Peer-to-peer avait été proposée en 2006 par le député Christian Paul.

Dans la même année, la sanction envisagée au départ est la contravention de ces téléchargements contenue dans la loi n° 2006-961 du 1er Aout 2006 relative au Droit d'Auteur et aux Droits Voisins dans la Société de l'Information[353] dite « loi DADVSI. C'est grâce à cette loi que la France transpose la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[354]. La sanction n'est pas

---

[351] Livre blanc sur le Peer to Peer, page 41, édition des Parques, Paris, novembre 2005

[352] Cf. Dictionnaire du droit de la propriété intellectuelle de **BERNAULT Carine** et **CLAVIER Jean-Pierre**, Ellipses éditions, Paris, 2008.

[353] Cf. JORF n°178 du 3 août 2006 page 11529 texte n° 1

[354] La directive est parue au Journal officiel des communautés européennes n° L 167 du 22/06/2001 p. 0010 – 0019.

retenue dans la mesure où le Conseil constitutionnel dans sa décision du 27 juillet 2006 a déclaré non conforme à la Constitution une grande partie des mesures votées[355]. Le Conseil constitutionnel reste donc uniquement sur l'application de la sanction de la contrefaçon c'est-à-dire 3 ans d'emprisonnement et 300 000 euros d'amende.

En 2008, Jacques ATTALI remet un rapport au Président de la République, le 23 janvier, préconisant la mise en œuvre de la licence globale comme alternative de contrôle au téléchargement illicite. La licence globale est cependant écartée.

Les critiques adressées aux concepteurs de ces peer to peer conduisent ces derniers à mettre en place des sites légaux et payants ou presque[356]. A l'instar de ces sites de partages de fichiers, le site Skype créé par le fondateur de Kazaa, Niklas Zennström, est un service de téléphonie gratuite basé sur le mode des Peer-to-Peer[357]. Du fait de cette gratuité, Skype a été signalé en France comme opérant des manœuvres contrevenant à la loi. En effet, l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) a en charge de veiller à la déclaration des opérateurs de télécommunications dès lors que ces entités veulent délivrer des services. Le problème de Skype[358], c'est qu'il ne se reconnaît pas ce statut d'opérateur de télécommunication. L'ARCEP a émis plusieurs avertissements à l'endroit de la structure Skype, qui, rappelons-le, est un service de nationalité américaine mais qui délivre des prestations en France, en tant que multinationale[359]. Ces avertissements sont restés sans réponse de la part de Skype.

---

[355] Cf. **DERIEUX E.** et **GRANCHET A.,** lutte contre le téléchargement illégal, collection Lamy Axe Droit, Paris, 2010. Et la décision du Conseil Constitutionnel décision n° 2006-540 parue au JO du 3 août 2006, p. 11541, n°63-65.

[356] « Presque » dans la mesure où le système d'appel utilisé par Skype est gratuit. Les utilisateurs créditent en général leur compte d'appel pour effectuer des communications téléphoniques. Mais lorsqu'il s'agit d'appel d'ordinateur à ordinateur, le service est totalement gratuit.

[357] Cf. **STROWEL A**., le P2P : un problème pressant en attente d'une réponse législative in La propriété intellectuelle en questions : regards croisés européen colloque 16-17 juin 2005, IRPI, éditions LexisNexis, 2006

[358] Skype est un mode de communication gratuite développé par Niklas ZENNSTROM en 2003

[359] Voir le communiqué de presse sur le site de l'ARCEP en date du 12 mars 2013, cf. http://arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5buid%5d=1593&tx_gsactualite_pi1%5bannee%5d=&tx_gsactualite_pi1%5btheme%5d=&tx_gsactualite_pi1%5bmotscle%5d=&tx_gsactualite_pi1%5bbackID%5d=26&cHash=baebcd8ef257d3194065360ecec41a90.

A ce sujet, les sites comme MEGAUPLOAD, site de téléchargement en direct et son attenant MEGAVIDEO, site de streaming[360] font l'objet d'enquêtes depuis 2010 de la part du bureau d'investigation fédéral américain (FBI). La diffusion de flux ou *le streaming* est défini dans le Vocabulaire de l'audiovisuel comme « *le procédé permettant de diffuser un programme par l'internet avant son téléchargement complet* ». Les fondateurs de ces sites sont accusés de violation des droits d'auteurs et de blanchiment d'argent. D'ailleurs, à l'issue des enquêtes lancées, ces dirigeants sont arrêtés par le FBI le 19 janvier 2012[361]. Dans cette affaire, ce qui est prohibé, c'est la pratique de téléchargement directs d'œuvres d'auteurs (pourtant commercialisées du fait des droits qui y sont attachés) pour les partager gratuitement par le biais des Peer-to-Peer à d'autres internautes. Ces pratiques sont contraires au respect des droits des auteurs et la sanction appliquée a été la fermeture des sites interdits dès l'arrestation des fondateurs.

En France, l'organisme en charge de lutte contre les téléchargements illicites est la Haute Autorité Pour La Diffusion Des Œuvres Et La Protection Des Droits Sur Internet (HADOPI). Cette autorité est controversée du fait d'un amendement 138 du Paquet Telecom.

Cette autorité a été mise en place à la suite du rapport OLIVENNES de novembre 2007, qui préconise la lutte contre le téléchargement illégal[362]. C'est par la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet[363], dite Loi HADOPI que les dispositions du code de la propriété intellectuelles ont été modifiées pour intégrer ladite loi en son article L 132-27. Dirigée par des magistrats, l'autorité HADOPI envoie environs 2000 avertissements par jours à des personnes suspectées de partage de films, musiques, textes littéraires[364]. La question qui se pose quant à cette

---

[360] Cf. Vocabulaire de l'audiovisuel paru au JORF n°14 du 18 janvier 2005 page 845, texte n° 89.

[361] cf. Journal Le Monde, partie Technologie du 19 janvier 2012, article de **LELOUP D**., « *La justice américaine ferme le site de téléchargement Megaupload* ». Voir également le journal Le Figaro du 23 janvier 2012 *« Megaupload, 2 arrestations »*.

[362]Cf. **OLIVENNES Denis**, *le développement et la protection des œuvres culturelles sur les nouveaux réseaux*, Ministère de la culture et de la communication, novembre 2007.

[363] cf. Loi du 12 juin 2009 parue au JORF n°0135 du 13 juin 2009, texte n°2

[364] **BRANCO Juan**, Réponses HADOPI suivi d'un entretien avec Jean-Luc GODARD, éditions CAPRICI.

autorité est celle de la portée de ses interventions. En d'autres termes quelle est l'efficacité d'une telle structure non seulement en termes de contrôle mais également en termes de répression ? Dans sa décision du 29 juillet 2004, le Conseil constitutionnel français a précisé que « Lutter contre les nouvelles pratiques de contrefaçon qui se développent sur le réseau internet (…) répond à l'objectif général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle ». En effet, les chiffres d'études officielles révèlent d'importantes infractions dans le domaine[365]. Dans ce cadre, le Centre National du Cinéma en collaboration avec l'association contre la piraterie audiovisuelle (ALPA) font état de ce que près de 94% des films piratés sur internet sont disponibles avant leur sortie vidéo en France et 40% des films sortis en salle en 2006 sont piratés sur internet l'année de leur sortie. L'efficacité et l'importance d'HADOPI ont été remises en cause par des internautes qui soulèvent la possibilité par exemple de créer de fausses adresses IP pour brouiller les pistes des autorités[366]. Il faut ajouter qu'en réponse à la recherche de sanction contre le téléchargement illicite, la responsabilité des éditeurs de logiciels avec les dispositions de l'article L 336-1 du code de la propriété intellectuelle qui impose une décision du Président du tribunal de grande Instance statuant en référé en vue d'ordonner des mesures techniques comme filtrer des fichiers échangés. Cette mesure est le volet civil de la sanction. Elle a un volet pénal qui est contenu dans l'article L 335-2 du même code qui lui prévoit une peine de 3 ans de prison et de 300000 euros d'amende. Cette peine est celle prévue en cas de contrefaçon.

En France, après les vives tensions pour mettre en place la loi HADOPI 1, les modifications ont été intégrées pour donner naissance à HADOPI 2. Ce dispositif

---

[365]Cf. **DERIEUX Emmanuel** et **GRANCHET Agnès**: lutte contre le téléchargement illégal: lois DADVSI et HADOPI, Edition LAMY, France, 2010**.**

Voir également le Rapport « offre pirate de film sur internet, publié en 2007 par le centre national de la cinématographie :http://www.cnc.fr/CNC_GALLERY_CONTENT/DOCUMENTS/publications/etudes/Piraterie_121007.pdf.

[366] « *Hadopi, Loppsi 2… la succession de textes diabolise internet, sans pour autant apporter des réponses viables à son contrôle »* suivi d'une interview de l'interview de GUILLAUME LOVET, responsable de l'équipe de lutte contre les menaces informatiques de l'éditeur de solutions antivirus Fortinet cf. Magazine Capital du 16 juin 2009.

législatif répond à l'objectif de lutter efficacement contre le téléchargement illégal et protéger les droits d'auteurs notamment en matière de musique et d'œuvres cinématographiques. Et pourtant, il est déjà question de remise en cause de l'HADOPI et de sa suppression du fait des vives tensions générées par le texte créant cette haute autorité ainsi que les sanctions contre le téléchargement illégal qu'il prévoit. Le rapport LESCURE rassemble l'ensemble des propositions en faveur d'une suppression de la Loi HADOPI et par conséquent de l'autorité qu'elle a mise en place. Le rapport LESCURE est un document qui a été remis au Président de la République française le 13 mai 2013, à la suite de la mission LESCURE. Cette mission composée de magistrats et de techniciens du droit a reçu pour sujet de réflexion l'exception culturelle et l'autorité en charge du respect des droits d'auteurs. Par ailleurs, le téléchargement et son encadrement juridique sont au cœur des préoccupations du rapport LESCURE. L'ensemble de ces réflexions a conduit à envisager d'autres solutions pour lutter contre le téléchargement illicite comme la réponse graduée faisant de nouveau intervenir la HADOPI.

La réponse graduée consiste d'abord en une mise en demeure ou un avertissement par courrier électronique ou par Lettre recommandée adressée à l'internaute qui s'adonne au téléchargement. Ensuite, si l'avertissement reste sans effet ou de changement de la part de l'internaute, une sanction financière de 38 euros pour le téléchargement et 150 euros pour la mise à disposition de fichiers, est prévue. Cette sanction pécuniaire est contenue dans les dispositions de l'article L 335-2 du Code de la propriété intellectuelle.

Le Journal d'informations quotidiennes Metro du 11 décembre a publié un article[367] faisant apparaître les statistiques de l'institution HADOPI quant à cette réponse graduée. A partir des données chiffrées proposées de 2009 au 30 juin 2013, un tableau peut être fait. Il peut supporter l'analyse de la réponse graduée proposée comme solution au téléchargement illicite en France.

Mesures ou sanctions	Chiffres sur la période observée 2009-

[367] Cf. Journal Metro News du 11 décembre 2013, article de **ZANCHI Jean-Sébastien** « *La HADOPI vante le payant* », p. 4 et 5.

	Juin 2013
Premier mail d'avertissement	1.912. 847
Second mail d'avertissement	186. 153
Etude de dossier par la Commission de protection des droits en cas de piratage avéré sur une période de 12 mois	663
Délibération de l'HADOPI, dossiers transmis ou non au Parquet. En cas de procès 1500 euros d'amende.	51

Tableau des chiffres de la réponse graduée d'HADOPI de 2009 à juin 2013

En l'analysant, ce tableau traduit l'efficacité des avertissements. C'est surtout le fait de payer une amende pour avoir téléchargé de manière illicite ou encore pour avoir mis à disposition des fichiers qui semble dissuasif pour les internautes. La différence entre chiffres relatifs aux premiers mails avertisseurs et les dossiers effectivement transférés au Parquet est énorme.

Chez nos voisins britanniques, la pratique des avertissements peine à être de mise. L'entrée en vigueur du *"Digital* Economy Act*"*, qui introduit un dispositif de réponse graduée contre le téléchargement illégal au Royaume-Uni a été récemment repoussée[368]. Cette loi, à l'image de la loi française HADOPI prévenant les internautes va plus loin dans la mesure où elle prévoit en plus d'avertir les internautes concernés, de les ajouter à une liste noire consultable par les ayant-droits en cas de deux récidives[369].

En Allemagne, le texte punit le téléchargement illégal de cinq ans de prison avec un seul avertissement à l'internaute contrairement à la France où la loi prévoit trois

[368] Cf. "*Royaume-Uni : la loi contre le téléchargement illégal repoussée* », in Journal Le Monde du 27 avril 2012, voir également sur www.lemonde.fr

[369] http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf

avertissements avant de punir. La sanction dépend du moment de la commission du téléchargement illégal. Le fait d'être pris flagrant délit de téléchargement illégal entraîne pour l'internaute une peine de prison entre 3 et 5 ans de prison, ou une amende proportionnelle à ses revenus. Par ailleurs, la loi peut obliger les Fournisseurs d'Accès à Internet (FAI) à livrer les données personnelles d'internautes suspectés de piratage à des ayants droit qui s'estiment lésés[370].

Quant à la Suède, le piratage est sévèrement sanctionné grâce à la loi anti piratage *Ipred* entrée en vigueur le 1er avril 2009 : elle donne le droit aux ayant-droits d'œuvres de collecter les adresses IP des pirates présumés. D'ailleurs, les applications ne se sont pas faites attendre dans la mesure où ce dispositif a permis de sanctionner les quatre responsables du site The Pirate Bay à un an de prison et à 2,7 millions d'euros de dommages et intérêts.

L'arrêt mérite de connaître les circonstances puisque la décision des juges suédois a été approuvée par la Cour Européenne des Droits de l'Homme dans son arrêt du 19 février 2013[371]. Il ressort des faits que la société The Pirate Bay favorise le recours aux partages de fichiers sans respect des droits d'auteurs. Pour ces faits, le tribunal suédois a condamné ses responsables, en 2009, pour complicité d'atteinte au copyright à raison d'un an d'emprisonnement et à verser 3,3 millions d'euros en guise de dommages et intérêts aux victimes. Les responsables, font appel et la Cour d'appel de Svea les condamne à nouveau en 2010. S'estimant lésés et notamment sur le plan de leur liberté d'expression, les responsables de The Pirate Bay envisagent de saisir la Cour Suprême, qui refuse leur saisine. Ils saisissent de ce fait la Cour Européenne des Droits de l'Homme afin de faire valoir leurs droits. Devant la Cour Européenne, Niel et Sunde, les co-fondateurs de The Pirate Bay soulèvent l'article 10 de la Convention Européenne des Droits de l'Homme et du Citoyen.

---

[370] cf. « Du laisser-faire à la loi : ce que font les autres pays contre le piratage », Journal Le Monde du 13 mai 2009, p. 11.

[371] cf. CEDH 5è section, requête 40397/12, Neij et Sunde Kolmisoppi c. Suède du 10 janvier 2013.

Pour rendre leur décision, les magistrats de la Cour Européenne font la balance entre le recours illégal aux partage de fichiers lésant les ayant droits et la violation nécessaire de la liberté d'expression des requérants. La Cour a précisé *qu'eu égard en particulier à la nature des informations partagées et aux raisons solides invoquées, l'ingérence dans l'exercice par les requérants de leur liberté d'expression était nécessaire dans une société démocratique* ».

L'exemple suédois devrait servir de support dans d'autres Etats même si la loi est sévère et semble donner un pouvoir aux ayant droits. Malheureusement, ce n'est pas dissuasif pour les pirates qui créent dès l'année suivante une technique de contournement de la loi.

Cette inefficacité conduit des pays comme l'Espagne à refuser ce genre de législation. Il en va de même pour la France.

Aux Etats-Unis d'Amérique, dans un arrêt GROKSTER du 27 juin 2005, arrêt Metro-Goldwyn- Mayer Studios Inc. v. GROKSTER, 545, US, 27 juin 2005, la Cour suprême américaine corrige la conception de la responsabilité des producteurs dans le partage des fichiers P2P notamment en ce qui concerne la contrefaçon des œuvres musicales.

Il ressort de ce paragraphe que les sanctions contenues dans les différentes incriminations concernent deux catégories de personnes : d'une part les délinquants qui commettent des infractions, soit contre les supports informatiques, soit contre les réseaux mobiles ou encore à l'encontre des réseaux de télécommunication ; d'autre part, ce sont les responsables des services à l'instar des fournisseurs d'accès internet, des responsables d'entreprises en charge de traitement qui sont sanctionnés notamment lorsque leur responsabilité est mise en cause ou engagée. Au titre de la responsabilité, il faut observer que les prestataires de service et les hébergeurs sont la plupart du temps indirectement visés à la suite des activités illégales opérées sur les réseaux et les serveurs dont ils assurent la gestion.

Du point de vue des peines prévues pour punir la cybercriminalité, elles revêtent essentiellement la forme de peine de prison, d'amendes financières, d'interdiction d'exercer une activité professionnelle, d'interdiction d'accès au matériel informatique et aux systèmes afférents et de responsabilités civile et pénale. Les sanctions dépendent

également de la nature juridique des personnes en cause c'est-à-dire qu'il peut s'agir de personnes physiques, de personnes morales ou d'Etats.

En présence de personnes physiques, toutes les peines a priori ont vocation à s'appliquer en fonction du degré de gravité des infractions commises. Il en va autrement pour des personnes morales et des Etats pour qui, le niveau de responsabilité est établi en fonction du dirigeant et des pouvoirs délégués ou non dans le cadre de la commission des infractions cybercriminelles.
Par exemple, dans le cas d'un salarié qui commet une intrusion frauduleuse sur ordre de son supérieur hiérarchique ou dans le contexte de ses attributions dans l'entreprise, la responsabilité sera certes celle du salarié mais pour l'entreprise, personne morale, c'est la qualité de dirigeant du supérieur hiérarchique qui contribue à définir la responsabilité en supplément. L'amende (peine retenue dans ce cas) est, de ce fait, fixée en fonction de ces paramètres.

Toutes les incriminations étudiées supposent une analyse cohérente pour évaluer dans quelles mesures les sanctions affiliées peuvent effectivement être mises en place. Ce travail est le rôle des juges.

Le rôle des juges quant à ces incriminations met en lumière les politiques de lutte contre la cybercriminalité

§2- Le rôle des juges dans la lutte contre la cybercriminalité

La détermination de la compétence permettra de mieux appréhender les rôles respectifs des juges dans la lutte contre la cybercriminalité, cette criminalité transversale. Elle soulève donc des questions de compétences particulières du fait des différentes incriminations possibles d'une part et d'autre part, elle permet de préciser des questions relatives à la compétence territoriale. Trouver la compétence territoriale suppose de définir un critère de rattachement.

La théorie du critère de rattachement, propre au droit international privé est de mise en l'espèce. L'absence de frontière qu'implique la cybercriminalité suggère de

rechercher ce critère. C'est cet élément qui permet de déterminer le juge qui connaît de l'affaire et par conséquent sanctionne le cybercriminel. Une fois la compétence territoriale attribuée, se posent les questions de compétence de fond. Sous cet angle, plusieurs spécialités interviennent et méritent d'être explicitées. Différentes procédures interfèrent simultanément. A ce stade, mention doit être faite du rapprochement des procédures pénales des Etats membres de l'Union européenne notamment avec des résolutions comme celle relative à l'interception légale des télécommunications en date du 17 janvier 1995[372].

Pour une approche analytique du travail des juges dans le domaine de la cybercriminalité, il est intéressant de comparer le travail des juges dans les Etats de l'Union Européenne d'une part et d'autre part d'observer comment le juge communautaire appréhende les questions relatives à la criminalité numérique. Un axe sous-jacent aux deux premiers, est la part contributive de l'arbitre dans la résolution des questions de répression d'actes cybercriminels. Dans la mesure où la résolution des litiges de manière générale, ne lui est pas confiée naturellement (comme c'est le cas pour le juge), il faut envisager le rôle de l'arbitre au niveau des Etats et au sein de l'Union européenne.

A- La compétence des juges nationaux dans les affaires cybercriminelles

Le juge se voit attribuer des compétences en fonction de critères de rattachement précisés par les textes de lois ou issus des liens de l'affaire à un territoire considéré. C'est en cela que la compétence légale rejoint le plus souvent la compétence juridictionnelle. Il arrive souvent que ces deux chefs de compétence ne coïncident pas. Dans ce cas, la loi compétente trouve à s'appliquer mais les faits concernés écartent la compétence du tribunal ou de la juridiction saisie. A titre d'illustration, la Cour d'appel de Grenoble dans sa décision du 10 décembre 2013 a écarté la compétence du tribunal de Grenoble dans une affaire mettant en cause des propos tenus sur un blog belge, alors que la loi française

[372] Résolution du 17 janvier 1995 parue au Journal Officiel des Communautés Européennes n° C 329 du 4 novembre 1996, p. 1.

était compétente pour juger des faits considérés[373]. Il ressort des faits à l'origine de l'arrêt que monsieur P., policier affecté à la direction du renseignement de Lyon, en France, et domicilié en Belgique s'est rendu coupable, lors de son congé maladie longue durée, de révélations d'informations secrètes relatives à l'organisation d'une antenne de police. Il a procédé à la communication d'informations confidentielles par le canal de son blog tenu en Belgique. Il a donc été entendu par les juges et ceux du premier degré l'ont condamné sur le fondement de l'article L 226-13 du code pénal à une peine d'emprisonnement de 2 mois avec sursis. En appel, les juges ont déclaré les juridictions françaises incompétentes compte tenu du fait qu'aucun acte de procédure n'a été adressé à Monsieur P. en France. Tous les actes lui ont été adressés en Belgique au lieu de sa résidence et de son domicile connu des services de police.

En matière de cybercriminalité puisqu'il faut partir de l'absence de frontière d'internet et des réseaux numériques, comment est réglée la question de l'attribution de compétence territoriale ?

Une fois la compétence territoriale trouvée, comment les compétences d'attribution vont-elles s'exercer ?

a- La détermination de la compétence territoriale

En matière de compétence territoriale, l'article 23 de la Convention de Budapest est très général en précisant des options de compétence : « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:*

a sur son territoire; ou

b à bord d'un navire battant pavillon de cette Partie; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou

[373]Cf. Cour d'appel de Grenoble 1ère chambre Arrêt du 10 décembre 2013, consultable sur http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3988.

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat. (…)

La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée, visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites».

L'article 22 de la Convention organise la détermination de la compétence de manière à ce qu'il y ait au moins un juge compétent. Ce choix multiple de critères de compétence n'est pas toujours facile à mettre en œuvre et différentes décisions de justice permettent de s'en rendre compte. En matière de cybercriminalité, la question se situe plus au niveau des délits que des contrats mais certaines qualifications soumises à hésitations impliquent d'analyser toutes les hypothèses.

Le juge est territorialement compétent soit parce que la théorie de l'accessibilité est retenue, soit du fait de la théorie de la focalisation. Les différentes décisions de justice permettent d'appréhender ces deux théories.

Concernant la théorie de l'accessibilité, c'est la possibilité de diffusion des contenus au public par le site, qui définit la compétence territoriale du juge.

C'est dans ce cadre que la jurisprudence reconnaît dans l'ordonnance rendue en référé, appelée communément[374] *arrêt Yahoo* du Tribunal de Grande Instance de Paris en date du 22 mai 2000, la compétence des juridictions françaises dès lors que le site concerné était accessible en France. Il ressort des faits qui ont donné lieu à cet arrêt qu'une publicité pour des objets nazis en ventes aux enchères sur le site Yahoo a été adressée en France aux usagers de ce site. Le problème essentiel de cet arrêt est la compétence des juges français à connaître d'une affaire de vente aux enchères d'objets nazis sur un site internet.

---

[374] Décision dénommée « arrêt YAHOO » dans le langage des juristes alors qu'il s'agit d'une ordonnance rendue en référé par le Tribunal de grande Instance de Paris le 22 mai 2000.

La solution qui est retenue est la compétence de la juridiction française en s'appuyant sur le fait que *« en permettant la visualisation en France de ces objets et la participation éventuelle d'un internaute installé en France à une telle exposition-vente, Yahoo! Inc. commet une faute sur le territoire français* » et « *que le dommage étant subi en France* ». Le juge retient donc le fait que l'infraction ait été commise sur le territoire mais également le fait que les dommages aient été subis en France. Cette décision de référé prise par le juge pour faire cesser la diffusion de ventes aux enchères d'objets nazis soulève la question de compétence relancée plus tard dans d'autres cas. La consécration de cette théorie se fait par la Chambre civile de la Cour de cassation française avec l'arrêt *Cristal* de 2003.

L'arrêt *Cristal* du 9 décembre 2003[375] a été l'occasion de soumettre à nouveau à la première chambre civile de la Cour de cassation la question de la compétence des juridictions françaises pour la réparation de dommage subi sur le territoire français. De l'espèce, il faut retenir que la société Louis Roederer est un propriétaire de champagne ainsi que sur les contenants de sa production à savoir la bouteille. Cette bouteille a une forme particulière et cette forme est répertoriée comme une marque du fait de sa forme et avait pour nom « *Cristal* ». La société *Castellbajac*, en Espagne, a commercialisé sans autorisation cette bouteille en la présentant sur son site web alors que le propriétaire Louis Roederer l'a créée expressément pour le territoire français. L'argument que la société espagnole fait prévaloir est celui du territoire limité aux consommateurs espagnols. Il a été reproché aux juridictions françaises de ne pas tenir compte de l'absence de frontières du web[376]. Ces reproches se sont accentués avec le caractère instable du critère retenu pour statuer sur la compétence du juge français. En effet, les critiques de cette théorie soulèvent la crainte du *forum shopping* c'est-à-dire « le stratagème pour échapper à l'application d'une loi et consistant, pour un plaideur à porter son litige devant une juridiction étrangère, qui ne sera pas obligée d'appliquer cette

[375] Arrêt de la première chambre civile de la Cour de cassation du 9 décembre 2003, publié au bulletin 2003, I, n° 245, p. 195.

[376] Cf. **LARDEUX G.,** revue Lamy Droit de l'immatériel n° 81.

loi»[377]. Il s'ensuit la naissance d'un mouvement contraire des juges du fond quant à la détermination des critères de compétence. Ce mouvement est amorcé par la Cour d'appel de Paris[378] le 6 juin 2007. Selon les faits, la société AXA et son groupe (Avansur et Direct Assurances) constate que lors de l'utilisation du moteur de recherche Google, la saisie des termes AXA, Directe Assurances et AGIPI, fait apparaître des annonces publicitaires pour des sociétés qui sont concurrentes. La société AXA assigne alors Google Inc. et Google France devant le Tribunal de Grande instance pour contrefaçon de plusieurs marques. Le juge de première instance se déclare compétent et rend une ordonnance dont Google interjette appel le 8 août 2006. Pour écarter la compétence des juges français, le juge d'appel s'appuie sur le fait que les sites dont il est question sont hébergés à l'étranger et que par conséquent, le tribunal de grande instance de Paris n'est pas compétent. L'affaire arrive en cassation et dans son arrêt du 23 novembre 2010[379], la Chambre commerciale de la Cour de cassation annule la décision d'appel quant à l'incompétence du juge français. La haute Cour renvoie les parties devant la Cour d'appel, estimant les juridictions françaises compétentes. Le critère de l'accessibilité n'est pas satisfaisant compte tenu de l'insécurité juridique qu'il crée. C'est pourquoi, la seconde théorie, qui, elle, retient la compétence à la suite d'analyse de faisceaux d'indices, est retenue.

La théorie de la focalisation est issue de la pratique des tribunaux américains depuis l'arrêt de la Cour Suprême dans une affaire *International Shoe Co contre Washington*[380] du 3 décembre 1945. La compétence du juge est déterminée en fonction d'un faisceau d'indices.

Dans de nouvelles décisions, la chambre criminelle de la Cour de cassation s'est fondée sur la théorie de la focalisation et ce, notamment dans l'arrêt *Le Monde* du 9 septembre

---

[377] cf. Lexique des termes juridiques, p. 414, 19ème édition, Dalloz, Paris 2012.

[378] Cour d'Appel de Paris, 4e ch., sect. A, 6 juin 2007, Sociétés Google Inc. et Google France c/ Axa et autres.

[379] cf. Chambre commerciale de la Cour de Cassation. 23 novembre 2010, n° de pourvoi: 07-19543, voir aussi sur www.legifrance.gouv.fr

[380] Cour Suprême, International Shoe Co contre Washington, 3 déc. 1945, 326 US.310.

2008[381]. En l'espèce, dans le cadre de son contrat de rédacteur qui le lie à la société française, éditrice du Journal Le Monde, monsieur Antonio Z, de nationalité italienne rédige un texte destiné à l'exclusivité du journal Le Monde intitulé « Fatwa à l'italienne ». Sans l'autorisation de l'auteur Antonio Z, ni de la société éditrice du journal Le Monde, Monsieur Giuliano X a reproduit, dans la parution datée du 9 octobre des éditions papier et électronique du quotidien italien Il Foglio, l'intégralité du texte exclusif sus-mentionné et ce, dans le cadre d'un article intitulé " *Antonio Z...sostiene che l'Elefantino vuole ammazarlo* " (Antonio Z...soutient que l'Éléphanteau veut le tuer). La cour d'appel a condamné Monsieur Giuliano X à payer la somme de 10 000 euros pour contrefaçon par édition et par diffusion. La Cour d'appel s'est fondée sur la nationalité française de la victime, la diffusion du journal en France et l'accessibilité de la version internet sur le territoire français. Monsieur Giuliano X s'est pourvu en cassation en estimant que la juridiction française n'est pas compétente. La Cour de cassation casse l'arrêt de la Cour d'appel au motif qu'elle n'a pas suffisamment motivé sa décision et n'a pas répondu qu'aux conclusions du prévenu.

Pour suivre cette nouvelle vague jurisprudentielle, *l'arrêt du 14 décembre 2010*[382] a été l'occasion pour la chambre criminelle de fonder la répression d'un acte de contrefaçon sur le fait que *« le site incriminé soit orienté vers le public français »*. Les faits qui ont conduit à rendre cette décision sont les suivants : le site internet " *www. universal.music.de* " a publié, sous formes d'extraits musicaux, des chansons tirées de plusieurs albums de M. Y..., dit Z.

Ce site est hébergé en Allemagne et exploité par la société allemande Universal Entertainment GMBH, dirigée par Monsieur X, de nationalité allemande. Dans sa mission d'assermenté de l'agence pour la protection des programmes, un agent a constaté cette publication. Or, Monsieur Y n'avait pas autorisé la diffusion de ces phonogrammes. Il fait alors citer le dirigeant, Monsieur X, devant le tribunal correctionnel du chef de contrefaçon. Le tribunal a déclaré le dirigeant coupable. Monsieur X a soulevé l'exception

[381] Crim. 9 septembre. 2008, n° de pourvoi 07-87281.

[382] Crim. 14 décembre 2010, n° de pourvoi 10-80088, Dalloz 2011, p. 1055, obs. Dreyer E.

d'incompétence en faisant valoir que la loi française n'était pas applicable dès lors que la contrefaçon n'avait pas été commise en France. La Cour d'appel a écarté l'exception d'incompétence et a déduit de plusieurs éléments, qu'en dépit de sa rédaction en langue allemande, le site est destiné au public français. Ses arguments tiennent premièrement à la constatation des faits sur le territoire national, deuxièmement à l'appartenance des chansons de Z..., artiste-interprète français, au répertoire de la musique française, troisièmement à l'absence de la traduction des titres de la musique en allemand sur le site litigieux et quatrièmement au fait que les icônes permettant de faire fonctionner celui-ci (le site) ne nécessitent pas la connaissance de cette langue. Monsieur X se pourvoit alors en cassation.

Selon la Cour de cassation, ces motifs utilisés par les juges du fond ne suffisent pas à déduire que le site est orienté vers le public français. La haute Cour casse l'arrêt en estimant que l'un des éléments constitutifs de l'infraction, que constitue la perpétration sur le territoire français, n'existe pas en l'espèce. La Cour de cassation renvoie l'affaire devant la Cour d'appel de Paris.

En commentant cette nouvelle ère jurisprudentielle du critère de fondement de l'attribution de la compétence juridictionnelle, M. Sylvain BOLLEE a souligné à juste titre que cette prise de position salutaire pourrait aller à l'encontre de l'effectivité répressive[383]. En fonction de la technique retenue que ce soit l'accessibilité ou la focalisation, l'étendue de la compétence varie : Compétence globale ou compétence locale.

Il convient de noter la particularité des conditions d'attribution des compétences territoriales en Allemagne. Cet Etat est gouverné par la théorie de la territorialité d'une manière générale et de manière spécifique une application double de la théorie de la territorialité et de la théorie de l'ubiquité (Übiquitätstheorie) prévue à la section 9 StGB[384].

---

[383] Cf. **BOLLEE S**., Rapport de synthèse in Revue Lamy Droit de l'Immatériel, n° 81, p. 123

[384] Cf. **SIEBER Ulrich**, Cybercrime and jurisdiction, op. cit. p. 188 et s.

La théorie de l'ubiquité consiste dans le fait de tenir compte à la fois du lieu de commission d'un acte et du lieu de ses effets. C'est dire que les critères de détermination de la compétence du juge sont la commission de l'acte incriminé sur le territoire allemand et la production des effets sur le même territoire. Selon CHILSTEIN, la théorie de l'ubiquité revient à utiliser en les juxtaposant les théories de l'action ou du résultat : c'est-à-dire les consacrer indifféremment l'une et l'autre[385].

On ne tient pas compte de la diversité des incriminations dans cette théorie pour attribuer la compétence répressive au juge. Cette théorie est appliquée aux cyber-délits bien que cette application ne soit pas exempte de critiques.

Les règles de compétence sont à la fois légales et juridictionnelle. Elles tiennent compte de ces deux critères.

Les compétences territoriales ainsi envisagées soulèvent la question relative à l'exercice des compétences d'attribution aux juges ?

b- Les critères d'attribution de compétence

La compétence territoriale se détermine par rapport à plusieurs indices.

Il s'agit des parties en présence à savoir les Etats, les personnes physiques ou morales, de la nature des faits ou des actes juridiques (contrats ou délits) mais également en fonction des liens existants.

Il revient à la chambre criminelle de la Cour de cassation d'étudier les dossiers relatifs à la cybercriminalité. Le rôle de la haute juridiction consiste surtout à veiller à assurer, dans la réalité des condamnations, le facteur d'aggravation expressément prévu par la loi[386].

Cette précision se veut importante. Elle rappelle le principe fondamental de la légalité des délits et des peines : « pas de légalité sans texte »[387]. Autrement dit, les magistrats de la

[385] Cf. **CHILSTEIN D.**, droit pénal international et lois de police, Essai sur l'application dans l'espace du droit pénal accessoire, Dalloz, Nouvelle bibliothèque des thèses, 2003, p. 167.

[386] Cf. **QUEMENER M.**, Cybercriminalité, droit pénal appliqué, édition Economica, 2010.

Cour de cassation ne peuvent pas se contenter de donner le sens législatif aux textes relatifs à la cybercriminalité. C'est dire qu'ils ne peuvent expliciter ou n'apporter leurs lumières que sur des dispositions contenues dans les textes de lois. Il s'agit du principe de l'interprétation stricte de la loi pénale. Et dans la mesure où les sanctions et incriminations sont relatives au fond du droit, c'est une interprétation stricte qui leur est appliquée et non une interprétation extensive, utilisée pour les lois de procédure[388]. Et cette règle est tout à fait respectée. En cela, les compétences des juges de la Cour de cassation doivent être spécifiques.

En outre, le rôle de la Cour de cassation est de fixer les contours juridiques des moyens d'investigation dans le cadre des recherches de preuve[389].

En effet, si la recherche du gain facile et rapide est généralement le mobile des cybercriminels, cette hypothèse n'est pas exclusive. La prolifération des techniques de spamming, de « fausses promesses de richesses[390] sous réserve de divulguer des données bancaires via Internet sont des exemples et justifient dans une certaine mesure que ces affaires soient confiées aux sections financières et économiques de la Cour de cassation.

Il existe cependant d'autres raisons qui poussent les cybercriminels à commettre leurs exactions, ces crimes pouvant revêtir alors d'autres formes. C'est pourquoi, dans les affaires pouvant faire intervenir des mineurs, nécessitant des enquêtes approfondies, il est fait appel aux juges des mineurs, au juge d'instruction, aux juges de la Détention et des Libertés, mais aussi au juge civil. De la sorte, certains délits liés aux systèmes d'information et réalisés dans un but ludique ou académique sont souvent traités au civil. C'est notamment le cas lorsqu'il est question d'exercice de la liberté d'expression. Dans une ordonnance prise en référé en date du 26 mai 2003, le Tribunal de Grande Instance de

---

[387] L'article 111-3 du Code de 1993 reformule le même principe : « Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement. »

[388] **BOULOC B**., Précis Dalloz, Procédure pénale, 23eme édition, Paris, 2012.

[389] **CHARPENEL Y**., Cybercrime : Jurisprudence de la Cour de cassation, Cahier de la Sécurité n° 6, octobre 2008, INHES (Institut National des Hautes Etudes de Sécurité).

[390] Comme c'est le cas avec les promesses d'héritage de Bill Gates ou d'un riche souverain africain, envoyées par mail via des *spams*.

Paris a statué sur l'envoi massif d'e-mail dans une boîte électronique en estimant que « *dépasse l'exercice normal de la liberté d'expression l'envoi massif d'e-mails dans une boîte de réception afin de bloquer celle-ci, cette manifestation électronique ayant un objectif caractérisant une intention malicieuse* ».

D'autres délits dont la réalisation est facilitée par les systèmes d'information (délits de droit commun, vol, escroquerie, attaques de sites commerciaux, Denis de Service Distribué ou Distributed Denial of Service c'est à dire des déni de service (*DDos),*ou (il s'agit pour des cybercriminels d'utiliser des attaques virales ou des logiciels malveillants comme des chevaux de Troie, pour paralyser des interfaces de services publics par exemple l'interface d'accueil en ligne de la Caisse d'Allocations Familiales. Ces attaques bloquent les pages ciblées, créant une panne qui bloque le système informatique et les rende inaccessible par les usagers et inopérant pendant un certain temps. Ce type d'actes malveillants est jugé au pénal.

Les choix comparatifs opérés quant aux pays sont dépourvus de toute connotation particulière. Il s'agit d'une volonté de comparer des systèmes de culture judiciaire différents bien que tous les pays se réclament de l'Union Européenne.

Cette comparaison suppose de s'interroger sur le déroulement des procédures selon que l'institution du juge d'instruction est maintenue ou supprimée. En effet, cette précision est de taille dans la mesure où les attributions de compétence pourraient modifier les modes d'investigation ainsi que les méthodes de travail à l'égard de la criminalité informatique.

Dès lors, il convient de distinguer les procédures pénales intégrant le juge d'instruction de celles qui l'écartent (1).

1- Les procédures pénales avec juge d'instruction

En droit français, la composition des juridictions pénales et leur fonctionnement imposent un travail collaboratif de la part des juges. C'est ainsi qu'interviennent à concurrence de leur compétence, le juge d'instruction, le juge des libertés et de la détention et le juge de l'application des peines ou encore le Procureur de la République.

En ce qui concerne le juge des libertés et de la détention (JLD), traditionnellement, ce juge a pour compétence de déterminer les délais de sortie ou de renouveler ou encore de décider de la durée de détention d'une personne punie d'une peine d'emprisonnement.

Le JLD a des compétences particulières en matière de cybercriminalité puisque la loi lui donne pouvoirs pour autoriser des interceptions, et ce, sur requête du Procureur de la République. Cet aspect montre bien la collaboration entre les différents juges qui interviennent sur une affaire. D'ailleurs, ce n'est qu'à la suite de cette autorisation, que le juge d'instruction instruira à charge et à décharge les faits qui auront été commis. S'agissant de ce dernier, il a un rôle fondamental en matière de collecte de preuves et d'investigations qu'il s'agisse d'enquête préliminaire, de flagrance ou autre.

En clair, le juge d'instruction et le juge des libertés et de la détention interviennent à compétence partagée selon qu'il y a instruction, enquête ou flagrance. Ils interviennent en effet, tous les deux selon le moment pour les réquisitions informatiques ainsi que les perquisitions de la même nature.

En France, l'alinéa 2 de l'article 60-2 du code de procédure pénale dispose que : « *l'officier de police judiciaire intervenant sur réquisition du Procureur de la République préalablement autorisé par ordonnance du Juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs. De cette disposition légale, il ressort explicitement que c'est au Juge des libertés et de la détention que revient le pouvoir d'autoriser l'OPJ à effectuer des réquisitions informatiques* ». Ce pouvoir est toutefois reconnu au Juge d'instruction en cas d'enquête, lors de la phase d'instruction. C'est l'article 99-4 du code de procédure pénale, cette fois qui contient la disposition. Au stade de l'enquête préliminaire, c'est l'article 77-1-1 du même code qui confère au Procureur de la République, la possibilité d'autoriser les réquisitions en général et particulièrement celles informatiques. D'ailleurs sur ce point, la chambre criminelle de la Cour de cassation dans son arrêt du 22 novembre 2011 applique ce

texte[391]. Des faits, il ressort que dans le cadre d'une enquête de transferts de stupéfiants commis en bande organisée, le Juge d'instruction a donné l'autorisation aux officiers de police judiciaire de procéder à toutes remises de documents permettant de rapporter la preuve des faits, y compris une réquisition judiciaire sur une ligne de téléphonie auprès d'un opérateur de télécommunication.

Parallèlement à cette réquisition, le Procureur de la République a également autorisé une réquisition. Les personnes présumées coupables saisissent le juge pour voir annuler les réquisitions informatiques pour violation de leur vie privée du fait de cette interception. Sur la question, le juge de cassation répond que : «les juges ont fait une exacte application de l'article 77-1-1 du code de procédure pénale et du texte conventionnel invoqué, dès lors que la remise de documents au sens du premier de ces textes s'entend également de la communication, sans recours à un moyen coercitif, de documents issus d'un système informatique ou d'un traitement de données nominatives, tels ceux détenus par un opérateur de téléphonie et qu'une telle mesure n'entre pas dans le champ d'application de l'article 5 § 3 de la Convention européenne des droits de l'homme relatif au contrôle de la privation de liberté ». Par cette argumentation, la Cour de cassation vient préciser le sens précis de l'article 77-1-1 du Code de procédure pénale.

Il est certes apparent que c'est le moment qui détermine la compétence du juge d'instruction, ou du Juge des Libertés et de la Détention (JLD) mais ce partage de compétence a conduit Madame LEMONNIER à s'interroger sur l'éventuelle mise en place d'un régime unique de ces autorisations de réquisitions informatiques. En effet, compte tenu de ce partage de la même compétence, Madame LEMONNIER propose[392] un régime unique à savoir confier au juge des libertés et de la détention, l'autorisation des réquisitions informatiques quel que soit le stade de la procédure et quelle qu'en soit la nature.

Les réquisitions informatiques ont fait l'objet de questionnement quant à leur conventionalité notamment à la lumière d'une décision de la chambre criminelle de la

[391] Cf. Cass. Crim. 22 novembre 2011, n° de pourvoir 11-84308, publié au Bull. Crim., n° 234.

Cour de cassation du 6 novembre 2013[393]. Dans cette décision, les faits à l'origine de l'intervention des enquêteurs de police judiciaire sont des faits de trafic de produits dopants exercés par Monsieur X. lors des perquisitions réalisées au domicile de Monsieur X, des adresses électroniques sont retrouvées inscrites sur un sac de sport. Monsieur X refuse de donner son consentement, mais les Officiers de police judiciaire ayant reçu l'autorisation de faire toutes les réquisitions utiles notamment informatiques en vue de la manifestation de la vérité, les sociétés Google et d'autres entités de communications ont été sollicitées pour déterminer les identités des titulaires des adresses inscrites. Monsieur X a formé un pourvoi contre la décision de la Cour d'appel de Grenoble en estimant que la Chambre de l'instruction de la Cour d'appel n'avait pas justifié sa décision sur le fondement de l'article 32 précité. Selon le pourvoi, « e*n retenant, sur ce fondement, que la localisation du site internet hors du territoire national ne faisait pas obstacle à la pénétration et la recherche de données sur ce site, par les enquêteurs, à l'aide d'un code d'accès qu'ils s'étaient légalement procuré, dans le cadre d'une perquisition, s'agissant pourtant de données qui n'étaient pas accessibles au public (source ouverte) puisque nécessitant un code d'accès, et en l'absence de tout constat que la personne légalement autorisée à divulguer ces données aurait donné un consentement volontaire, la chambre de l'instruction n'a pas légalement justifié sa décision*».

La Cour de cassation a statué sur le fondement de l'article 32 de la Convention de Budapest de 2001 sur la cybercriminalité. Selon cet article, « *une partie peut, sans l'autorisation d'une autre partie : a) accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou b) recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique* ». A la lecture de la décision de la chambre criminelle, les enquêteurs de la police judiciaire ont fait usage de leur propre matériel

---

[392] Cf. **LE MONNIER**, Le Juge des Libertés et de la Détention, p. 237

[393] Cf. Bulletin criminel 2013, n° 217.

d'une part et ont eu accès aux informations stockées grâce à un code d'accès trouvé dans les éléments couverts par l'autorisation du juge d'instruction. Le fondement de l'article 32 évoqué par le pourvoi n'étant en réalité pas utile.

Le régime de protection des données personnelles enregistrées via les nouvelles technologies de l'information est calqué sur le statut des écoutes téléphoniques en France.

Et cet alignement permet d'établir le lien entre le juge d'instruction et la répression des infractions commises via ces nouvelles technologies de l'information.

En effet, dans la loi du 11 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[394], les interceptions téléphoniques étaient ordonnées par le juge d'instruction, à l'exclusion du parquet, « lorsque les nécessités de l'information l'exigent. »

S'agissant du régime des écoutes téléphoniques et des interceptions, la législation française a réellement connu une évolution et un toilettage nécessaires seulement à la suite de la condamnation de la France par la Cour européenne des Droits de l'Homme dans ses célèbres arrêts HUVIG et KRUSLIN[395]du 24 avril 1990.

Dans les faits de l'arrêt HUVIG, il ressort que Monsieur HUVIG et son épouse sont poursuivis par l'administration fiscale pour fraude fiscale et recel de biens au titre de la société qu'ils gèrent. Dans le cadre de cette procédure, les époux ont fait l'objet d'écoutes téléphoniques.

Les faits de l'arrêt KRUSLIN sont également relatifs à une procédure d'écoutes téléphoniques mais dans un contexte pénal de complicité d'homicide. Des faits de cette seconde espèce, il apparaît que Monsieur KRUSLIN, sans domicile fixe et sans profession est mis aux arrêts à la suite des faits de vols de bijoux et de numéraires. Au cours de la période des faits, Monsieur KRUSLIN était hébergé par Monsieur T. Par

---

[394] Loi du 11 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications cf. JORF n°162 du 13 juillet 1991 page 9177.

[395] Cf. CEDH 24 Avril 1990, affaire HUVIG c. FRANCE (Requête n°11105/84), et CEDH 24 avril 1990, affaire KRUSLIN c. France (Requête n° 11801/85). Pour un commentaire des décisions voir par exemple **CHARPENEL Y**., Cybercrime : Jurisprudence de la Cour de cassation, Cahier de la Sécurité n° 6, octobre 2008, INHES (Institut National des Hautes Etudes de Sécurité).

décision du juge d'instruction, une procédure parallèle est entamée contre monsieur T. Cette dernière implique le placement sur écoute des lignes téléphoniques de Monsieur T. ces écoutes téléphoniques révèlent au cours de la procédure des conversations de KRUSLIN et T faisant référence aux affaires en cours. Monsieur KRUSLIN estimant que les écoutes téléphoniques qui lui sont par la suite opposées, doivent être annulées parce que faisant partie d'une autre procédure, saisit le juge. Il n'obtient pas gain de cause et se pourvoit en cassation. La Cour de cassation refuse de prononcer la nullité des écoutes. Monsieur KRUSLIN estime qu'il y a violation de son droit à la vie privée sur le fondement de l'article 8 de la Convention Européenne de Sauvegarde et des Droits de l'Homme, et saisit la Cour Européenne des Droits de l'Homme. L'Etat français a été condamné pour une violation de l'article 8 de la Convention Européenne et de sauvegarde des Droits de l'homme.

C'est à la suite de cette condamnation que le législateur français a légiféré sur les écoutes téléphoniques avec la loi du 11 juillet 1991.

A l'instar de la France, la question des interceptions téléphoniques a fait l'objet d'une décision de justice opposant un fonctionnaire du Royaume Uni à son Etat. C'est surtout sur le fondement du respect de la vie privée que la Cour Européenne des droits de l'Homme s'est prononcée.

En effet, l'article 8 de la Convention précise que : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. ». Sur le fondement de cet article qui garantit au plan européen, le droit au respect de la vie privée et familiale, du domicile et surtout de la correspondance, la Cour européenne des

Droits de l'Homme a rendu l'arrêt HALFORD contre Royaume Uni[396] en date du 25 juin 1997 répondant à la question de la protection des transmissions non publiques informatiques contre les interceptions sans droit. Cette décision a été l'occasion d'appliquer l'article 3 de la convention de lutte contre la cybercriminalité. Il ressort de l'espèce qu'en sa qualité de contrôleur général dans la police de Merseyside, Madame Halford s'est vue attribuer deux postes téléphoniques dont un réservé à son usage personnel. Il s'est avéré par la suite que ses communications en provenance de son domicile, considérée par la requérante comme en dehors des préoccupations professionnelles, ont été interceptés par des agents dans le cadre des appels professionnels. Madame Halford a par la suite postulé à un grade d'inspecteur général et s'est vu refuser le poste plusieurs fois au motif de faute professionnelle liée ses communications. Estimant que ses appels interceptés relevaient de sa vie privée, Madame Halford s'est sentie victime d'une atteinte à sa vie privée et saisit la Cour Européenne des Droits de l'Homme, sa requête devant les juges nationaux compétents n'ayant eu aucun succès. La question à laquelle la cour européenne a dû réponde est la suivante : l'article 8 de la Convention européenne relatif au respect de la vie privée est-il violé lorsque les appels d'un contrôleur interne de la police effectués dans les locaux professionnels sont interceptés sans information préalable de la part de l'administration? En réponse à cette interrogation, la Cour européenne s'est fondée sur sa jurisprudence pour répondre par l'affirmative. Elle considère qu'il y a eu violation de l'article 8 de la Convention européenne des droits de l'homme dans la mesure où il ressort clairement de sa jurisprudence que les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de "vie privée" et de "correspondance" visées à l'article 8 par. 1 (art. 8-1)[397].

---

[396] Décision de la Cour Européenne des droits de l'Homme rendue à la suite de la Requête n° 20605/92, Halford contre Royaume Uni, 25 juin 1997. Cf. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-62600# pour une version en ligne de l'arrêt.

[397] La jurisprudence en la matière est constituée par les arrêts de la CEDH : CEDH, époux HUVIG du 24 avril 1990, l'arrêt NIEMIETZ contre Allemagne, Requête n°13710/88 ; CEDH, du 24 avril 1990, arrêt KLASS et autres contre Allemagne et arrêt MALONE c. Royaume-Uni du 2 août 1984 publié à la série A n°82, p.30

D'ailleurs, avec la loi du 14 mars 2011[398], une perquisition électronique est instaurée et le juge d'instruction voit ses pouvoirs étendus en la matière. Cette perquisition s'aligne-t-elle sur celui de la perquisition traditionnelle de droit pénal ? Quels sont les pouvoirs du juge d'instruction sur la question ?

L'usurpation d'identité numérique permet de mieux analyser le rôle du juge d'instruction spécifiquement ses pouvoirs de coercition et de recherche d'informations en vue de la manifestation de la vérité.

Concrètement, le juge d'instruction pourra, du fait de ses pouvoirs, interroger les ordinateurs qui auraient selon les faits, servis à commettre l'infraction. Il pourra ainsi grâce à une veille remonter le chemin d'accès notamment pour se procurer des données usurpées encore stockées dans le disque dur de l'ordinateur ayant servi à la connexion. La veille est une manipulation technique et vise spécifiquement à installer un logiciel qui opère des recherches dirigées de l'ordinateur. Elle consiste à mettre des critères précis pour retracer l'historique d'utilisation ou de consultation sur l'ordinateur. De la sorte les techniques de stockage, d'analyse et de conservation des données transitant sur l'ordinateur et le réseau afférent sont répertoriées.

Il existe des cas dans lesquels, le juge d'instruction est remplacé par le ministère public.

2- Les procédures menées par le ministère public

Dans ces procédures, l'instruction est confiée au ministère public. C'est le cas en Allemagne, aux Etats-Unis et en Italie.

En Allemagne, depuis 1975, le juge d'instruction a été supprimé dans les procédures en général. Le ministère public (*Staatssanwaltschaft*) a donc pour rôle d'enregistrer les plaintes, de déclencher les poursuites dont il a le monopole et dirige l'enquête de police[399]. La police joue un rôle secondaire puisqu'elle est chargée d'assister le ministère public.

Le juge de l'enquête préliminaire n'intervient que lorsque le ministère public ne peut

---

[398] Loi n° 2011-267, du 14 mars 2011, JORF n°0062 du 15 mars 2011 page 4582.

[399] Cf. **WITZ C**., Le droit allemand, p 84 et s.

prescrire certains actes relevant de la liberté individuelle à savoir ordonner la détention provisoire ou le placement provisoire dans un établissement psychiatrique[400]. Le ministère public a donc un rôle important et plus large que le juge de l'enquête préliminaire.

De plus, la criminalité internationale relève de la compétence de l'office fédéral criminel.

Dans le cas de l'Italie également, le ministère public est chargé de l'enquête préliminaire. Il engage les poursuites. C'est la police qui enregistre les plaintes et elle doit informer et assister le ministère public lors de l'enquête. Pendant l'instruction, le juge de l'enquête préliminaire est chargé du contrôle de la légalité des investigations et des décisions restreignant les droits fondamentaux.

Au pays de Galles et en Angleterre, c'est le Crown Prosecution Service qui est chargé de déclencher les poursuites. Seule la police est habilitée à mener l'enquête.
Le rôle du juge consiste uniquement à donner l'autorisation à la police pour effectuer des actes comme les mandats d'arrêt, les perquisitions et les saisies[401.]

En matière de perquisition ou de saisie, la vraie question qui se pose est celle de savoir comment appliquer les règles classiques de la perquisition à un espace virtuel comme le réseau internet et ses attenants ?

Cette interrogation se pose peu importe que la compétence soit celle attribuée au juge de l'instruction ou qu'elle soit plutôt reconnue au ministère public.

Il faut préciser à ce sujet que le critère de détermination du juge est le critère géographique. Or, ce critère n'est pas précis en matière virtuelle. Ce sont donc les droits d'accès qui définissent ce à quoi cet ordinateur concerné donne accès, qui seront les critères déterminant la compétence du juge qui va ordonner la perquisition[402.]

L'adaptation des parquets nationaux reste une question majeure dans la lutte contre la cybercriminalité

---

[400] Cf. les dispositions du §162, al. 2 StPO, du code de procédure pénale allemand.

[401] http://www.senat.fr/lc/lc195/lc195.pdf

En effet, la réforme des parquets notamment en France est importante par rapport à l'efficacité de l'action des juges qui interviennent sur les dossiers de cybercriminalité[403]. En France, l'année 2014 est marquée par la réorganisation du Parquet de Paris, principalement son pôle financier qui s'adapte à la cybercriminalité[404].

Le Parquet français se compose de plusieurs pôles dont le pôle financier, reformé pour être divisé en deux sections dont l'une a désormais exclusivement en charge la cybercriminalité. Cette nouvelle répartition est le gage de succès des opérations d'investigations dans le domaine de la cybercriminalité. Il apparaît plus simple pour les magistrats en charge des questions cybercriminelles notamment au niveau du pôle financier, de travailler exclusivement sur ces dossiers délicats. C'est à la lumière de la spécificité des dossiers que les magistrats en charge de la cybercriminalité ont essentiellement et exclusivement pour mission de traiter les affaires relatives aux faux virements et aux systèmes de traitement automatisés de données (STAD)[405]. La fonction secondaire de la section cybercriminalité est de venir en « *soutien technique des autres sections* » pour d'autres infractions cybercriminelles chaque fois que les besoins nécessiteront cette intervention.

Les dossiers de cybercriminalité comprennent des difficultés techniques en plus des aspects financiers.

A ce sujet, la loi n° 2013-1117 du 06 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière[406] modifie les articles du

---

[402]Cf. **AUROUX J-B**., NTIC et droit pénal, Revue Lamy Droit de l'immatériel 2006

[403] Cf. Journal Libération du 1er septembre 2014, le parquet national financier a pris ses dossiers au Parquet de Paris.

[404] Cf. E. FANSTEN et S. FAURE, « *le parquet doit s'adapter à la cybercriminalité* » in Journal Libération du 1er septembre 2014, p. 12. Compléter avec M. QUEMENER, Le Procureur financier, architecte de la lutte contre la corruption et la délinquance économique et financière, in *Revue internationale d'intelligence économique*, 2014/1 (Vol. 6), p.27-35.

[405] Cf. Interview du procureur de Paris François MOLINS par Dalloz Actualité, édition du 17 septembre 2014.

[406] Cf. Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière publiée au JORF n°0284 du 7 décembre 2013 page 19941 texte n° 4.

code pénal notamment les articles 706-148 et suivants dont les dispositions sont relatives aux pouvoirs du juge de la détention et des libertés quant aux avoirs saisis ou confisqués. L'article 24 de la loi précise les modalités et les conditions de saisie, de confiscation de ces avoirs.

L'un des apports les plus importants de cette loi est de conférer une compétence concurrente au Procureur de la République, au juge d'instruction et au tribunal correctionnel de Paris pour certaines infractions précises. L'article 705 du code de procédure pénale dispose en effet depuis cette réforme que : « *Le procureur de la République financier, le juge d'instruction et le tribunal correctionnel de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles 43, 52, 704 et 706-42 pour la poursuite, l'instruction et le jugement des infractions* (…).

Elle organise ainsi la gestion des avoirs criminels saisis ou confisqués.

Les réformes concernent le Parquet essentiellement. D'autres juges comme celui du civil ou des mineurs interviennent dans les affaires de cybercriminalité. Qu'en est-il s'agissant de leur rôle ?

3- Les juges des mineurs et du civil

Sous un autre angle et pour les mêmes raisons de composition judiciaire, le juge des mineurs et le juge civil interviennent sur des affaires de cybercriminalité, notamment de cyber-pédopornographie.

- L'intervention du juge des mineurs

Le juge des mineurs pourra connaître des affaires de cyber pédopornographie notamment. En quoi consisterait son intervention ? Uniquement qualifier les infractions et déterminer les peines applicables ou le juge exerce-t-il au-delà de ses fonctions traditionnelles, des missions spécifiques en matière de cybercriminalité ?

- L'intervention du juge civil dans la répression de la cybercriminalité

S'agissant du juge civil, selon le CLUSIF, le juge civil a à connaître du volet civil des infractions cybercriminelles. En effet, deux volets sont à distinguer s'agissant d'une infraction cybercriminelle : d'une part un délit civil et d'autre part le volet pénal de l'acte

posé. Il arrive que le juge civil intervienne dans les affaires de lutte contre la cybercriminalité en matière de jeux en ligne.

C'est ainsi que le Tribunal de Grande Instance de Paris a rendu une ordonnance de référé en date du 08 juillet 2005, obligeant la société Ze Turf à cesser de proposer ses jeux en ligne aux clients français. Cette ordonnance a été confirmée par la Cour d'appel de Paris en 2006[407].

A ce sujet, il faut préciser que le fait pour les sites de jeux en ligne de proposer leurs jeux aux clients français constituent une infraction, précisément un délit dans la mesure où seuls la Française des Jeux et la Société française de paris de jeux en ligne sont les seuls organismes habilités par l'Etat français à proposer ces prestations.

D'ailleurs, il arrive que le juge prononce des sanctions comme la cessation des jeux en ligne concernés comme c'est le cas dans la décision de la Chambre commerciale de la Cour de cassation du 21 janvier 2014[408]. Dans les faits à l'origine de la décision de la Cour de cassation, la société Darty Telecom s'est déclarée auprès de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) comme fournisseur d'accès internet pour la société 5dimes installée en Costa Rica. Cette dernière propose des jeux en ligne, sans avoir d'agrément de l'Autorité de Régulation des Jeux en ligne (ARJEL). Elle a de ce fait été sommée de cesser son activité d'offre des jeux en ligne et de jeux d'argent et de hasard en direction de la France. La société 5dimes a tout de même poursuivi son activité. L'ARJEL a dès lors saisi le Tribunal de Grande Instance pour faire injonction à Darty Télécom de procéder à la mise en œuvre du blocage des sites de 5dimes.

Darty Telecom saisit le juge pour voir la décision du juge de première instance infirmée compte tenu de sa qualité de fournisseur d'accès et non d'opérateur de service. N'ayant pas obtenu gain de cause devant le juge d'appel, la société se pourvoit en cassation.

---

[407] Cour d'appel de Paris, 14ème Chambre, section A Arrêt du 4 janvier 2006.

[408] Cf. Cass. Com. 21 janvier 2014, n° de pourvoi 13-11704 13-15548, publié au bulletin n° Bulletin 2014, IV, n° 14.

La Cour de cassation répond à Darty Télécom sur le fondement des articles 61 de la loi n° 2010-476 du 12 mai 2010 et 6,1,1 de la loi n° 2004-575 du 21 juin 2004 « *qu'en cas d'inexécution par un opérateur non autorisé de l'injonction de cesser son activité d'offre de paris ou de jeux d'argent ou de hasard, l'arrêt de l'accès à ce service peut être ordonné aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne. que ces personnes sont ainsi qualifiées par la loi pour défendre à l'action tendant au prononcé d'une telle mesure, sans qu'il y ait lieu de distinguer entre opérateurs de services ou de réseaux et peu important que l'opérateur considéré ait ou non la possibilité de procéder lui-même au blocage de l'accès au site litigieux ; qu'ayant constaté que la société Darty télécom s'était déclarée en qualité de fournisseur d'accès à internet auprès de l'Autorité de régulation des communications électroniques et des postes, la cour d'appel en a exactement déduit que cette société avait qualité pour défendre à la demande d'injonction formée à son encontre* ». Il faut comprendre par cette décision que le juge entend expliquer au Fournisseur d'accès son niveau de responsabilité en termes de respect des dispositions légales liées à son statut.

D'autres magistrats plus spécialisés interviennent dans les affaires de cybercriminalité. Il s'agit des juges interrégionaux spécialisées ou juridictions interrégionales spécialisées.

4- Les juridictions Interrégionales spécialisées (JIRS)

Ces juridictions ont été instituées par la loi Perben II du 9 mars 2004[409]. Elles sont au nombre de huit en France: elles sont présentes à Paris, Lille, Nancy, Lyon, Marseille, Bordeaux, Rennes et Fort-de-France.

Comme l'indique leur appellation, ce sont des juridictions spécialisées aux termes de l'article 704 du code de procédure pénale pour traiter des infractions économiques et financières tout d'abord.

Elles sont ensuite compétentes pour connaître des atteintes aux systèmes de traitement automatisés de données selon les dispositions des articles 323-1 à 323-4 du code de procédure pénale. Ces derniers chefs de compétence sont directement liés à la cybercriminalité puisqu'il s'agit des infractions informatiques.

La désignation des magistrats qui les compose ne figure pas expressément dans les textes de loi et certains auteurs ont pu en déduire que cette désignation est le fait de la compétence et de la formation professionnelle des magistrats du siège ou des juges d'instruction qui la composent. Il n'existe cependant pas à ce jour de jurisprudence foisonnante en la matière et pourtant les cas de cybercriminalité et notamment d'atteinte aux systèmes de traitement automatisé de données se multiplient chaque jour.

Les compétences attribuées à ces juridictions tiennent compte de la commission en bande organisée des infractions relevant de la cybercriminalité. Partant, les moyens mis à la disposition de ces juges sont conséquents.

Le rôle des juges se mesure aussi bien au plan national qu'au plan européen. C'est pourquoi, il nous faut examiner le juge européen face à la cybercriminalité.

B- Le juge européen face à la cybercriminalité

D'une manière globale, la compétence pénale de l'Union européenne a traversé plusieurs étapes pour en arriver à sa conception actuelle**[410]**.

---

[409] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité publiée au JORF du 10 mars 2004, p. 4567.

En 1981, avec l'arrêt de la CJCE du 11 novembre 1981, procédure pénale contre Guerrino Casati[411], la Cour de Justice estime que si une législation pénale nationale est en contradiction avec le droit communautaire, elle doit être écartée. A ce sujet, il faut souligner que le Traité de Maastricht créant le troisième pilier du droit de l'Union, lui conférait dans le champ pénal un cadre de coopération entre les Etats membres. Ce cadre était flou. C'est avec le Traité d'Amsterdam qu'est affirmée la compétence pénale directe de l'Union grâce à l'article 31§1 TUE qui dispose que « *l'action en commun dans le domaine de la coopération judiciaire en matière pénale vise, entre autres à : a) faciliter et accélérer la coopération entre les ministères et les autorités judiciaires ou équivalentes compétents des Etats membres, y compris, lorsque cela s'avère approprié, par l'intermédiaire d'Eurojust, pour ce qui est de la procédure d'exécution des décisions ; b) faciliter l'extradition entre Etats membres ; c) assurer, dans la mesure nécessaire à l'amélioration de cette coopération, la compatibilité des règles applicables dans les Etats membres ; d) de prévenir les conflits de compétences entre Etats membres ; e)adopter progressivement des mesures instaurant des règles minimales relatives aux éléments constitutifs des infractions pénales et aux sanctions applicables dans le domaine de la criminalité organisée, du terrorisme et du trafic de drogue* ».

D'un point de vue procédural, la Communauté n'a aucune compétence attribuée par le Traité dans le secteur pénal. Ses compétences sont donc en principe d'attribution. Il apparaît dès lors délicat de parler de la compétence du juge européen en matière de cybercriminalité. Il existe une parade pour favoriser de manière indirecte l'action du juge européen quant à la cybercriminalité : les questions préjudicielles (a).

D'un autre point de vue, le recours au juge européen est nécessaire pour trancher des questions relatives à la coopération judiciaire. C'est le cadre de l'Espace de sécurité, de justice et de Libertés (b).

---

[410] Cf. **BEAUVAIS P.**, *Droit pénal et droit de l'Union Européenne : vers un droit pénal fédéral*, in Droit pénal et autres branches du droit, Actes du colloque de l'AFDI sous la direction de Jean –Christophe Saint-Pau, éditions Cujas.

[411] Cf. CJUE, Procédure pénale c. Guerrino Casati, 11 novembre 1981, aff. 203/80.

a- La part contributive des questions préjudicielles

En matière de compétence, la Cour de justice de l'Union Européenne est surtout sollicitée pour des questions préjudicielles par des juges nationaux. Sous le couvert de ces questions préjudicielles, il ressort de ses décisions qu'elle clarifie certes de questions relatives à la compétence, mais ses interventions sont une manière de légiférer puisqu'elle opère des précisions de qualifications juridiques et souvent des éclaircissements sur les interprétations des directives européennes. C'est dans ce contexte que, dès 2000, les juridictions françaises saisissent la Cour de Justice, par un jugement du 20 novembre 2000, pour trancher sur le problème de leur compétence dans l'affaire opposant l'association Union Internationale des Juifs de France (UIJF) et Yahoo Inc., une société américaine. Il est question du critère de l'accessibilité des contenus publics. A cette occasion, la Cour de Justice est questionnée sur la directive de l'Union Européenne sur le commerce électronique.

Dans la dynamique de la recherche de compétence du juge dans les affaires relatives aux cyberdélits, la Cour de Justice est saisie. C'est dans ce cadre qu'elle a eu à se prononcer dans un arrêt Fiona Shevill contre Press Alliance[412], du 07 mars 1995 en matière de diffamation de presse. Dans cet arrêt, c'est la détermination du lieu où le fait dommageable s'est produit qui a été appliquée au délit de presse, comme critère de compétence. Une option de compétence est laissée à la victime de la diffusion diffamatoire par voie de presse. La Cour de Justice a dans sa décision précisé que *ce lieu devait être interprété au sens que la victime peut intenter contre l'éditeur une action en réparation soit devant les juridictions de l'Etat contractant du lieu d'établissement de l'éditeur, compétentes pour réparer l'intégralité du dommage, soit devant les juridictions de chaque Etat contractant dans lequel de la publication diffamatoire a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation, compétente pour connaître des seuls dommages causés dans l'Etat de la* juridiction saisie.

[412] CJUE, Fiona Shevill c. Press Alliance, 7 mars 1995, aff. C-68/93

La Cour de Justice de l'Union Européenne a également statué sur la compétence du juge en matière d'atteinte alléguée aux droits de la personnalité au moyen de contenus mis en ligne sur un site internet. Elle a ajouté une option de compétence en donnant « *la possibilité à la victime de saisir la juridiction de l'Etat membre dans lequel se trouve ses intérêts* », et ce dans l'arrêt eDate Advertising contre Martinez[413] du 25 octobre 2011.

Sous le couvert d'une question de compétence, la Cour de Justice procède à une qualification. Elle précise l'interprétation et définit par conséquent un terme ambigu et peu clair « la réutilisation » de la directive du 11 mars 1996, directive 96/9/CE[414]dans l'arrêt Dataco Ltd[415] du 18 octobre 2012. Dans un litige opposant Football Dataco, société détentrice de droits sui generis sur une base de données selon le droit du Royaume Uni et Sportradar GmbH, une compagnie de diffusion, qui aurait violé ce droit par des actes d'extraction interdits sur le fondement de la directive du 11 mars 1996, la Cour d'appel d'Angleterre (High Court of Appeal) introduit une question préjudicielle. La Cour de justice est saisie pour l'interprétation de l'article 7 de la directive précité. La société Sportradar conteste la compétence de la Cour d'appel qui s'est déclarée compétente mais seulement sur la responsabilité conjointe de Sportradar et de ses clients utilisant son site web au Royaume Uni. Elle s'est donc déclarée partiellement incompétente pour statuer sur la responsabilité principale de l'assigné Sportradar du fait de la violation. Football Dataco a alors interjetté appel.

La Court of Appel a sursis à statuer et a saisi la Cour de Justice de l'Union sur d'une part la qualification des faits à la lumière de la directive 96/9/CE et d'autre part sur le lieu de leur commission. Il faut souligner que le terme réutilisation posait problème quant à sa définition selon la directive. La Cour de Justice de l'Union a répondu en précisant qu'il

---

[413] CJUE, eDate Advertising c. Martinez, 25 octobre 2011, aff. C-509/09 et C- 161/10

[414] Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique

des bases de données, JO L77, p. 20.

[415] Cf. Football Dataco Ltd c. Sportradar GmbH, aff. C-173/11

« faut définir la réutilisation largement ». La Cour de Justice se fonde sur un précédent arrêt du 9 novembre 2004, The British Horseracing Board et autres[416].

Sur la seconde branche de la question préjudicielle, la Cour de Justice précise que l'objectif de la directive est de supprimer les barrières quant à la circulation dans le marché intérieur, les spécificités d'un droit dans un Etat qui confère des privilèges restent applicables seulement au niveau local et n'ont pas vocation à être étendues à l'échelle de l'Union. Par cette précision, la Cour de Justice détermine l'étendue de la compétence locale. Elle renvoie à deux autres arrêts : un premier arrêt Football Dataco et autres[417] du 1er mars 2012 et un second arrêt, l'arrêt Wintersteiger[418] du 19 avril 2012. Les faits de ce dernier arrêt sont les suivants : la société WINTERSTEIGER, basée en Autriche, produit et vend à l'international des machines d'entretien de ski. Elle commercialise par ailleurs des accessoires ainsi que les pièces de change afférentes à ses équipements. Elle est propriétaire de la marque WINTERSTEIGER. Parallèlement, la société allemande Product 4U, basée en Allemagne propose les produits de la même catégorie et aussi pour le compte de la société Wintersteiger. Depuis 2008, Products 4U a réservé le mot clé « l'Adword » Wintersteiger dans le cadre de son système publicitaire.

A la suite de ces arrêts posant directement des questions préjudicielles à la CJUE, il se dégage un droit qui finalement prend racine pour former la jurisprudence de la Cour. Elle semble certes en construction mais dans une certaine mesure elle est la trame légale des problèmes traités. Le droit lié aux activités numériques est un droit jeune, et par conséquent en élaboration. Il n'est pas encore parfait mais sa construction par la jurisprudence le rendra complet et suffisamment élaboré au fur et à mesure des décisions rendues.

En dehors des questions préjudicielles, l'espace de coopération, de justice et de liberté constitué par l'Union européenne connaît d'autres problématiques liées à la répression de la cybercriminalité et ces problématiques sont importantes puisqu'elles

---

[416] cf. The British Horseracing Board et autres, aff. C-203/02, Rec. p I-10415, points 45 46 51 et 67.

[417] Cf. Football Dataco e. a., 1er mars 2012, aff. C-604/10 non encore publié au recueil en ses points 148

[418] Cf. Wintersteiger, 19 avril 2012, aff. C-523/10, non encore publié au Recueil, point 25.

concernent essentiellement le cadre de la coopération dans l'espace de justice et de liberté entre les Etats membres de l'Union européenne.

b- La coopération judiciaire dans l'espace de sécurité de justice et de liberté

La cybercriminalité est une forme de criminalité qui transcende les frontières. Par conséquent, il est fondamental qu'en cas d'actes cybercriminels commis par exemple dans un Etat donné, le cybercriminel puisse être appréhendé grâce aux procédures de coopération et d'entraide judiciaire qui lient les Etats membres de l'Union Européenne. C'est dans ce cadre que s'inscrit la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959[419].

Si la convention d'entraide est vieille de par sa date, force est de constater qu'elle a été renforcée par le règlement (CE) N° 1882/2003 du Parlement Européen et du Conseil du 29 septembre 2003 portant adaptation à la décision 1999/468/CE du Conseil des dispositions relatives aux comités assistant la Commission dans l'exercice de ses compétences d'exécution prévues dans des actes soumis à la procédure visée à l'article 251 du Traité CE.

Selon cette disposition communautaire, *« la Commission présente une proposition au Parlement européen et au Conseil. Le Conseil, statuant à la majorité qualifiée, après avis du Parlement européen:*

- s'il approuve tous les amendements figurant dans l'avis du Parlement européen, peut arrêter l'acte proposé ainsi amendé,

- si le Parlement européen ne propose aucun amendement, peut arrêter l'acte proposé,

- dans les autres cas, arrête une position commune et la transmet au Parlement européen. Le Conseil informe pleinement le Parlement européen des raisons qui l'ont conduit à arrêter sa position commune. La Commission informe pleinement le Parlement européen de sa position.

---

[419] Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 publiée à la Série des Traités n° 030.

Si, dans un délai de trois mois après cette transmission, le Parlement européen:

a) approuve la position commune ou ne s'est pas prononcé, l'acte concerné est réputé arrêté conformément à cette position commune;

b) rejette, à la majorité absolue des membres qui le composent, la position commune, l'acte proposé est réputé non adopté;

c) propose, à la majorité absolue des membres qui le composent, des amendements à la position commune, le texte ainsi amendé est transmis au Conseil et à la Commission, qui émet un avis sur ces amendements.

La Convention d'entraide a surtout été renforcée par un premier protocole additionnel du 17 mars 1978[420] qui écarte certaines dispositions comme le refus d'accorder l'entraide pour des infractions fiscales[421]. Un second protocole additionnel signé à Strasbourg le 8 novembre 2001 s'ajoute à la Convention pour en retirer les difficultés d'application. Ce protocole est publié par le décret n° 2012-813 du 16 juin 2012 portant publication du deuxième protocole additionnel à la Convention d'entraide[422].

Cette Convention d'entraide a un caractère spécifique. C'est ce qui explique qu'elle ait été plusieurs fois améliorée par d'autres textes comme les protocoles additionnels et que le règlement 2003 vienne encadrer les compétences d'exécution des organes institutionnels (la Commission et le Parlement) qui l'utilisent.

---

[420] Cf. décret n°91-386 du 17 avril 1991 portant publication du protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959, fait à Strasbourg, le 17 mars 1978 et signé par la France le 28 mars 1990, publié au JORF n°98 du 25 avril 1991 page 5476.

[421] C'est l'article 2 a) qui précise que : « *L'entraide judiciaire pourra être refusée :si la demande se rapporte à des infractions considérées par la partie requise soit comme des infractions politiques, soit comme des infractions connexes à des infractions politiques, soit comme des infractions fiscales* ».

[422] Cf. décret n° 2012-813 du 16 juin 2012 portant publication du deuxième protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale (ensemble une réserve et des déclarations françaises), signé à Strasbourg le 8 novembre 2001 publié au JORF n°0142 du 20 juin 2012 page 10201 texte n° 1.

La spécificité de la Convention d'entraide s'accentue avec le mandat européen qui en fait partie. Il représente en effet, un maillon important dans la répression de la cybercriminalité.

1- L'importance du mandat européen dans la répression de la cybercriminalité

La décision de créer un mandat européen est née du constat des limites territoriales à l'exécution des décisions de justice[423]. Le mandat européen est en réalité un concept qui remplace celui de l'entraide judiciaire contenue dans la Convention européenne d'entraide judiciaire en matière pénale[424]. C'est pourquoi lors de l'Assemblée des 14 et 15 décembre 2001 à Laeken, les membres du Conseil ont signé un accord relatif à un mandat européen.[425] La décision-cadre 2002/584 du Conseil relative au Mandat d'arrêt européen et aux procédures de remise entre Etats membres du 13 juin 2002[426] définit en son article 1er, le mandat européen comme « *une décision judiciaire émise par l'autorité judiciaire compétente d'un Etat membre de l'Union européenne appelée autorité judiciaire d'émission, en vue de l'arrestation et de la remise par l'autorité judiciaire compétente d'un autre Etat membre, appelée autorité d'exécution, d'une personne recherchée pour l'exercice de poursuites pénales ou pour l'exécution d'une peine ou d'une mesure de sûreté privative de liberté.* »

L'absence de liberté de circulation des décisions de justice au sein de l'Union Européenne est à l'origine de la mise en place d'un mandat européen. Ce dernier est également établi en vue de l'obtention des preuves nécessaires à toute procédure pénale. Il faut à cet effet souligner l'alourdissement des procédures judiciaires et des investigations policières lié au principe de souveraineté des Etats.

---

[423] http://www.robert-schuman.eu/question_europe.php?num=sy-84

[424] La Convention est publiée à la Série des Traités de la Communauté Européenne sous le numéro 030 et est entrée en vigueur le 12 juin 1962. Elle est complétée avec « Le mandat européen »et la constitution française sur http://www.robertschuman.eu/question_europe.php?num=sy-84.

[425] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/fr/ec/68779.pdf, pour d'autres références voir également http://www.monde-diplomatique.fr/cahier/europe/a12143

[426] Décision-cadre 2002/584 du Conseil relative au Mandat d'arrêt européen et aux procédures de remise entre Etats membres du 13 juin 2002 publié au JO L 190, 18 juillet 2002. La décision-cadre a été modifiée

En droit français, c'est par la loi constitutionnelle du 25 mars 2003[427] que le mandat européen a été intégré au corpus législatif. Grâce à cette révision de la Constitution, la France met en application la décision-cadre du 13 juin 2002. Il faut à ce propos, préciser les différences entre les décisions-cadre et les directives et les règlements de l'Union Européenne. Une fois qu'elles sont adoptées par un organe de l'Union, les décisions cadre constituent de véritables actes de droit dérivé du Traité sur l'Union européenne (et non du Traité de Rome comme c'est le cas pour les directives et règlements) à la différence des deux précédentes sources du droit communautaire.

Quant aux belges, c'est en 2004 que le mandat européen a été introduit aux normes législatives.

Si l'article 1 de la décision cadre précise les conditions propres aux textes du mandat européen, l'article 2 du même texte traite de la nature des infractions concernées. Il apparaît dans cet article que la cybercriminalité fait partie des infractions il est possible d'utiliser le mandat européen.

Outre le mandat européen, créé pour garantir la coopération judiciaire en matière de cybercriminalité, l'Union européenne s'est dotée de magistrats de liaison qui travaillent dans le cadre d'EUROJUST, le réseau mis en place pour assurer la coopération judiciaire notamment au plan des enquêtes et des arrestations.

2- Les magistrats de liaison

Les magistrats de liaison constituent une institution créée pour améliorer davantage la coopération judiciaire entre les Etats membres de l'Union européenne.

---

par la décision-cadre du Conseil 2009/299/JAI. Elle est contenue dans le Code pénal de l'Union Européenne, 2è édition, BRUYLANT, Bruxelles, 2013.

[427] Loi constitutionnelle n° 2003-267 du 25 mars 2003 parue au JORF n°72 du 26 mars 2003 relative au mandat européen. Il s'agit de l'article 88-2 de la constitution complété par un alinéa ainsi rédigé : *« la loi fixe les règles relatives au mandat européen en applications des actes pris sur le fondement du Traité sur l'Union européenne »*. Pour une version en ligne de la convention européenne d'entraide judiciaire en matière pénale, cf. : http://www.conventions.coe.int/Treaty/fr/Treaties/Html/030.htm. En France, cette convention a été ratifiée par une loi parue au Journal Officiel de la République Française n°0168 du 22 juillet 2011 page 12530 (texte n° 2 et c'est la loi n° 2011-855 du 20 juillet 2011 autorisant la ratification du deuxième protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale

L'institution existe grâce à des accords bilatéraux entre la France et trois pays : l'Italie, les Pays-Bas et les Etats-Unis en 1993. Ce sont des magistrats mis à disposition par le ministère de la justice auprès des ministères des affaires étrangères.

Dès 1996, le Conseil à l'Union européenne a adopté deux actions communes : l'action commune 96/277/JAI du 22 avril 1996 relative au cadre d'échange de magistrats de liaison[428] et l'action commune 96/602/JAI du 14 octobre 1996 concernant le cadre d'orientation de commun pour les initiatives des Etats membres en matière d'officiers de liaison[429].

La première action commune est entrée en vigueur depuis le 27 avril 1996 et la seconde a été abrogée avec l'entrée en vigueur de la décision 2003/170/JAI du 27 février 2003 relative à l'utilisation commune des officiers de liaison détachés par les autorités répressives des Etats membres[430].

En appui de cette institution de magistrat de liaison, il faut mentionner le réseau judiciaire européen qui est devenu aujourd'hui le réseau EUROJUST grâce auquel plusieurs infractions en matière de cybercriminalité sont instruites et des réseaux de criminels démantelés.

En effet, pour lutter efficacement contre le fléau des attaques numériques, l'Union européenne via la Commission et le Conseil de l'Union ont réfléchi à la mise en place de systèmes harmonisés des droits nationaux et particulièrement des procédures pénales. C'est dans cette optique qu'ont été créés des points de contact pour centraliser les plaintes contre les attaques dont seraient victimes les Etats. Pour une suite à l'activité de ces points de contact, des magistrats de liaison sont institués. En réalité, ils sont placés à des lieux stratégiques dans la mesure où ils ne sont pas vraiment représentés dans tous les Etats[431]. On les retrouve auprès des autorités judiciaires des États-Unis, de l'Espagne, du Canada, du Royaume du Maroc, de l'Allemagne, du Royaume Uni et de la République

---

[428]Cf. JO L 105 du 27 avril 1996, p1-2.

[429] Cf. JO L 268 du 19 octobre 1996, p 2-4.

[430] Cf. J.O. L 67 du 12 mars 2003, pp. 27-30.

[431]Cf. **QUEMENER M.,** Cybercriminalité, droit pénal appliqué, p 211-212.

Tchèque.

Il convient de s'interroger sur les raisons d'un nombre aussi infirme comparé à l'ensemble du réseau numérique, qui est quotidiennement, objet, outil ou lien de commission d'actes cybercriminels ?

En matière pénale, le Traité d'Amsterdam[432] permet en 1997, d'intégrer les accords Schengen[433] dans le cadre juridique de l'Union européenne. Cet accord prévoit le renforcement de la coopération et de la collaboration entre les services de police et les autorités judiciaires. C'est dans ce cadre qu'il prône l'unification des forces de police dans l'espace Schengen pour éviter des délits comme la criminalité organisée, la fraude ou les crimes contre les enfants.

Le Traité Schengen prévoit des dispositions relatives aux systèmes d'informations mais il n'élabore pas encore le cadre juridique des envois indésirables ou spams par exemple. Il traite des questions de visas, de contrôles d'accès aux frontières. Seules les frontières géographiques sont prévues et encadrées dans ce traité.

3- L'espace Schengen et les données à caractère personnel

L'espace Schengen a été créé dans l'optique de faciliter une libre circulation des personnes et des marchandises dans cette zone géographique composée par les 22 Etats signataires.

S'agissant d'un espace garantissant la liberté de circulation des personnes et des marchandises, des échanges de données vont s'y développer. De même les services et les prestations vont générer des flux de données. C'est dire que les personnes concernées seront amenées par ces échanges à communiquer des données à caractère personnel.

---

[432] Le Traité d'Amsterdam a été signé le 2 octobre 1997, cf. Traité d'Amsterdam modifiant le Traité de l'Union Européenne, les Traités instituant les Communautés européennes et certains actes connexes, Journal officiel de l'Union Européenne n° C 340 du 10 novembre 1997.

[433] L'accord Schengen date du 14 juin 1985 et est entré en vigueur en 1995. Il permet aux Etats signataires d'abandonner leurs frontières internes pour une frontière extérieure unique.cf. Protocole intégrant l'acquis de Schengen dans le cadre de l'Union Européenne, Journal officiel de l'Union Européenne n° C 340 du 10 novembre 1997.

Par exemple, si deux personnes dont l'une vit au Luxembourg et l'autre en France souhaitent passer un contrat de fourniture de service ou de quelque prestation que ce soit, elles devront se communiquer les différents éléments permettant de s'identifier à savoir la raison sociale ou le nom, le prénom, l'adresse postale, les courriels et toutes informations utiles à la conclusion du contrat.

Le Traité Schengen a en son dispositif une partie propre à ces systèmes d'information des données appelées Système d'Informations Schengen IIe génération. Que comporte ce système ?

Le texte fondamental sur lequel se fonde le système Schengen SIS II est le Règlement (CE) n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)[434].

Le système SCHENGEN a en son sein deux branches : d'une part les autorités de contrôle aux frontières et de contrôles juridictionnels peuvent via ce système obtenir des informations sur les personnes et les objets dans l'espace Schengen et on note qu' il existe une interconnexion entre le système central de chaque Etat membre encore appelé système informatique national du système d'information Schengen[435](N-SIS) à un système central (C-SIS) ; d'autre part le réseau est complété par un autre système appelé SIRENE c'est-à-dire *Supplementary Information Request at the National Entry,* qui est l'interface humaine du système SIS.

En France, le contenu des systèmes d'information figure depuis le 1er janvier 2014 au Code de la sécurité intérieure aux articles R 231-9 et suivants.

La nomenclature de l'espace Schengen en ce qui concerne la communication des données laisse apparaître la construction d'interconnexion mais surtout une autre forme de

---

[434] cf. Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, publié au JOUE L 381/4 du 28.12.2006, p. 4 - 23.

[435] Cf. Décret n°95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS publié au JORF n°108 du 7 mai 1995 page 7420 et désormais codifiée à l'article R 231-9 du Code de la sécurité intérieure.

contrôle sournoise de l'Union quant aux flux de données qui transitent dans cet espace. Il plane une forme de non contrôle des frontières mais en réalité toutes les données échangées sont enregistrées et stockées même si elles ne sont pas utilisées en temps réel. Il s'agit en fait d'une atteinte déguisée à l'intimité et à la vie privée de ces personnes dont les données sont stockées. La seule différence avec une violation injustifiée c'est qu'elle se fonde sur la raison d'Etat et la sécurité du plus grand nombre. Il sera en effet possible grâce à ces informations collectées à l'insu (et sans consentement exprès) des concernés d'assurer des contrôles en cas de fraude ou d'attaques par exemple.

4- La perspective de la proposition de règlement des données à caractère personnel

La cybercriminalité est un domaine transversal qui implique nécessairement le traitement de données à caractère personnel. En effet, par l'intermédiaire des systèmes informatiques et des nouvelles technologies, des échanges sont opérés et ces flux concernent des données publiques ou privées. Or, ces données se réfèrent en première ligne aux individus. Dans le cadre de la protection des données des individus, la loi française est à l'origine de la protection des données échangées et contient des dispositions sanctionnant des comportements jugés répréhensibles et qui pourraient tomber sous la qualification de comportements cybercriminels. La collecte des informations permet de rebondir sur la consistance des incriminations cybercriminelles liées au traitement des données dans des systèmes d'information. En effet, aux infractions traditionnellement réprimées par les codes pénaux européens s'ajoutent les infractions classiques qui sont commises via les technologies de l'information et de la communication. Ce qui amène à considérer l'ensemble des directives pour encadrer les données à caractère personnel en plus de la directive initiale de 95. Ainsi, la directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 relative à la protection des bases de données[436] a son importance dans le cadre de la répression de la cybercriminalité dans la mesure où les bases de données sont des supports de commission des infractions. Il est crucial de savoir comment ces supports sont protégés au plan européen pour définir la nature suffisante ou non des dispositions protectrices. Il est

[436] Directive publiée au J.O.C.E., n° L. 77 du 27 mars 1996, p. 20

permis de faire état du degré de protection puisque les bases de données sont l'une des cibles prisées par les cybercriminels.

Malgré cette protection de plus, la directive n'a pas suffisamment de force légale, ainsi que l'indiquent les retards observés dans sa transposition par les différents Etats membres de l'Union européenne. Ces retards traduisent le peu d'intérêt que suscite la protection des données à l'égard des Etats. C'est l'impression générale qui se dégage de la tardiveté de transposition de la directive dans les cadres législatifs des Etats membres de l'Union. C'est pourquoi, il est apparu utile de réfléchir à une source plus contraignante, de nature différente tel le règlement, pour réguler les données à caractère personnel au sein de l'Union.

Le 27 janvier 2012, par une communication, une proposition de règlement sur les données à caractère personnel a été soumise au Parlement européen. Cette proposition vise à changer la nature actuelle (de directive) du texte protégeant les données à caractère personnel au sein de l'Europe. L'objectif est clair de rendre plus contraignant ce texte fondamental et instaurer ainsi une sécurité juridique plus accrue. Cette proposition de règlement est selon la CNIL une action nécessaire et louable.

L'un des points essentiels en discussion dans la proposition de règlement sur les données à caractère personnel au sein de l'Union Européenne est la création d'un guichet unique qui règlerait les litiges intervenus à la suite de la gestion des données des consommateurs par les entreprises. L'idée est de confier les éventuels contentieux à la CNIL de l'Etat où l'entreprise concernée a son siège en lieu et place d'une consultation de l'ensemble des structures en charge de la protection des données au plan européen. Cette proposition est l'œuvre du député Viviane Reding. La question est débattue au Conseil *Justice et Affaires intérieures* qui, a réuni les ministres européens, le 6 décembre 2013 et l'Allemagne, suivie par la Hongrie, le Danemark et Islande opposent un refus de la technique proposée.

Si les instances étatiques, comme l'institution judiciaire sont sollicitées pour le règlement des litiges liés à la cybercriminalité, la nature complexe de cette infraction mérite d'être analysée par d'autres instances sous l'angle des modes alternatifs de règlement de litiges. C'est la question du règlement proposé par l'arbitrage.

C- L'arbitrage dans la répression de la cybercriminalité

Le droit pénal n'est pas naturellement une matière arbitrable mais la nature des contrats et des rapports et faits juridiques intervenants dans le domaine de la cybercriminalité oblige à s'interroger sur l'intervention de l'arbitre dans le cadre de la répression de cette criminalité informatique particulière. C'est pourquoi, bien qu'il ne soit pas un juge national, l'arbitre peut jouer un rôle dans les contentieux liés à la cybercriminalité.

Est-il possible d'avoir recours à un tribunal arbitral en cas d'infractions cybercriminelles ? La question mérite d'être traitée dans la mesure où elle est abordée pour toutes les questions contractuelles liées à l'internet notamment à travers les principes d'Online Dispute Resolution (ODR).

Le fait que la cybercriminalité en général et les contrats ou délits liés au numérique en particulier soient considérés comme des actes et faits juridiques spéciaux justifie-t-il pour autant de confier ces domaines à un juge autre que le juge traditionnel ?

Si l'on se réfère aux différents cas relevant de la compétence du juge pénal ou parfois du juge civil, il n'est pas rare de voir que la question de la qualification juridique des faits est soulevée et difficilement résolue par ces juges. Ce ne sont pas leurs compétences qui sont remises en cause mais la complexité de traitement de la matière même de la cybercriminalité. Elle comporte à la fois et bien souvent des aspects techniques liés aux normes numériques mais également des aspects traditionnels civils et pénaux. Le fait que toutes ces composantes se mêlent ne rend pas facile le travail du juge de droit commun ou même du juge spécialisé (notamment en droit pénal).

Partant, certains auteurs ont suggéré une *lex electronica*[437] (qui rappellerait la *lex mercatoria*[438], la loi des marchands en matière de résolution des litiges commerciaux internationaux) comme référence à la résolution des litiges nés des activités numériques.

---

[437] Lex electronica c'est à dire la loi électronique.

[438] Lex mercatoria définie comme l'expression désignant les règles aménagées par les professionnels, en matière de contrats internationaux et suivies spontanément par les milieux d'affaires.

C'est en général dans le domaine de l'arbitrage que des règles spécifiques de ce type peuvent être utilisées comme loi des parties en cause. Dès lors, sous quelle forme peut se constituer un tribunal (arbitral) réglant les conflits cybercriminels ?

Certains domaines de la cybercriminalité comme les problèmes relatifs aux cyber-squattage ou aux infractions relatives aux noms de domaine sont régis par les règles de l'arbitrage.

a- La diversité des arbitrages possibles en matière de cybercriminalité

Plusieurs arbitrages existent et sont envisageables : l'arbitrage de l'OMPI, de l'ICANN et celui de la Chambre arbitrale Internationale de Paris. L'arbitrage est-il une voie pour régler les contentieux et sanctionne-t-il suffisamment en cas d'infractions cybercriminelle ?

1. L'arbitrage de l'Internet Corporation Assigned Names and Numbers.

Les noms de domaine sont des noms associés à des domaines pour faciliter l'identification des réseaux[439]. Il existe deux niveaux de domaines : certains sont génériques ou à dimension internationale par exemple « *.com* » et d'autres sont nationaux et spécifiques comme le « *.fr* ».

L'organisme en charge de l'adressage des noms de domaine au plan international est l'Internet Corporation Assigned Names and Numbers en abrégé ICANN[440]. Cet organisme a été créé en Amérique en novembre 1998 avec la coopération du Ministère du commerce américain et d'une entreprise privée[441] en charge de la gestion des noms de domaine. La société la Network Solution Inc. (NSI) signe avec le Ministère du commerce américain plusieurs amendements à la suite desquels l'enregistrement des noms de

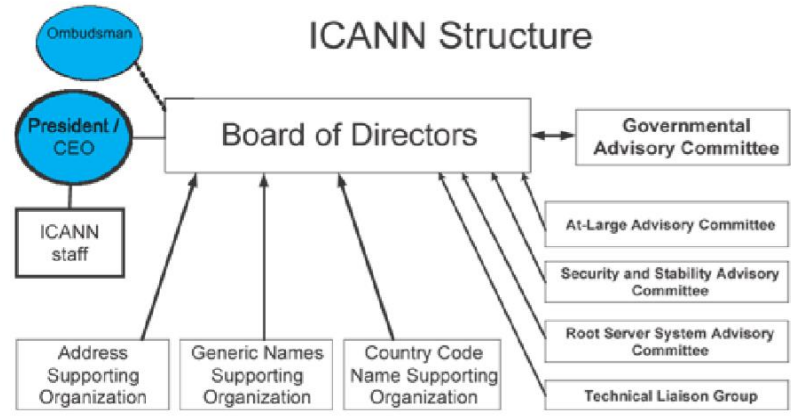
---

[439] Voir **ITEANU O**., « L'Icann, un exemple de gouvernance originale ou un cas de law intelligence ? », *Les Cahiers du numérique* 2/ 2002 (Vol. 3), p. 145-157.

[440]Cf**. CHEVALIER J.,** L'Etat régulateur, Revue française d'administration publique, 2004/3 n°111, p. 473-482.

[441] Cf. **POULLET Y**., Technologies de l'information et de la communication et « co-régulation » : une nouvelle approche ? Liber Amicorum Michel Coipel, in Droit & nouvelles technologies, 2004.

domaine est confié à l'ICANN, organisme à but non lucratif[442]. C'est donc depuis l'expansion d'Internet dans la société civile que les noms de domaines sont gérés par l'ICANN et ce de manière centralisée[443]. Le graphique suivant permet d'avoir un aperçu de l'organisation de l'ICANN.



source : www.icann.org

L'ICANN met en place dès lors des processus ou des procédures en vue de régler les conflits dont il a à connaître notamment dans l'attribution des noms de domaine. C'est la mise en place de tels procédés de gestion des conflits intervenant dans le monde des affaires principalement que l'ICANN possède en ses organes un centre d'arbitrage.

L'Internet Corporation for Assigned Names and Numbers (ICANN) [444] a recours à un tribunal d'arbitres indépendants pour résoudre les litiges issus de l'attribution des

[442] cf. http://www.icann.org/en/resources/registrars/accreditation/history; voir également, **SCHULZ Th.,** Online Dispute Resolution, p. 37.

[443] Cf. **BERLEUR J.et POULLET Y.,** Quelles régulations pour l'Internet, *manuscript proposed for publication,* Cahiers du Centre de Recherche Informatique et Droit n° 22, 2001, P.133-151, 2001.

[444] L'ICANN est l'Autorité internationale en charge de l'attribution des noms de domaines.

noms de domaine surtout s'agissant des conflits entre marques[445]. En quoi consiste cette procédure ?

Pour adopter cette procédure, l'ICANN a confié depuis 1999, à des centres d'arbitrage accrédités, des litiges relevant des activités numériques. La procédure est connue sous le nom de l'Uniform Domain Name Dispute Resolution Policy (UDRP) [446].

Pour déléguer ses pouvoirs, l'ICANN a confié à l'OMPI l'arbitrage des conflits en matière de cybersquatting.

2. L'arbitrage de l'Organisation Mondiale pour la Propriété Intellectuelle

Grâce à l'intervention de son Centre d'Arbitrage et de Médiation, l'Organisation Mondiale de la Propriété Intellectuelle règle les litiges nés des contrats de propriété intellectuelle. Dans ce cadre, deux procédures particulières que sont l'arbitrage classique et l'arbitrage accéléré sont concernés. Elles offrent ainsi la possibilité aux particuliers de résoudre les problèmes sans aucun recours aux tribunaux traditionnels.

En rapport avec la cybercriminalité, le centre d'arbitrage de l'OMPI traite essentiellement des litiges relatif au *cybersquatting* c'est-à-dire des abus de déclaration de noms de domaine portant atteinte à des marques existantes.

C'est ainsi que le centre d'arbitrage de l'OMPI a été saisi de litiges opposant des célébrités à un cybersquatteur. Dans les faits, un cybersquatteur déclare des noms de domaines « brucespingeer.com » et « celineDion.com » auprès de registraire. S'estimant lésées, les chanteurs concernés ont saisi l'OMPI pour régler ces litiges.

S'agissant de Bringspingeer, l'OMPI décide de ne pas restituer le nom de domaine au chanteur. Par contre pour ce qui est de Céline Dion, l'OMPI décide le contraire.

Une troisième institution intervient dans le domaine de l'arbitrage : c'est la Chambre arbitrale internationale de Paris.

---

[445] Cf. **WARUSFEL Bertrand**, La propriété intellectuelle et l'internet, Dominos, Flammarion, 2001.

[446]Cf. **KAUFMANN-KOHLER G. & SCHULZ Th.,** Online Dispute Resolution Challenges for Contemporary Justice Kluwer Law International, International Arbitration, The Hague, The Netherlands, 2004.

3. L'arbitrage de la chambre Arbitrale Internationale de Paris

La Chambre Arbitrale Internationale de Paris intervient comme un acteur de l'arbitrage dans les affaires commerciales. Elle est en effet une institution à but non lucratif dont la vocation est de mettre à disposition des entreprises des règlements d'arbitrage et des solutions alternatives au règlement judiciaire de leurs conflits avec leurs partenaires d'affaires. Cet arbitrage est surtout sollicité par les entreprises dans leurs relations d'affaires avec leurs partenaires et fournisseurs en cas de conflits contractuels. Mais il peut arriver que des questions se posent quant à des cas de fraudes cybercriminels notamment à l'encontre de sociétés. Dans cette optique, l'arbitrage de la Chambre de Commerce peut être requis comme mode de règlement des litiges. C'est le cas notamment en matière de propriété industrielle ou d'application des règles propres aux brevets. Pour illustration, la chambre arbitrale internationale a reçu une demande d'arbitrage le 24 janvier 2007 et a rendu une sentence relative à l'utilisation d'une licence d'exploitation d'un brevet par une société[447]. Les faits soumis aux arbitres de la Chambre arbitrale sont relatifs aux difficultés d'exécution d'un contrat de licence d'exploitation signé entre deux sociétés. Le contrat avait pour objet lors de sa signature en 2001, la concession d'une licence exclusive d'exploitation à la société licenciée en vue de l'usage d'un brevet déposé pour des dispositifs de climatisation. Selon le contrat, *la société licenciée avait seule le droit de fabriquer, faire fabriquer en France, utiliser, vendre et faire vendre l'invention objet du brevet, en application de l'article I.2 du contrat du 8 juillet 2000.* Par la suite, la société concédant a estimé qu'il fallait transformer la licence exclusive d'exploitation en licence simple, la société licenciée ne payant pas convenablement les droits liés à son exploitation. En mars 2011, la société licenciée dépose la marque X alors que le concédant lui reprochait l'insuffisance d'exploitation au cours de l'année 2006. Naît un conflit entre l'utilisation de la licence d'exploitation qui

[447] Cf. publication des sentences arbitrales disponibles sur le site de la Chambre arbitrale internationale de Paris : http://www.arbitrage.org/admin/style/js/tinymce/uploaded/publications/sentences%20anonymes/S9931.docx.

est désormais simple (à la suite de la notification par le concédant) et le dépôt de la marque X par la société licenciée.

Les circonstances de cette affaire montrent la compétence de la Chambre arbitrale internationale de Paris dans le règlement des conflits dans les relations contractuelles d'affaires en matière de propriété industrielle.

La volonté de rechercher d'autres moyens qu'étatiques pour régler les litiges nés de l'usage des réseaux numériques est louable mais au regard des règles de base de l'arbitrage, se posent plusieurs difficultés.

b- Les difficultés de l'arbitrage dans le domaine de la cybercriminalité

Les difficultés liées à l'arbitrage concernent les aspects procéduraux c'est-à-dire nature des litiges et la sentence arbitrale prononcée d'une part et les aspects de souveraineté d'autre part.

1. Les difficultés procédurales

La première difficulté est liée à la nature même des litiges concernés.

En effet, en matière de conflits pouvant être réglés par la voie de l'arbitrage, il faut un lien entre les parties en conflit. Ce lien est pour la plupart du temps un lien contractuel. Il est aisé de procéder à un règlement à l'amiable entre parties contractantes, à moindre coût et avec la rapidité qui est reconnue à la procédure d'arbitrage. La question s'analyse en d'autres termes s'agissant des actes de la cybercriminalité.

Prenons l'exemple exploité : le cybersquatting. Il y a conflit entre une marque (en général de renom, donc qui a pignon-sur-rue du fait de ses activités), et un nom de domaine enregistré par une personne dont l'intention est clairement de porter préjudicie à ladite marque en monnayant le retrait de cette inscription aux services d'enregistrement des noms de domaine. Cette contrainte, à l'origine du conflit n'est aucunement contractuel puisqu'il n'existe aucun lien entre le cyber-squatteur et la marque concernée. De ce point de vue, il faut élaborer une règle spéciale visant à organiser ce type de règlement de litige et pouvant par conséquent donner compétence aux arbitres indépendants pour statuer sur l'objet du conflit.

Hormis la nature même du litige qui remet en cause le recours au tribunal arbitral, la sentence prononcée est la seconde difficulté : la sentence arbitrale, dans les règles de base n'a autorité de la chose jugée qu'à la condition que le détenteur de cette sentence en demande l'exequatur au juge compétent. C'est dire que la décision qu'aura rendu l'arbitre ou le tribunal arbitral n'est pas contraignante en elle-même, ni automatiquement comme c'est le cas pour une décision de justice rendue par un juge étatique.

De ce point de vue, il n'est pas certain qu'un cyber-squatteur contre lequel une sentence arbitrale a été rendue se voit dans l'obligation, de facto, de l'exécuter et de retirer son enregistrement de nom de domaine auprès des services concernés.

Si l'arbitrage est un recours efficace pour régler les problèmes de cyber-squatting, il n'en va pas automatiquement de même pour les autres composantes de la cybercriminalité. La virtualité liée à la cybercriminalité ne facilite pas le règlement des conflits sous l'angle de l'arbitrage tel qu'utilisé dans les relations commerciales d'affaires traditionnelles.

2. Les difficultés liées à la souveraineté

Le recours au juge non étatique, c'est-à-dire à l'arbitrage aurait dû permettre d'éviter à nouveau les critiques liées à la souveraineté des Etats surtout dans le domaine de la cybercriminalité où les frontières n'existent pas en réalité. Il n'en est rien. Les critiques adressées à l'encontre de la gestion des noms de domaine par l'ICANN cachent des questions de politique, de gouvernance de l'Internet par les Etats-Unis. Le droit technique des réseaux et de leur attribution se heurte ainsi au droit des Etats[448].

L'ICANN est lui-même critiqué au niveau de ses compétences : les missions dévolues ne sont pas limitées au domaine technique et touche la gestion économique[449].

Sa procédure d'UDRP est également critiquée en ce qu'elle paraît peu transparente.

---

[448]Cf. **ROJINSK C**., cyberespace et nouvelles régulations technologiques, Dalloz 2001, Chronique p.84.

[449] Voir sur ce point **ADAM Nicolas**, L'ICANN et la gouvernance d'Internet: une histoire organisationnelle. *Cahier de recherche*, 2007, vol. 7, p. 01.

Par ailleurs, la remise en cause des décisions d'autres organismes comme l'OMPI pour la gestion des suffixes nationaux450 dans les cas de cybersquatting est révélateur de complications : l'arbitrage n'est pas accepté en tant que procédure adéquate pour régler des cas de cybersquatting.

En réponse aux critiques relatives au choix de l'OMPI comme organisme d'arbitrage, il faut répondre que les faits de la décision Céline Dion contre le cybersquatteur font intervenir deux particuliers. Ce sont donc les concernés qui ont choisi de confier leur litige à un arbitre et donc la compétence en l'espèce est d'attribution, elle n'est pas définie par les lois étatiques.

---

[450] Interview avec **FROMKIN**, Expert américain L'OMPI veut surtout accroître l'activité de son centre d'arbitrage, http://www.transfert.net/a4321.

Conclusion du chapitre 1

L'approche européenne de la politique de lutte contre la cybercriminalité est particulière dans la mesure où les Etats de l'Union Européenne adhèrent d'abord à la politique mise en place par le Conseil de l'Europe[451] pour ensuite, et sur ce fondement, construire la stratégie de lutte de l'Union. Pour preuve, la Convention de lutte contre la cybercriminalité, texte fondamental en la matière, est élaborée par le Conseil de l'Europe. Cette adhésion de l'Union Européenne à la stratégie du Conseil de l'Europe est une articulation particulière de l'Europe politique (qui dépasse le seul cadre des Etats membres de l'Union Européenne) avec l'Europe économique (qui, elle, est restreinte aux membres de l'Union Européenne). D'ailleurs les questions relatives à la cybercriminalité intéressent beaucoup le Parlement européen tout comme le Conseil de l'Europe.

Aussi bien au niveau de l'espace communautaire européen (Union européenne) que dans l'espace politique européen (Conseil de l'Europe), le corpus normatif de lutte contre la cybercriminalité est riche de textes d'un point de vue de la sanction contre ce phénomène.

Il y a des incriminations concernant chacune des composantes de la criminalité informatique même si cette législation peut être qualifiée de touffue et éparses. Il pourrait lui être reproché son abondance en incriminations, d'autant plus qu'elles ne sont pas toujours contenues dans le code pénal. Mais cette richesse est un avantage et permet de mieux cerner la spécificité des infractions composant la cybercriminalité.

Cette spécialisation des types d'infractions est d'ailleurs source de difficulté dans la coordination juridictionnelle. Il faut le souligner en tenant compte des diverses attributions aux juges. L'Union Européenne et surtout ses Etats membres gagneraient davantage en qualité si une réelle coordination existait entre les différents juges intervenant au plan de la répression de la criminalité contre la haute technologie. A

[451] Dans la mesure où les Etats de l'Union européenne ont accepté de ratifier la Convention du Conseil de l'Europe sur la cybercriminalité et de l'intégrer à leur corpus juridique, il est possible d'arguer que ces Etats ont accepté la politique mise en place par le Conseil de l'Europe par le biais de la Convention de Budapest.

l'instar des Juridictions Interrégionales Spécialisées, la collaboration à une échelle plus étroite doit être accentuée.

L'arbitrage et les modes alternatifs de règlement des litiges font apparaître des sanctions spécifiques comme le retrait des noms de domaine ou encore l'interdiction d'usage des noms de célébrités dans des enregistrements de noms de domaine ou en tant que marque par exemple.

Si les Etats de l'Union Européenne ont une politique aussi fournie, appuyée par des organismes comme la CNIL, le Groupe article 29 et des structures européennes comme le contrôleur européen, il n'en est pas de même pour les Etats de l'Afrique de l'Ouest.
Cet espace est en réelle construction de sa charpente combattive contre la cybercriminalité.

CHAPITRE 2 :

LA CONCEPTION OUEST- AFRICAINE DE LA LUTTE CONTRE LA CYBERCRIMINALITE

En ce qui concerne l'Afrique en général et l'Afrique de l'Ouest en particulier, il convient de parler de conception en matière de lutte contre la criminalité informatique.
L'Afrique de l'Ouest est géographiquement composée de 16 Etats qui sont : le Bénin, le Burkina Faso, le Cap-Vert, la Côte-d'Ivoire, la Gambie, le Ghana, la Guinée, la Guinée Bissau, le Libéria, le Mali, la Mauritanie, le Niger, le Nigéria, le Sénégal, la Sierra Léone et le Togo.

Deux optiques sont à analyser en ce qui concerne ce continent :

D'une part, le fait que les nombreuses infractions perpétrées aient pour origine l'Afrique et singulièrement des Etats comme le Nigéria, la Côte-d'Ivoire, le Ghana, le Sénégal, amène à se préoccuper des conséquences de ces infractions dans les échanges internationaux, avec l'Europe notamment.

D'autre part, l'Afrique ne saurait rester en marge des avancées technologiques actuelles.
En effet, l'Afrique a pris en marche le réseau internet mais la véritable question afin de régler celle de la lutte contre la cybercriminalité est celle de savoir auprès de qui a-t-elle trouvé cette technologie ? Est-ce au contact des européens dans ses relations traditionnelles d'échanges ? Auquel cas, il serait convenable d'étudier l'impact des divers accords intercontinentaux existants pour en extraire des explications et des solutions au problème présent.
Ou alors l'avènement de l'internet africain et par ricochet des technologies de l'information gravitant autour de ce réseau, a-t-il d'autres origines comme les Etats-Unis ?
Il est certain que la source des origines des Technologies de l'Information et de la Communication (TIC) en Afrique de l'Ouest pourrait justifier des accords établis par alignement des conventions existantes.

Force est cependant de remarquer que le continent africain accuse un certain retard qui n'est toutefois pas négatif (section 1). Ce retard est un gage de correction, à l'avenir, des erreurs commises par les prédécesseurs dans la lutte contre la criminalité informatique. En d'autres termes, il serait possible de tenir compte des failles des systèmes de coercition déjà en place en Europe notamment pour éviter les pièges et les écueils commis.

Le cas de l'Afrique de l'Ouest est intéressant dans la mesure où cette région est amenée à construire une répression régionale de la cybercriminalité à l'instar de l'Union Européenne mais avec des améliorations (section2).

L'Afrique n'est pas encore dotée de système de surveillance d'internet à l'image de certains Etats comme la Chine[452], le Brésil ou même le Canada[453] et l'Afrique du Sud qui se sont dotés de système de surveillance d'internet. En réponse à ce manque, la coopération générée par l'Union européenne avec l'Afrique pourrait permettre de lutter efficacement contre la cybercriminalité.

La lutte contre la cybercriminalité a plus d'un intérêt en ce qui concerne le continent africain dans sa globalité. Il faut mentionner que les technologies donnent des possibilités inimaginables pour résoudre de réels dilemnes. En témoigne l'exemple de l'apport de la haute technologie en matière d'études statistiques sur des régions enclavées. Ne serait-ce que résoudre le problème d'accès à ces zones notamment par des outils technologiques en lieu et place des hommes, permet de sauver des vies. Dans cette

---

[452] Du fait de son système autoritaire de communisme, la Chine a placé internet sous haute surveillance. Voir pour une présentation détaillée : http://actu-obsession.nouvelobs.com/internet-chine.html et aussi http://obsession.nouvelobs.com/high-tech/20050302.OBS0094/la-censure-d-internetva-etre-renforcee.html ou encorehttp://obsession.nouvelobs.com/high-tech/20100313.OBS9717/google-devrait-fermer-son-service-en-chinois.html.

[453] Lire à ce sujet l'article de presse dans le journal Le Monde du 15 février 2012 « *Le Canada renforce la surveillance de l'Internet* ». Pour une version en ligne, consulter http://www.lemonde.fr/technologies/article/2012/02/15/le-canada-renforce-la-surveillance-d-internet_1643454_651865.html. Cette proposition parlementaire se présente sous la forme d'un projet de loi C-30 édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois. Le projet est disponible sur http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5380965&file=4

optique s'inscrit la télémédecine. Il ressort de ces deux illustrations que internet revêt d'autres aspects tout aussi importants que la communication.

Fort de toutes ces raisons, il convient d'analyser les retards accusés par l'Afrique de l'Ouest pour y remédier à travers la mise en place de systèmes juridiques fiables.
L'étude de ce retard et de l'instauration des normes répressives est un facteur de compréhension pour parvenir à lutter efficacement contre le fléau cybercriminalité.

Section 1 : Le retard dans la sanction contre la cybercriminalité

Il est étonnant que l'Afrique de l'Ouest ait accusé un retard dans la lutte contre la cybercriminalité dans la mesure où cette partie du continent entretient depuis plusieurs années d'importantes liaisons internet avec l'Europe et les Etats-Unis.

En effet, les réseaux existent entre l'Afrique de l'Ouest, la France, le Royaume-Uni et les Etats-Unis[454]. Bien que ces réseaux de communication existent, il faut constater que leur utilisation s'est faite tardivement en comparaison des connexions dans les pays précurseurs comme les Etats-Unis. Pour ces derniers, elles se sont opérées dans les années 40, alors que le continent africain a attendu 40 ans après pour utiliser les réseaux numériques. Ce n'est d'ailleurs qu'après 1995 qu'internet a réellement remplacé le recours aux réseaux téléphoniques[455].

Le 15 octobre 1994, les universitaires et les chercheurs africains en informatique, en mathématiques et en sciences de la vie, réunis à Ouagadougou ont, dans le cadre du second colloque africain sur la télématique pour le développement en Afrique (CARI'94) [456] adopté ce qu'il est convenu d'appeler la déclaration de Ouagadougou. Cette convention a été signée entre 22 Etats dont 18 pays africains et elle affirme que « internet

---

[454] Cf. **BERNARD E.**, Internet et ses frontières en Afrique de l'Ouest, Annales Géo, n°645, 2005, pages 550-563.

[455] Idem. Voir aussi, **BA Abdoul**, Internet, cyberespace et usages en Afrique, édition l'Harmattan, 2003.

[456] La première édition a eu lieu en 1992 à Yaoundé au Cameroun sur l'initiative de l'université des nations unies et de l'institut National de Recherche en informatique et en Automatique (INRIA) cf. page 12 de Internet, cyberespace et usages en Afrique, Abdoul BA édition l'Harmattan, 2003

permet le libre accès à l'information et à la communication à l'échelle internationale et représente donc un enjeu essentiel pour les pays en développement ». La signature de la déclaration de Ouagadougou a été suivie de la signature le 03 mai 1995 à Addis-Abeba de la résolution 795 intitulée « mise en place de l'autoroute de l'information en Afrique[457] ».

A la suite de cette résolution, le 07 mai 1996, la Commission Economique pour l'Afrique en a adopté une autre : la résolution n° 812 intitulée « Mise en œuvre de l'initiative société africaine à l'ère de l'information[458] ». Compte tenu de la mise en place de ce dispositif, il convient de s'interroger sur ce retard considérable accusé par le continent africain dans le déploiement d'internet et des autres technologies afférentes.

§1- Les raisons du retard général des Etats ouest-africains

Le fait pour l'Afrique de l'Ouest de s'être tardivement mise à sanctionner les contrefacteurs et autres délinquants informatiques se justifie par plusieurs raisons.

Hormis la connexion tardive qui est la raison première, l'utilisation même des outils informatiques s'est faite longtemps après les autres continents. Il convient d'insister sur le recours à l'informatique de manière globale dans la mesure où d'une manière discrète, et sur un plan technologique, il faut remonter dans les années 80, précisément en 1987 pour découvrir que la ville d'Abidjan, capitale actuelle de la Côte - d'Ivoire est reliée à cette période aux réseaux télématiques de IBM[459].

---

[457] La résolution a été adoptée au cours de la XXI e réunion de la conférence des ministres de la Commission Economique pour l'Afrique des Nations Unies et est consultable sous le lien suivant : http://www.uneca.org/fr/pages/795-xxx-mise-en-place-de-lautoroute-de-linformation-en-afrique.

[458] Cf. Résolution 812 (XXXI): Mise en œuvre de l'Initiative société africaine à l'ère de l'information (AISI) (Adoptée par la vingt-deuxième réunion de la Conférence des ministres de la Commission économique pour l'Afrique (CEA), le 07 mai 1996) disponible sur le site de l'UNECA : http://www.uneca.org/fr/pages/812-xxxi-mise-en-oeuvre-de-linitiative-societe-africaine-lere-de-linformation-aisi.

[459] Cf. **DESBOIS Dominique, VIDAL Georges**, *Abidjan devient le premier nœud africain du réseau télématique EARN.* In: Tiers-Monde.1988, tome 29 n°116. pp. 1237-1243.

D'ailleurs, les connexions des particuliers ne sont pas encore alignées sur celles des entreprises à l'heure actuelle.

Il faut même se réserver quant à l'existence de réels accès internet en ce qui concerne les entreprises : la répartition des connexions internet n'est pas égale pour les entreprises d'un pays à l'autre. Ne serait-ce qu'au niveau des fonds nécessaires au financement de ces structures informatiques, se posent de réels problèmes. Quels budgets les Etats sont-ils prêts à investir dans la mise en place des connexions internet des ménages quand on sait que d'autres priorités existent notamment la stabilité des Etats, les questions vitales de santé et d'alimentation au quotidien ? Les structures entrepreneuriales privées sont-elles plus avancées sur ce plan financier ?

A- Les raisons technologiques du retard

Les raisons techniques sont celles relatives au fonctionnement de base à savoir l'implantation des connexions de communication ou des réseaux de télécommunication. (a). Elles sont également celles des structures.

a- L'implantation des connexions de communication

Tout d'abord, le retard des pays africains dans l'accès aux technologies de l'information et indirectement le retard dans la création de législations contre les infractions informatiques s'explique par le fait que pendant longtemps l'Afrique n'a eu qu'un seul câble sous-marin, le South Atlantic 3 (SAT- 3) reliant le sud de l'Europe à l'ouest du continent africain[460].

Ensuite, la dépendance technologique de l'Afrique par rapport à l'Europe et aux Etats-Unis n'est pas de nature à faciliter son développement numérique. En effet, l'Afrique ne dispose pas de cette technologie. Elle l'importe et tous les contrats en

[460] cf. **Abdoul BA,** Internet, cyberespace et usages en Afrique, édition l'Harmattan, 2003 ; voir aussi **CHENEAU-LOCQUAY A.**, Les fractures numériques nord/sud en questions, Cean-CNRS/ Africa'nti, collection Cahier des sciences sociales sur les enjeux des technologies de la communication dans les suds, éditions L'harmattan, DL 2004 p 70-71 ; et regarder en plus http://www.lemonde.fr/week-end/article/2011/02/18/internet-en-afrique-la-fin-du-desert-numerique_1464281_1477893.html. Compléter avec J. BONJAWO, Révolution numérique dans les pays en développement, l'exemple africain, éditions Dunod, Paris 2011.

matière d'installation et de vente d'outils informatiques ne sont jamais accompagnés d'un transfert de technologie. Ce qui explique que les Etats africains ont constamment besoin de faire appel à de la main d'œuvre étrangère qualifiée pour l'implantation des infrastructures. Importer de la main d'œuvre qualifiée et de la technologie représente pour l'Afrique un coût qu'elle n'est pas toujours en mesure d'assurer.

Il pourrait être reproché à des structures de téléphonie, implantées en Afrique de l'Ouest de ne pas déployer suffisamment d'infrastructures en ce sens. Mais ce reproche sera très rapidement écarté dans la mesure où le caractère privé de ces structures ne leur donne pas, même si elle le désirait, toute la latitude pour agir sur des territoires gouvernés par des politiques bien déterminées. Elles doivent nécessairement avoir les accords et les agréments nécessaires pour déployer leurs technologies d'autant plus qu'elles répondent souvent à des appels d'offres élaborés par les Etats eux-mêmes. C'est surtout que géographiquement, les sociétés de téléphonie et de communication sont limitées par les engagements qu'elles signent avec les Etats, qui comptent bien préserver leur souveraineté dans certains domaines tels que la communication. En 1996, 30.000 lignes téléphoniques en Côte-d'Ivoire sont ouvertes.

L'objectif est d'atteindre 500.000 lignes. Le lancement du marché de téléphonie mobile pour le Sénégal s'est fait en même temps que le téléphone fixe. Alors qu'en Côte-d'Ivoire, ce lancement s'est fait en deux phases en séparant le fixe du téléphone mobile. Il faut noter l'interconnexion qui se crée du fait de ces créations de lignes fixe et de mobile. La méthode du « prépayé » change la donne en 2000. La carte SIM est alors vendue à 25 000 F CFA.

Enfin, l'absence d'écoles pour former les ingénieurs qualifiés, l'insuffisance de la couverture énergétique des territoires et les difficultés structurelles comme l'accès des routes sont autant de freins à l'émergence d'une « Afrique connectée ».

Quelles sont les difficultés structurelles à considérer ?

b- Les difficultés structurelles

La difficile implantation du numérique dans les milieux ruraux est due aux conditions structurelles comme l'accès des routes, lui-même lié à la couverture rurale de l'énergie dans ces zones.

C'est ensuite la grande importance numérique des populations rurales qui est à l'origine du retard dans l'utilisation des connexions informatiques.

En effet, la densité des populations en milieu rural est si importante qu'il reste difficile de répondre aux besoins de tous les ménages. L'exemple des populations du Sénégal est illustratif. Et ce n'est pas le seul Etat dans lequel ce constat est réalisé. Selon une étude réalisée par des chercheurs africains[461] : plus de 60% de la population a exprimé un besoin en moyen de communication moderne c'est-à-dire, le téléphone, la connexion Internet. Dans les faits, il ressort de l'approche de terrain faite par ces chercheurs qu'il n'existe pas de télé-centres implantés. Or cette implantation est primordiale dans la diffusion des moyens de communication susmentionnés. C'est dire que les zones rurales (pour la plupart) et certaines zones urbaines ne sont pas suffisamment équipées pour avoir un réel accès au réseau.

C'est à s'interroger sur les fonds investis par les pouvoirs publics en matière de couverture en réseaux.

Enfin, la pédagogie qui doit suivre l'implantation desdites connexions reste à faire.

A cette dépendance technologique et ces difficultés structurelles s'ajoutent les questions financières.

B- Les raisons financières du retard africain

Les raisons financières constituent un autre frein à une excellente lutte contre la cybercriminalité en ce qui concerne les pays africains.

En effet, il faut considérer les budgets mis en place pour favoriser une étendue de l'utilisation transparente des réseaux numériques.

Pour ce faire, il faut une première phase de mesure les attentes des populations en termes de besoin quant à l'accès au numérique. Cette phase permet de tenir compte de la fracture numérique. Il s'agit de la différence entre les Etats développés (comme ceux de l'Union européenne) et les Etats en voie de développement (comme c'est le cas pour la plupart des pays de l'Afrique de l'Ouest) au niveau de l'usage de l'informatique.

La fracture numérique est définie sous plusieurs angles. Et dans cette optique, FULSSACK estime qu'elle revêt différentes formes et concerne à la fois l'accès, l'usage, le contenu et la prise de décision[462].

L'OCDE quant à elle, estime dès 2000, dans son rapport annuel, que la fracture numérique est devenue un terme prioritaire. C'est pourquoi elle en propose une définition, en 2001. Et cette définition est communément reprise dans la plupart des études[463]. Elle précise que la fracture numérique est le terme se référant aux disparités entre individus, foyers, entreprises et aires géographiques aux différents niveaux socio-économiques en termes d'accès aux TIC et d'utilisation de l'Internet pour une large variété d'activités[464]. Pour mettre fin à ce fossé entre les Etats ayant accès à la technologie numérique et ceux qui en sont privés, plusieurs initiatives mondiales sont élaborées. C'est d'ailleurs dans ce cadre que l'ONU prend en compte la proposition de

---

[461] **BEN HENDA M. ET TONYE E.,** Tic et éducation applications, recherches et perspectives, éditions L'Harmattan, p.97-98.

[462] Cf. **FULSSACK J-L. et al.** « Fracture numérique » in Commission nationale Française pour l'UNESCO, La société de l'information : glossaire critique, Paris, La Documentation Française, 2005.

[463] Cf. **RALLET A. et ROCHALENDET F.**, *la fracture numérique : une faille sans fondement*, Revue Réseaux n° 127-128, éditions la Découverte, 2004.

[464] Pour la version originale en anglais, cf. *Understanding the digital divide, OECD*, 2001, p. 3: **"**The gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the internet for a wide variety of activities. The digital divide reflects various differences among and within countries. The ability of individuals and businesses to take advantage of the internet varies significantly across the OECD area as well as between OECD and non-member countries. Access to basic telecommunications infrastructures is fundamental to any consideration of the issue, as it precedes and is more widely available than access to and use of the internet".

l'Union Internationale des Télécommunications de mettre en place le sommet mondial de la société de l'information en 2003, à Genève puis en 2005 à Tunis[465].

La place prioritaire qu'occupe dès lors l'accès aux technologies ou la transformation de la société en société de l'information exige des investissements d'ordre financier. Sous cet angle, quel diagnostique peut-on établir quant à l'importance des fonds injectés par chaque Etat dans son accès aux technologies de l'information et de la communication ?

Le constat est simple : les Etats développés engagent plus de frais en termes de coûts d'investissement dans le domaine de l'informatique en particulier et de la communication en général. Ces Etats ont une avance quant à la technologie. Il n'y a qu'à observer le nombre de foyers dotés d'un ordinateur portable ou fixe et l'utilisation qui en est faite au quotidien. L'habitude de travailler sur les outils informatiques est à peine naissante en Afrique de l'Ouest.

Les Etats africains en sont encore au stade de l'éducation des habitudes des populations à l'usage du numérique. Il est même possible de remarquer que les entreprises sont à peine dotées de suffisamment d'outils. Quant aux ménages, très peu de personnes (à part les classes sociales aisées) bénéficient d'une connexion internet.

Dès lors, les priorités budgétaires ne sont pas réellement au stade de la dotation numérique des entreprises et des ménages même si ce n'est pas le cas dans certains pays comme la Côte-d'Ivoire, le Sénégal ou le Burkina Faso, où les entreprises et les particuliers sont de plus en plus équipés d'ordinateurs. On est pour ces pays à l'ère du tout numérique et il faut croire avec les équipements des administrations publiques en matériel informatique que la tendance sera de travailler avec ces outils et d'en exiger la sécurité des systèmes liés.

---

[465]Cf. **FRANCO Richard**, « la fracture numérique : diagnostic et parades », Politique étrangère, 2006/3 Automne, P. 531-544.

Une fois la phase d'identification des attentes des populations réalisée, la seconde phase est celle de l'évaluation concrète des budgets à déployer pour couvrir ces attentes en termes d'évolution numérique ou technologique.

Il faut remarquer que ces préoccupations financières sont à l'heure actuelle au cœur des réflexions étatiques africaines. Certes, ces nations ont accusé un retard mais la diffusion d'internet et l'accès aux technologies de l'information à tous sont traités. C'est notamment le cas en Côte d'Ivoire avec l'adoption d'un décret remplaçant le Fond National des Télécommunications (FNT) par l'Agence Nationale du Service Universel des Télécommunications / TIC (ANSUT), une société d'Etat dont les missions sont essentiellement de permettre l'accès de toutes les populations, en particulier, les plus défavorisées, aux outils et prestations essentiels de télécommunications/TIC, sur l'ensemble du territoire national. Cette société a été mise en place par le décret portant organisation et fonctionnement de la société d'Etat dénommée Agence Nationale du Service Universel des Télécommunications / TIC (ANSUT)[466].

Ces nouvelles initiatives des Etats montrent la volonté de rattraper le retard accusé. En effet, l'objectif de permettre à toutes les couches sociales d'avoir un accès aux outils des nouvelles technologies est rassurant contrairement au passé où d'autres priorités étaient mises en avant.

Les raisons technologiques naturelles ou financières sont certainement des explications à la lenteur dans la mise en place des dispositifs répressifs de la cybercriminalité. Il convient par ailleurs d'analyser les accords qui avaient pour but de favoriser le développement des pays africains compte tenu de leurs relations d'affaires avec le continent européen. Quelle est la place ou le rôle des accords de partenariats mis en place entre l'Afrique et l'Europe dans la lutte contre la cybercriminalité ?

---

[466] Décret portant organisation et fonctionnement de l'ANSUT, agence créée par l'article 157 de l'ordonnance n° 2012-293 du 21 mars 2012 publiée au Journal Officiel de la République de Côte-d'Ivoire du 10 janvier 2013.

§2- La place des accords de partenariat Afrique - Europe dans la lutte contre la cybercriminalité

L'Europe et l'Afrique ont toujours entretenu des rapports de coopération dans divers domaines.

En rappel, la seconde guerre mondiale laisse la place aux différentes conquêtes coloniales qui sont suivies de la volonté d'indépendance des Etats colonisés.

Après ces grands bouleversements, de nouveaux changements arrivent avec la décolonisation de ces Etats et la capacité de ces derniers à se prendre en charge par rapport aux colonisateurs. C'est dans le cadre de cette autonomie de ces peuples anciennement dominés que s'insèrent les accords ACP-UE.

Les premiers accords interviennent dans les années 60 à Yaoundé au Cameroun.

Par la suite, sont signés les accords de Lomé de 1975 à 1995 puis les années 2000 voient les accords de Cotonou signés à Cotonou au Bénin, le 23 juin 2000 et révisés le 25 juin 2005 au Luxembourg[467].

Tous les domaines et secteurs d'activité comme l'énergie, l'industrie, l'agro-alimentaire, l'aéronautique et l'informatique sont concernés. Mais la priorité est laissée au développement des villages et des zones rurales. Certains secteurs comme la communication s'en trouvent délaissés.

L'Europe a souvent manifesté sa participation dans cette coopération Europe-Afrique par des contributions financières permettant la réalisation d'un certain nombre de projets.

C'est pourquoi, dans le cadre de la lutte contre la cybercriminalité, certaines institutions de l'Union européenne comme la Banque Européenne d'Investissement, apportent leur

[467] cf. Union européenne, Direction générale du développement, Accord de partenariat ACP-CE signé à Cotonou le 23 juin 2000: révisé à Luxembourg le 25 juin 2005, Office des publications officielles des Communautés européennes, Luxembourg, 2006 ; voir également, **DIALLO Amadou**, la dimension politique du partenariat UE/ACP depuis l'accord de Cotonou : les défis, enjeux et perspectives, thèse de droit sous la direction de Albert Bourgi, Université de Reims Champagne Ardenne, 2008.

soutien par des engagements financiers dans le domaine des médias, de l'informatique et de l'innovation technologique.

A- Les engagements respectifs dans le cadre des ACP-UE

Il est intéressant de partir de l'accord entre les ACP[468] et les pays de l'Union européenne pour comprendre les raisons autres que techniques du retard des Etats africains dans la sanction des infractions cybercriminelles. Le contexte général de ces conventions permet d'en saisir les applications spécifiques à la cybercriminalité.

a- Le contexte général

Le contexte général des accords ACP-UE est à l'origine, celui de la *coopération économique et commerciale*[469].

Aujourd'hui, ces accords de coopération ACP-UE incluent aussi des domaines autres que le commerce et l'aide.

En effet, l'Union européenne octroie des subventions par l'intermédiaire de la Banque européenne d'investissement et du Fonds européen de développement (FED) pour financer les nouveaux secteurs comme le renforcement des infrastructures de base et de l'inter connectivité ...

A titre illustratif, le secteur de l'inter connectivité et celui de l'intégration régionale de l'Afrique de l'ouest, font l'objet de lignes budgétaires spécifiques définies sur la base d'études économiques réalisées pour les Etats membres de la CEDEAO en partenariat avec l'Union européenne. Ces études permettent de renseigner le Document Stratégie d'intégration régionale pour l'Afrique de l'Ouest[470] pour la période de 2011 à 2015.

---

[468] Cf. **LEMESLE Raymond-Marin**, la convention de Lomé : principaux objectifs et exemples d'actions 1975-1995, 20e anniversaire de la Coopération Union Européenne- Etats ACP, Paris, 1995, p.30. Voir également Rapport de la Commission Européenne sur La coopération UE-ACP en 1995, quel ajustement structurel ? Direction générale du Développement, Courrier ACP-UE, Tielt-Belgique, Juin 1996.

[469] Cf. « *Accord de partenariat ACP-UE* », Centre européen de gestion des politiques de développement-ECDPM, in Le Monde diplomatique du 03 mai 2005.

[470]Cf. BANQUE AFRICAINE DE DÉVELOPPEMENT FONDS AFRICAIN DE DÉVELOPPEMENT, Document de Stratégie d'Intégration Régionale pour l'Afrique de l'Ouest 2011-2015, départements

Selon les informations qu'elles contiennent, le programme pour faciliter l'intégration de l'Afrique de l'Ouest grâce aux nouvelles technologies intègre le budget alloué aux infrastructures à hauteur de 331,890 dollars d'Euros. Ces sommes importantes sont des aides accordées aux Etats dans le cadre général des accords UE-ACP.

Il existe à en parallèle de cette aide générale, des applications spécialement rattachées à la cybercriminalité.

b- Les applications spéciales liées à la cybercriminalité

Les applications liées à la cybercriminalité permettent d'aborder le délaissement des secteurs des communications. La radio par exemple, est l'un des moyens de communication répandu en Afrique dans les années 1990. Et pourtant, ce n'est pas un secteur réellement développé et mis en avant dans les politiques des Etats. Il faut dire que les gouvernants de l'époque étaient frileux à l'idée que les médias puissent servir d'outil de propagande politique notamment. Cette frilosité, n'est pas un gage de sécurité pour ces Chef d'Etats, qui entendaient protéger leurs acquis[471]. D'ailleurs, par la suite, la radio est un moyen pour diffuser les idéaux démocratiques. Les partis politiques uniques d'alors sont menacés par les idées d'opposition qui naissent avec la démocratie qui entre en ligne de compte dans les arènes politiques. La radio est un puissant média grâce auquel les populations reçoivent les informations nationales et internationales. Il est un véritable vecteur pour inciter les peuples[472].

Avec tous les accords internationaux de partenariat entre les Etats de l'Union Européenne (anciennement Communauté européenne), on peut raisonnablement s'étonner du retard accusé par les Etats dits partenaires : ils devraient être au moins au plan des législations au même niveau. Or, il faut constater qu'il n'en est rien.

---

régionaux – ouest (ORWA/ORWB) département du NEPAD, de l'intégration régionale et du commerce (ONRI), mars 2011.

[471] cf. **TOZZO E.**, « La réforme des médias publics en Afrique de l'Ouest, Servir le gouvernement ou le citoyen », *Politique africaine* 2005/1 n°97, p. 99-115.

[472] cf. **CAPITANT Sylvie** « La radio en Afrique de l'Ouest, un « média carrefour » sous-estimé ? », *Réseaux* 4/2008 (n° 150), p. 189-217.

Il existe plusieurs justificatifs à un tel écart entre les partenaires de l'Afrique de l'Ouest (principalement) et ceux de l'Union Européenne.

D'abord, il ne faut pas omettre le temps mis pour faire transposer de nouvelles dispositions règlementaires du type directive communautaire ou accord bilatéral dans les divers ordres juridiques nationaux. Cette étape est longue quel que soit l'avancement des systèmes législatifs et la rigueur dans la tenue des assemblées des députés et autorités qui légifèrent.

Ensuite, les accords établis entre les Etats de l'Union Européenne et les ACP ont évolué en fonction des avancées culturelles des Etats signataires. C'est dans ce cadre qu'il est convenu de parler de la maturité des accords UE-ACP de départ. Ces accords ont vu leurs objectifs initiaux évoluer avec les besoins des Etats ACP et leurs capacités à s'adapter aux changements liés à la mondialisation notamment.

Sous l'angle de ces accords, la Commission européenne est intervenue pour aider les pays membres des accords UE-ACP à établir leurs bases règlementaires de lutte contre la cybercriminalité. Cette aide épouse diverses formes et s'inscrit surtout dans le cadre du partenariat avec l'Union Internationale des Télécommunications[473]. Diverses actions sont menées pour en arriver à établir les bases règlementaires : il s'agit de :

- *L'aide à la construction de la législation*: par exemple pour l'élaboration de la Convention de l'Union Africaine sur la cybersécurité;
- *L'évaluation des besoins des Etats*, de *leur niveau de préparation aux cybermenaces et surtout de leurs aptitudes à réagir pour favoriser l'établissement des organes de lutte comme le CIRT o*u les équipes comme le Forum for Incidents Response and Security and Teams (*FIRST)* dans des Etats tels que le Burkina Faso, la Côte d'Ivoire, la Gambie, le Ghana, le Mali, le Niger, le Nigéria, le Sénégal, la Sierra Léone et le Togo.

[473] Cf. L'UIT consolide l'alliance mondiale contre les cybermenaces in *ITU NEWS, Cybersécurité*, n° 2, 2014 et pour une version en ligne : https://itunews.itu.int/Fr/5004-LUIT-consolide-lalliance-mondiale-contre-les-cybermenaces.note.aspx.

Enfin, il faut tenir compte des budgets votés pour mettre en application les lois adoptées. L'aspect financier a souvent fait défaut de la part des pays africains et les relations avec les banques et autres investisseurs étrangers servent à remédier à ce manque.

C'est dans ce cadre que la Banque Européenne d'investissement ainsi que des Etats européens et d'autres continents notamment asiatiques sont sollicités. C'est la question des instruments financiers des accords UE-ACP qui mérite d'être traitée.

B- Les instruments financiers des accords ACP-UE

Plusieurs instruments financiers interviennent dans la mise en œuvre de l'aide des Etats européens dans le cadre des accords ACP-UE.

Deux d'entre eux correspondent au cadre étudié et il s'agit du Fonds Européen de Développement et de la Banque Européenne d'investissement.

a- Le Fonds Européen de Développement

Le Fonds Européen de Développement est l'instrument financier dédié aux pays africains membres des ACP. Depuis le 1er Janvier 2008, le 10ème FED remplace le 9ème FED et couvre la période de 2008 à 2013 pour une enveloppe budgétaire de 22,7 milliards d'Euros dont 22 milliards environ sont alloués aux pays ACP[474].

D'ailleurs, le règlement (UE) N° 566/2014 DU CONSEIL du 26 mai 2014 modifie le règlement (CE) n° 617/2007 en ce qui concerne l'application de la période de transition entre le 10e FED et le 11e FED, jusqu'à l'entrée en vigueur de l'accord interne relatif au 11e FED[475], est une précaution prise pour assurer la teneur des engagements pris.

---

[474] Cf. http://www.espace-economique.francophonie.org/Domaines-d-intervention,372.html.

[475] Cf. RÈGLEMENT (UE) No 566/2014 DU CONSEIL du 26 mai 2014 modifiant le règlement (CE) no 617/2007 en ce qui concerne l'application de la période de transition entre le 10e FED et le 11e FED, jusqu'à l'entrée en vigueur de l'accord interne relatif au 11e FED publié au JOUE L 157/35 du 27 mai 2014.

Certains pays comme le Burkina Faso bénéficient pour le secteur des Technologies de l'Information et de la Communication de l'aide des Etats de l'Union européenne.

En effet, du fait de sa situation peu favorable, de pays enclavé par rapport à d'autres Etats de la même région ouest- africaine, le Burkina Faso reçoit pour plusieurs projets réalisés dans ce pays, de l'aide extérieure et principalement de l'Union européenne. Dans le secteur des médias, le Burkina Faso a des partenariats avec l'Union européenne dans plusieurs domaines d'intervention comme l'appui à la croissance via une aide budgétaire de 343.42 millions d'euros soit 225 milliards de F CFA. Ce budget est alloué dans le cadre de la dixième édition du Fond Européen de Développement[476].

C'est par l'intermédiaire du Fonds Européen de Développement que l'aide de l'Union Européenne est accordée au Burkina Faso.

Ces instruments financiers sont régis d'un point de vue juridique par l'article 4 de l'annexe IV de l'accord de Cotonou. Cette disposition prévoit que : « *1. Dès qu'il a reçu les informations mentionnées ci-dessus, chaque État ACP établit et soumet à la Communauté un projet de programme indicatif, sur la base de ses objectifs et priorités de développement et en conformité avec ceux-ci tels que définis dans la SC. Le projet de programme indicatif indique:*

a) le ou les secteurs ou domaines sur lesquels l'aide doit se concentrer;

b) les mesures et actions les plus appropriées pour la réalisation des objectifs et buts dans le ou les secteurs ou domaines de concentration de l'aide;

c) les ressources réservées aux projets et programmes s'inscrivant en dehors du ou des secteurs de concentration et/ou les grandes lignes de telles actions, ainsi que l'indication des ressources à consacrer à chacun de ces éléments; (…).

Il ressort de cet article que l'action de l'Etat aidé par l'Union européenne et nécessaire à la définition des aides qui lui sont octroyées dans le cadre du Programme du FED.

Le tableau ci-dessous retrace la répartition de l'enveloppe A de l'aide accordée par l'Union Européenne au Burkina Faso via le FED : la portion concernée est uniquement l'enveloppe A soit 529 millions d'Euros.

Domaines	Allocation indicative (en millions d'euros)	% correspondant à la proportion de l'enveloppe A utilisée	Modalité de mise en œuvre
Renforcement des infrastructures de base et de l'inter connectivité	140	26	Aide projet et aide budgétaire sectorielle
Appui à la bonne gouvernance	50	10	Aide projet et aide budgétaire sectorielle
Appui au cadre macroéconomique et à la réduction de la pauvreté	320	60	Aide budgétaire
Total		**100**	

La seconde partie de l'aide c'est-à-dire l'enveloppe B est d'un montant de 8.2 millions d'euros destinés à couvrir des *besoins imprévus tels que l'aide d'urgence dès lors qu'elle ne peut être financée par le budget communautaire.*

La Banque Européenne d'Investissement pour sa part intervient en tant qu'instrument facilitant les investissements et ce sont les dispositions de l'annexe II de l'Accord de Cotonou qui le précisent.

b- La Banque Européenne d'Investissement

[476] Cf. Coopération Burkina Faso/Union Européenne, partie I, chapitre 2, document de stratégie pays et Programme indicatif national 10ème FED 2008-2013.

La Banque Européenne d'Investissement prend une part active dans l'aide adressée aux Etats membres des accords ACP-UE. Elle octroie des prêts à long terme aux Etats.

Les télécommunications ne sont pas dans un premier temps, un domaine privilégié dans les Etats africains particulièrement du fait des problématiques de développement des zones rurales. Dans de nombreux Etats signataires des accords UE-ACP, la priorité est l'alimentation, le développement des zones rurales reculées, la lutte contre la famine et l'électrification. Les objectifs d'aide reposent sur la volonté de permettre une meilleure gestion de la vie économique mais aussi industrielle. Il faut convenir que du point de vue de l'acheminement des produits, il est plus cohérent d'assurer une bonne tenue des routes mais aussi de bons moyens de communication favorisant les échanges.

L'après 95 permet d'aborder les accords de Cotonou de 2000 et leurs protocoles.

Les accords ACP-CE se sont d'ailleurs poursuivis jusqu'en 2008 puisqu'ils ont été renouvelés et reconduits avec d'autres thèmes et des motivations nouvelles pour les renforcer notamment l'accomplissement de la condition démocratique. Il est fait appel à des techniques juridiques pour faire respecter des principes comme les droits de l'homme[477]. C'est ce que prévoit l'accord de Cotonou dans l'alinéa 8 du préambule lorsqu'il affirme « *considérer la Convention de sauvegarde des droits de l'homme et des Libertés fondamentales du Conseil de l'Europe, la Charte africaine des droits de l'homme et des peuples, ainsi que la Convention américaine des droits de l'homme, comme des contributions régionales positives au respect des droits de l'homme dans l'Union Européenne et es Etats ACP* ».

Si les Etats des ACP ont décidé de faire siennes ces Conventions internationales notamment des droits de l'Homme, c'est parce qu'ils y adhèrent. Par conséquent, ils manifestent la volonté d'être traités à l'instar des Etats de l'Europe et de l'Amérique.

---

[477] **CAPITOLIN Jean- Louis**, « *l'enjeu de la conditionnalité démocratique*, in Les Relations ACP/UE après le modèle de Lomé : quel partenariat ? p. 372, éditeur Daniel PERROT, éditions Bruylant, Bruxelles, 2007.

Il faut cependant souligner que la fracture numérique qui existe en Afrique d'une manière générale doit être résorbée compte tenu de cette volonté de traitement égal manifeste. Les Etats de l'Union européenne ont dans cette optique répondu par l'affirmative. Il est possible de lire dans le chapitre 2, intitulé champ de la coopération commerciale et économique, les Etats signataires de l'Accord Afrique Pacifique Caraïbes, s'engagent à contribuer au développement des secteurs industriels.
Or, le développement des secteurs industriels passent par les réseaux de communication. Est donc pris en considération l'aspect communicationnel des échanges entre partenaires aussi bien au plan régional qu'international.

Partant, se pose la question de l'étendue de ces engagements des Etats signataires des accords ACP.

L'engagement pris pour contribuer au développement des secteurs industriels doit tenir compte du secteur des réseaux de communication. Le constat à l'heure actuelle est l'avancée des moyens de communication sans une homogénéité dans leur usage et encore moins dans leur règlementation. Certains Etats pourtant signataires de ces accords ne sont pas à la pointe de la technologie contrairement à d'autres. L'exemple des hôpitaux non pourvus d'ordinateurs suffisamment performants pour les listings des patients, leurs informations ou encore le simple suivi médical en 2003 par exemple en est la preuve[478].

Pour une meilleure gestion des budgets alloués aux Etats ACP dans le cadre des accords APE avec l'Union Européenne, plusieurs phases avaient été prévues et la seconde a été lancée en septembre 2002 à Bruxelles avec les négociations et poursuivie en 2003[479].

Sur le plan des télécommunications, les aides accordées ne sont intervenues que dans quelques Etats : il s'agit du Nigéria, de la Côte-d'Ivoire, du Burkina Faso et du Sénégal. Elle intervient surtout parce que le secteur est incontournable. Il n'intervient

---

[478] Cf. l'article de **LOOTS Michel**, *L'accès à l'information, un droit* fondamental, in Le courrier ACP-UE n° 201 de Novembre-décembre 2003, P. 32.

[479] Cf. l'article de **WAGNER Christophe,** *Où en sont les négociations sur les Accords de Partenariat économique entre les ACP et la CE*, in Le courrier ACP-UE n° 201 de Novembre-décembre 2003, P. 21.

qu'en lien avec d'autres domaines industriels ou vitaux. C'est ainsi que dans le cadre du Burkina Faso et de la Côte-d'Ivoire, la question de l'interconnexion des deux pays conduit à accorder un appui financier au Burkina Faso.

En ce qui concerne le Nigéria, la BEI dégage des fonds dans le cadre du programme panafricain « peste bovine », un programme de télécommunication aéronautique par satellite[480]. Ce sont donc les besoins de l'élevage qui imposent la mise en place de structures de télécommunications adéquates. Tel est le cadre dans les années 90 jusqu'à 1995.

La donne change dans les années 2000 et les accords sont d'ailleurs révisés en 2010 à Ouagadougou[481].

La Banque Européenne d'Investissements intervient surtout dans des domaines de développement et accorde surtout des prêts financiers aux petites et moyennes entreprises en Afrique de l'Ouest[482].

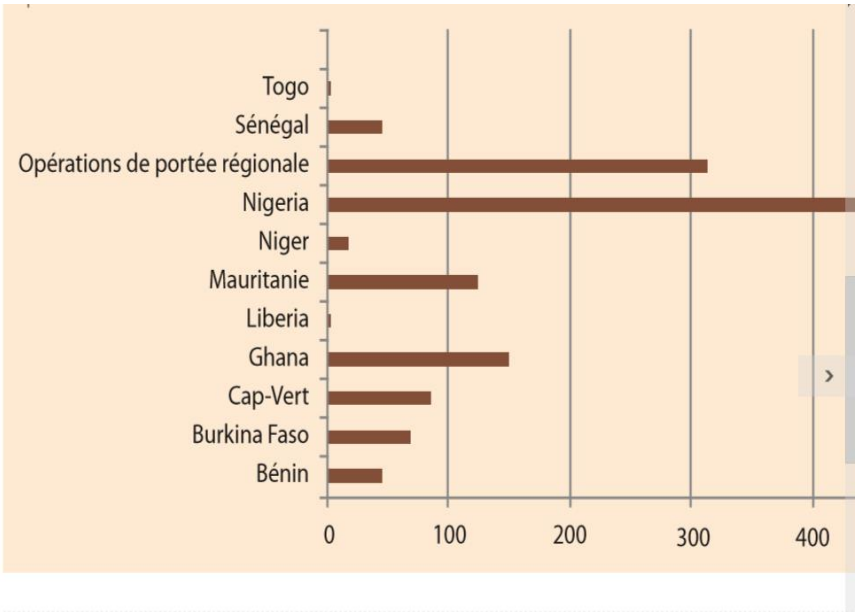
Le graphique qui suit permet de retracer l'aide de la BEI dans les Etats de l'Afrique de l'ouest de 2003 à 2012. Les secteurs d'intervention de la BEI en Afrique de l'Ouest sont essentiellement l'énergie, le secteur hydraulique et l'industrie.

---

[480] Les indications des aides de la BEI sont tirées du rapport de la Commission Européenne sur les ACP précité. Il n'est question que des années 90.

[481] Cf. Accord modifiant, pour la deuxième fois, l'accord de partenariat entre les membres du groupe des États d'Afrique, des Caraïbes et du Pacifique, d'une part, et la Communauté européenne et ses États membres, d'autre part, signé à Cotonou le 23 juin 2000 et modifié une première fois à Luxembourg le 25 juin 2005, Dossier interinstitutionnel: 2010/0114 (NLE), 9565/10, et Accord signé à Ouagadougou le 22 juin 2010 publié au JOUE L 287, 4.11.2010, p3.

[482] Cf. La Banque européenne d'investissement en Afrique de l'Ouest, Brochure de la BEI disponible en ligne : www.eib.org



Graphique extrait du rapport annuel 2012 sur l'activité de la BEI en Afrique, dans les Caraïbes et le Pacifique ainsi que dans les territoires d'outre-mer : répartition des aides par pays[483].

Dans le même but de soutien et d'appui à l'Afrique de l'Ouest, la BEI aide sur le plan financier les institutions comme la CEDEAO. C'est ce qui est repris par le Communiqué de presse de la Commission européenne du 11 décembre 2012 relatif à l'aide de la Banque européenne d'investissement[484].

L'Afrique de l'Ouest porte à son désavantage les retards dans la sanction de la cybercriminalité. Ces retards sont justifiés par les raisons technologiques et financières. Il n'en demeure pas moins qu'à compter des années 2000, des efforts sont mis en œuvre pour une mise en place de sanctions contre ce fléau sur ce continent. C'est ce qui explique la mise en place progressive de l'arsenal juridique de lutte contre la cybercriminalité.

---

[483] Pour une version en ligne, voir : http://www.eib.org/attachments/country/eib_in_west_africa_fr.pdf.

[484] Cf. Communiqué de presse BEI/12/194 du 11 décembre 2012, *Afrique de l'Ouest : la BEI accorde un prêt de 75 millions d'EUR à l'appui des réseaux d'électricité de pays en situation de post-conflit*, consultable sur : http://europa.eu/rapid/press-release_BEI-12-194_fr.htm

Section 2 : L'arsenal juridique naissant dans les Etats ouest-africains

Bien que l'internet ait commencé à se propager en Afrique dès 1992[485], l'arsenal juridique pour lutter contre les dérives numériques est à peine naissant. Ce qui conduit à parler d'une législation naissante d'un point de vue régional mais également au niveau de chacun des Etats (§1).

Le caractère récent de cette législation n'est pas lié à son absence mais bien au fait que l'ensemble des textes n'est ni communiqué ni vulgarisé auprès du public.
Et pourtant, en tant que première cible de la communication et des informations, c'est la population, qui est la première utilisatrice des réseaux de communication, comme on peut le noter à travers la circulation abondante des appareils de communication tels que le téléphone[486].

La téléphonie est plus que développée dans cette partie du monde.
Puisque la cybercriminalité touche toutes les technologies de l'information, il est convenable que les autorités en charge des ministères de la communication mènent une action coordonnée avec celles chargées des technologies de l'information et les législateurs songent à sensibiliser sur les dangers existant en matière de communication lorsqu'on a recours aux réseaux (peu importe qu'ils soient numériques ou téléphoniques).

La plupart des téléphones sont désormais équipés de technologies comme la photographie, les échanges de mails, les connexions internet à distance, alors pourquoi ne pas inciter les populations à avoir des comportements sans risque ? L'avance prise par certains Etats dans le traitement du fléau cybercriminel en Afrique doit être relevée.

---

[485] Dès 1992, l'Afrique du Sud s'est relié par son réseau interuniversitaire UNINET à celui d'ALTERNET en Virginie (USA) C'est en 1992 que l'Afrique du Sud pour activer des connexions supportant le protocole TCP/IP : Etude de l'historique d'internet en Afrique, Maison des Sciences de l'Homme d'Aquitaine, Pessac, 2003.

[486] Dans un communiqué de presse à Genève, le 26 avril 2004, l'UIT a précisé que l'Afrique, est le marché où le mobile connaît la plus forte croissance au monde. L'UIT s'est lors de cette communication interrogée sur le fait de savoir si la technologie du mobile est la clé de l'accès aux TIC en Afrique.

L'analyse de l'ensemble des législations africaines en comparaison avec celles de l'Union européenne permettra de faire la lumière sur les effets des normes édictées en vue d'une lutte efficace contre la cybercriminalité (§2).

§1- L'élaboration de la lutte contre la cybercriminalité dans les Etats Ouest-africains

Les échanges internationaux obligent le continent africain à s'aligner sur les normes internationales en matière de flux de données via les réseaux informatiques.
C'est la raison pour laquelle l'ensemble des structures mises en place pour lutter contre la cybercriminalité exigent de la part des Etats une législation adéquate. Ces exigences n'ont pas réellement de force contraignante directe sur les actes cybercriminels.

La construction normative de la lutte contre la cybercriminalité en Europe a suivi la progression technologique. Cette construction s'est alignée sur l'évolution des infrastructures de communication dont la plus récente, Internet, a généré de nouvelles manières de communiquer, de partager des informations mais aussi de consommer.

L'élaboration des normes législatives dans l'espace CEDEAO emprunte le même modèle : de 1992 à 2000 les infrastructures sont en phase de modernisation et se mettent en place peu à peu pour s'adapter aux besoins des populations[487]. Le constat est certes la lenteur de ces installations et de leur mise à jour mais l'effort fait est notable : le téléphone par exemple est plus accessible que les ordinateurs ; c'est ainsi qu'on peut voir le développement même dans des zones rurales de l'usage du téléphone comme moyen d'opérer des transactions financières. C'est le Système de *Money Bank*, de *Mpsa* au Kenya, pays précurseur en domaine. Cette pratique novatrice mérite d'être encadrée juridiquement non seulement parce qu'elle s'analyse en une nouvelle source des actes cybercriminels (il y a déjà des cas de détournements de fonds transitant via le système de money Bank).

---

[487] Cf. notamment l'article de **BOGUI J.J.**, « La cybercriminalité, menace pour le développement » Les escroqueries Internet en Côte-d'Ivoire, *Afrique contemporaine*, 2010/2 n° 234, p. 155-170.

A l'instar de ces actes, s'inscrivent les détournements de transferts de fonds de leur destination initiale. Il s'agit d'agents corrompus ou de délinquants déguisés qui enregistrent d'abord les coordonnées d'envoi ou de réception de fonds communiquées par un client destinataire, prétendent ensuite que ces coordonnées ne sont pas vérifiables ou prétextent d'une erreur dans la transmission des fonds concernés pour après les dérober. La pratique s'est plusieurs fois répétée dans des agences de transfert de fonds notamment en Côte-d'Ivoire, et les ambassades en ont été informées sans que des sanctions concrètes n'aient été prononcées.

La récente directive 06/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO de juin 2011 contient des dispositions sanctionnant les actes relevant de la cybercriminalité en Afrique de l'Ouest.

Elle vise différents domaines pour lesquels les Etats sont appelés à légiférer. Il s'agit de la technologie et des domaines des communications et des télécommunications, de la coopération judiciaire, de technologies de l'information et de la communication, de la protection des données à caractère personnel, des transactions électroniques, de l'entraide judiciaire en matière pénale et de l'extradition.

Au regard de l'ensemble de ces domaines visés par la directive CEDEAO portant lutte contre la cybercriminalité, il existe des sanctions édictées à l'encontre des délinquants.

La mise en place de l'arsenal juridique contre la cybercriminalité a été d'abord faite sur un plan régional. Certains Etats membres de la Communauté Economique ont ensuite transposé les directives et mis à jour leurs corpus législatifs. Dès lors, il serait intéressant d'analyser la construction législative régionale (A), pour mieux cerner par la suite les transpositions nationales (B).

Au niveau international, les pays africains travaillent avec l'ONU plus précisément avec la Communauté des Etats de l'Afrique en vue de réduire la

cybercriminalité[488]. Cette dimension a également un impact sur les diverses lois et fera partie intégrante des deux aspects précités.

A- La construction conventionnelle et législative dans les secteurs de transmission

Il nous faut distinguer les données à caractère personnel des autres secteurs de transmission comme les activités liées aux télécommunications, puisqu'ils sont des vecteurs facilitant la commission des actes relatifs à la cybercriminalité.

Aussi bien pour la protection des données à caractère personnel que pour le secteur des télécommunications, l'élaboration des textes en Afrique en général et en particulier en Afrique de l'Ouest est d'abord conventionnelle. Elle implique, pour des raisons d'efficacité, la mutualisation des efforts[489] des Etats à travers la signature de conventions entre eux. La politique de la lutte est donc sous-régionale.

Par la suite, les Etats transposent les textes dans leur ordre juridique interne pour les appliquer.

L'étude des différents textes élaborés dans le cadre de la lutte contre la cybercriminalité fait ressortir deux catégories de mesures. Les premières concernent le secteur de la télécommunication et les secondes sont propres à la cybercriminalité.

Au regard de la chronologie des différents textes adoptés, il y a une superposition des textes conventionnels et règlementaires, compte tenu de la diversité des acteurs en cause (Union Africaine, OIF, CEDEAO, UEMOA)[490].

Compte tenu de ces superpositions qui mêlent les échanges conventionnels aux normes nationales ou sous-régionales, il semble évident de procéder à une analyse des textes par institution. Il ressort de cette approche que l'UEMOA s'est concentrée sur la

---

[488] http://repository.uneca.org/codist/

[489] Pris individuellement, les Etats africains notamment seraient incapables de réussir efficacement la lutte contre les fraudes technologiques.

[490] Ce sont ces institutions qui sont concernées par la lutte contre la cybercriminalité en Afrique de l'Ouest.

régulation du secteur des télécommunications alors que la CEDEAO est intervenue aussi bien sur les problématiques des télécommunications que celles relatives à la cybercriminalité.

a- Dans l'espace UEMOA

Le Traité de l'UEMOA date du 10 janvier 1994 et a été modifié le 29 janvier 2003. Cet espace comprend à la fois des Etats francophones et des Etats anglophones.

Plusieurs actes ont été pris avec la particularité d'un règlement pris pour les systèmes de paiements et de six directives édictées dans le cadre des télécommunications.

Pourquoi ces normes sont-elles en rapport avec la cybercriminalité ?

Concernant les systèmes de paiements, les normes les encadrant sont en lien direct avec la cybercriminalité dans la mesure où cet ensemble d'infractions est surtout d'ordre financier (fraudes aux cartes bancaires, interceptions frauduleuses des données bancaires par exemple ou escroqueries en ligne).

En effet, c'est le Règlement 15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement, qui régit le système de paiements dans l'ensemble des pays membres de l'UEMOA. Il prévoit par exemple un dispositif de sécurité des paiements grâce à la technique de la signature électronique[491].

---

[491] Cf. article 23 du règlement : « *Un dispositif de création de signature électronique ne peut être considéré comme sécurisé que s'il satisfait aux exigences définies à l'alinéa 2 ci-après et s'il est certifié conforme à ces exigences dans les conditions prévues par l'alinéa 3 ci-dessous. Un dispositif sécurisé de création de signature électronique : doit garantir, par des moyens techniques et des procédures appropriés, que les données de création de signature électronique ne peuvent être : établies plus d'une fois et que leur confidentialité est assurée ; trouvées par déduction et que la signature électronique est protégée contre toute falsification ; protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers ; ne doit entraîner aucune modification du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer. Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies à l'alinéa 1 par des organismes agréés par la Banque Centrale et selon des règles définies par instruction prise à cet effet par elle. La*

S'agissant des télécommunications, sont prévues dans l'espace UEMOA, des dispositions encadrant l'interconnexion, les autorités de régulation des télécommunications et l'harmonisation des politiques de contrôle et de régulation du secteur des télécommunications. Les Etats membres de l'UEMOA ont donc établi six directives à ce propos. Il s'agit de :

- La directive 01/2006/CM/UEMOA relative à l'harmonisation des politiques de contrôle et de régulation du secteur des télécommunications :
- La directive n°02/2006/CM/UEMOA relative à l'harmonisation des régimes applicables aux opérateurs de réseaux et fournisseurs de services
- La directive n°03/2006/CM/UEMOA relative à l'interconnexion des réseaux et services de télécommunications
- La directive n°04/2006/CM/UEMOA relative au service universel et aux obligations de performance du réseau
- La directive n°05/2006/CM/UEMOA relative à l'harmonisation de la tarification des services de télécommunications
- La directive n°06/2006/CM/UEMOA organisant le cadre général de coopération entre les autorités nationales de régularisation en matière de télécommunications.

Il ressort de ces normes que la question de la cybercriminalité n'est pas clairement traitée par les dirigeants de l'UEMOA, en 2006.

C'est au sein de la CEDEAO que les préoccupations de la délinquance contre la haute technologie vont être prises en compte par les dirigeants ouest-africains.

b- Au niveau de la CEDEAO

La CEDEAO procède de manière chronologique dans la mise en place de la règlementation concernant la lutte contre la délinquance numérique et électronique.

---

délivrance d'un certificat de conformité est publiée dans un journal habilité à recevoir des annonces légales ou selon les modalités fixées par instruction de la Banque Centrale ».

Le premier secteur à bénéficier de cet encadrement est celui des télécommunications.

Cet encadrement normatif est initié dès 1994 avec la décision A/DEC. 11/12/94 relative à la création d'un Comité Technique Consultatif sur la règlementation en matière de communications. C'est la première étape du processus normatif.

La seconde étape date de 2005 avec la Décision A/DEC.14/01/2005 relative à l'adoption d'une politique régionale des télécommunications et du développement du Roaming Global System for Mobile (GSM) dans les pays membres.

A la suite de cette seconde étape, la CEDEAO a recours à plusieurs actes additionnels au Traité CEDEAO pour concrétiser la règlementation des télécommunications dans l'espace communautaire. Il s'agit de :

- L'acte additionnel A/SA.1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre règlementaire des secteurs des TIC
- L'acte additionnel A/SA.2/01/07 du 19 janvier 2007 relatif à l'accès et à l'interconnexion des réseaux et services du secteur des TIC
- L'acte additionnel A/SA.3/01/07 du 19 janvier 2007 relatif au régime juridique applicable aux opérateurs et fournisseurs de services
- L'acte additionnel A/SA.4/01/07 du 19 janvier 2007 relatif à la gestion du plan de numérotation
- L'acte additionnel A/SA.5/01/07 du 19 janvier 2007 relatif à la gestion du spectre de fréquences radioélectriques
- L'acte additionnel A/SA.6/01/07 du 19 janvier 2007 relatif à l'accès universel/service universel.

Tous ces actes ont vocation à encadrer les secteurs des technologies et des communications. Sont concernés aussi bien le cadre règlementaire des outils et moyens de communication que les acteurs qui interviennent pour les faire fonctionner et les contrôler.

Après avoir régulé le cadre des télécommunications, la CEDEAO prévoit des dispositions pour encadrer les données qui circulent via les réseaux électroniques et

numériques. L'acte additionnel (au Traité CEDEAO) A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel est signé par les autorités de la sous-région.

La CEDEAO aborde ainsi de manière explicite les questions relatives à la protection des données à caractère personnel.

Cet article dispose à ce sujet que : « le présent Acte additionnel entre en vigueur dès sa publication dans le Journal officiel de la Communauté et dans ceux de chaque Etat membre. Le présent Acte additionnel est annexé au Traité de la CEDEAO dont il est partie intégrante ».

La directive CEDEAO vise à protéger particulièrement les données à caractère personnel tant dans leur confidentialité que dans leur intégrité.

Concernant la confidentialité, elle est protégée par l'article 8 de la directive. Selon les dispositions de cet article 8, « *le fait pour toute personne d'intercepter, de tenter d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique, à destination, en provenance ou à l'intérieur d'un système informatique constitue une infraction au sens de la Directive du 19 août 2011* ». La précision de transmission non publique dans la disposition précise l'origine des données concernées et en détermine le régime juridique applicable. Il s'agit à la lecture de cette précision de données transmises dans un cadre privée. C'est de la sorte la garantie du secret des données électroniques à l'instar des correspondances[492].

Quant à l'article 9 de la directive, il précise que la modification frauduleuse des données informatiques constitue une infraction. Il traite ainsi de l'intégrité des données et il vise plusieurs actions à savoir l'endommagement, l'effacement, la détérioration, l'altération et la modification frauduleuse. Il semble à la lecture de l'article que le législateur africain a aligné des synonymes mais il n'en est rien. En effet, *endommager* la donnée informatique revient à la mettre en mauvais état, l'*effacer* c'est la faire disparaître. Quant à *altére*r la

[492] **P. A. TOURE**, « *la cybercriminalité dans les législations communautaires intégrées en Afrique* », support de formation à l'ERSUMA, formation des magistrats, des avocats et des officiers de l'Interpol, 02 au 05 septembre 2013, Bénin.

donnée, il s'agit de la fausser, en changer la nature, la modifier en mal et enfin quand il parle de modifier la donnée informatique, le législateur de la CEDEAO vise le fait de la transformer sans altérer sa nature.

Il faut noter que les incriminations de ces actes sont sanctionnées concrètement par les Etats membres de la CEDEAO, la directive ayant laissé cette tâche aux autorités nationales de déterminer les peines principales. C'est l'article 28 de la directive qui traite de ce point avec la précision que les sanctions doivent être « *dissuasives et proportionnées* ».

Au titre des peines complémentaires, la directive CEDEAO prévoit en son article 29 des sanctions complémentaires à la condamnation : il s'agit de la confiscation des matériels, des équipements, des instruments, des programmes informatiques ou des données ainsi que des sommes ou produits résultant de l'infraction et appartenant au condamné.

Si la CEDEAO procède par adjonction d'actes additionnels au Traité CEDEAO pour le cadre normatif du secteur des télécommunications, quelles sont les contributions de l'Union africaine et de l'Organisation Internationale de la francophonie dans ces domaines ?

c- Les contributions de l'Union Africaine et de l'Organisation Internationale de la Francophonie

Au cours du Xe sommet de la francophonie en 2004 à Ouagadougou au Burkina Faso, les chefs d'Etats déclarent leur attachement à la protection des données. La troisième étape est ainsi franchie.

Depuis 2007, une Autorité régionale des Données Personnelles a été créée et elle a une dimension plus étendue qu'en Afrique. Il s'agit d'une autorité francophone internationale. Elle organise régulièrement des rencontres et facilite ainsi des échanges d'expériences au niveau de la protection des données entre les différentes autorités qui y ont adhéré.

Si le processus de mise en place de dispositif de la protection des données à caractère personnel par la CEDEAO paraît long et récent, certains Etats ont envisagé la démarche avant l'adoption définitive d'une législation commune. C'est ainsi que certains

d'entre eux disposent avant 2010 de lois protégeant les données à caractère personnel au niveau national.

d- Au niveau des Etats

Il faut envisager ici l'encadrement juridique des données à caractère personnel et le secteur des télécommunications.

1. Les données à caractère personnel

Au niveau des lois, les pays comme le Burkina Faso se sont dotés de législations protégeant les données personnelles. Depuis 2004, cet Etat a légiféré et possède une loi n° 010-2004 du 20 avril 2004 relative à la protection des données personnelles[493].

La Côte-d'Ivoire possède quant à elle, un texte de loi de 2004, encadrant les données échangées dans le cadre des investissements en Côte-d'Ivoire : la Loi n 2004-429 du 30 août 2004 instituant le régime de la zone franche de la biotechnologie et des technologies de l'information et de la communication en Côte d'Ivoire. Ce texte de loi hybride[494] traite de manière partielle de l'encadrement des données. Il faut attendre 2013 pour que le texte spécifique à la protection des données soit élaboré. C'est la loi du 19 juin 2013. Elle clarifie la situation et témoigne d'une meilleure appréciation et approche de la protection des données à caractère personnel d'une part et le cadre des données biotechnologiques d'autre part, en Côte-d'Ivoire. Il faut souligner qu'avant 2013, l'Etat ivoirien traite sous la même loi de protection, les biotechnologies et les technologies de l'information et de la communication. Cela peut paraître étonnant dans la mesure où les premières relèvent du domaine de la santé et les secondes de la communication d'une manière générale. A l'inverse, cette adjonction des deux technologies relèvent de la recherche, on peut dès lors concevoir de les protéger par un texte unique. Cette précision peut se révéler particulièrement intéressante puisqu'elle permet de faire la jonction entre

[493] Cf. loi n° 010-2004 du 20 avril 2004 relative à la protection des données personnelles publiée au Journal Officiel du Burkina Faso du 24 juin 2004.

[494] Loi instituant le régime de la zone franche de la biotechnologie et des technologies de l'information et de la communication en Côte-d'Ivoire publiée au Journal officiel de la République de Côte-d'Ivoire du 23

la protection des données personnelles en générale et celle des données médicales en particulier. Le texte de 2004, précisions-le, était un embryon dans la mesure où depuis 2013, le texte a évolué et s'est spécifié. C'est la loi n° 2013-450 du 19 juin 2013 sur la protection des données à caractère personnel qui permet de souligner l'évolution ivoirienne en matière d'encadrement de la protection des données à caractère personnel.[495] L'amateurisme en matière de gestion de l'outil informatique dans les différents secteurs d'activité pourrait d'ailleurs être une justification au texte de 2004.

La loi de 2013 quant à elle permet de mieux cerner les problématiques propres à la protection des données à caractère personnel.

Outre cet aspect de l'unicité de la protection des données personnelles prises globalement et les données spécifiques de la biotechnologie, il faut souligner la création dans ce même pays (en Côte-d'Ivoire) d'un village des technologies et de la biotechnologie : il est dénommé VITIB.

VITIB est une zone franche dédiée aux opportunités d'investissements en Côte-d'Ivoire. C'est une expérimentation dont le bilan n'a pas encore été fait. Ce n'est que récemment que les serveurs de cette plateforme ivoirienne réservée aux technologies de l'information ont été transférés en Côte-d'Ivoire, le lieu de l'implantation actuel de la plateforme. Cela paraissait en effet curieux que les serveurs se situent en Amérique spécifiquement aux Etats-Unis. L'explication est simple : c'est dans ces terres que les concepteurs ont décidé de ladite structure. Quel est le succès de cette zone franche spécifique localisée à Grand-Bassam, une ville à quelques minutes de la capitale économique ? Pourquoi créer cette zone et ne pas étendre des fonctions ou spécificités à l'ensemble des zones urbaines, puis du pays et enfin à la sous-région ouest - africaine ? Des difficultés d'accès à ce village, l'absence de bilan de VITIB, l'accès même au village poserait problème. D'ailleurs,

---

décembre 2004, p 946 - 950. La loi est par la suite scindée pour avoir une législation propre et spécifique aux données à caractère personnel uniquement en 2013.

[495] Loi n° 2013-450 du 19 juin 2013sur la protection des données à caractère personnel publiée au Journal Officiel de la République de Côte-d'Ivoire du 08 Août 2013.

VITIB aurait pu être une sorte de SILICON VALLEY[496], espace dédié aux entreprises de protection des infrastructures informatiques, ou même des données des personnes d'une manière générale.

Au Sénégal c'est grâce à la loi n°2008-12 du 25 janvier 2008[497] que la protection des données à caractère personnel est assurée. En ce qui concerne le Sénégal, la mise en place d'une commission de protection des données ne s'est faite que depuis peu avec le décret du 29 juin 2011 instituant les membres de ladite commission[498].

Le Ghana a quant à lui adopté une loi sur la protection des données à caractère personnel appelé Data Protection Act en 2010[499].

La réelle difficulté pour protéger les données dans ces Etats Africains doit être mentionnée au titre des blocages : il s'agit notamment de difficulté de collecte des informations, qui sont pour la plupart encore sous le format papier. Au sein même de l'administration, très peu de services sont équipés de technologies simples (en Europe par exemple) comme la numérisation. L'informatique n'est pas encore réellement intégrée[500] dans les habitudes en comparaison et au contraire des Etats européens. C'est le lieu de

---

[496] SILICON VALLEY, ou vallée du Silicium, du nom de la matière composant les semi-conducteurs, à l'origine de la création du pôle industrialisé et composé de plusieurs entreprises technologiques, inspiration de William Shockley. Il est situé en Californie aux Etats-Unis d'Amérique et date de 1956 grâce à la décision de, cf. **Timothy BRESNAHAN and Alfonso GAMBARDELLA,** Building High-Tech Clusters, Silicon Valley and Beyond, Cambridge University Press, UK, 2004 ; **T. WEIL**, Why and How European Companies reach out to Silicon Valley, Les notes de l'Institut Français des Relations Internationales (IFRI), n° 25, Paris 2000 ; **F. SACHWALD,** The New American Challenge and Transatlantic Technology Sourcing, Les notes de l'Institut Français des Relations Internationales (IFRI), n° 24, Paris 2000 ; **Robert D. COOTER and Hans-Bernd SCHÄFER**, Solomon's Knot, How Law can end the poverty of nations, Princeton University Press, United Kingdom, 2012.

[497] Loi 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel, publiée au Journal Officiel du Sénégal n° 6406 du Samedi 3 mai 2008**.**

[498] Décret n° 2011-929 du 29 juin 2011 portant nomination des membres de la Commission de protection des données personnelles, http://www.demarches.gouv.sn/ressource.php?id_esp=1&th=&ss_th=&id_actu=1271

[499]Cf. Data Protection Act, 2010**,** disponible sur le site du Parlement Ghanéen : http://www.parliament.gh/library.php?id=36.

[500] En Europe, il y a certains automatismes dans l'usage des technologies de l'information et de la communication au sein des administrations. Ces automatismes ne sont pas systématiques dans les administrations africaines. L'utilisation traditionnelle des documents sous la forme papier est encore de mise.

mentionner que le meilleur témoignage est fait par les entreprises de veilles stratégiques ou juridiques qui, lorsqu'elles sont consultées pour opérer des recherches de solvabilité pour le compte de leurs clients se retrouvent à procéder en amont à des collectes essayant de se conformer aux lois en vigueur.

Pour un aspect concret de la chose et un recul pratique, il nous a été permis d'interroger certains praticiens qui nous ont donné leurs vécus professionnels.
Dans ce cadre, nous avons interviewé un professionnel de la collecte des informations pour le entreprises privées et publiques en Côte-d'Ivoire. Cet échange a été l'occasion de prendre la question de la collecte des informations sous un aspect nouveau.

En effet, les informations en Afrique en général et en Côte-d'Ivoire en particulier sont encore sous le joug du secret, de la confidentialité notamment quant à leur communication et leur diffusion. Or, plus les informations sont diffusées, plus les personnes concernées en sortent gagnantes. C'est au niveau du traitement qui en est fait qu'il faut se rendre compte que les outils légaux et les processus (procédures) existent. Le cadre légal est également existant, c'est la pratique qui n'en fait pas encore cas et le fait que la plupart des administrations ne soient même pas encore passées aux automatismes comme la numérisation ne facilite pas la recherche des informations. Ce n'est pas tant la législation qui manque. C'est l'aspect de contrôle de l'informaticien par exemple qui détient et utilise les codes de connexion aux interfaces. Il est ressorti des retours d'expériences qu'il n'y a aucun contrôle des connexions, du respect de la confidentialité de la part de ces informaticiens ou des gestionnaires de plateformes. Et ce constat est général dans la mesure où il concerne aussi bien les entreprises privées que le secteur public. En d'autres termes, les failles des systèmes ne sont toujours occasionnées uniquement par des personnes extérieures mais peuvent avoir pour source des ressources internes même aux structures qu'elles soient publiques ou privées.

A la suite de la Côte d'ivoire, et du Sénégal, le Bénin fait partie des Etats dont la législation sur la protection des données existe. C'est par la loi du 22 mai 2009[501] que la

[501] Loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin :

République du Bénin entend protéger les données personnelles des individus. D'ailleurs cet Etat dispose d'une Commission Nationale de l'Informatique et des Libertés dont le site internet est malgré tout, difficilement consultable[502].

En observant les dates de ces textes, ils sont très jeunes comparés à ceux des Etats de l'Union Européenne qui eux, sont vieux de presqu'une quarantaine d'années (par exemple certains datent de 1973 comme pour la Suède et d'autres comme celui de la France de 1978).

Cette récente législation est surtout due à l'ensemble des échanges internationaux entretenus avec d'autres Etats avec le continent africain. En effet, ces échanges supposent des transferts de données. Or, du fait de la montée du phénomène cybercriminel surtout en provenance des pays africains, la méfiance s'installe dans le monde des affaires du côté des entreprises et même des investisseurs européens ou d'autres continents. Dès lors, il se trouve que la mise à jour des différents systèmes juridiques africains, est une urgence exigée pour la bonne marche des affaires. La sécurité juridique étant un gage de sérénité, les Etats africains en général et ceux de l'Afrique de l'ouest en particulier ont joué le jeu coopératif avec leurs partenaires, fournisseurs ou clients européens. C'est d'ailleurs dans ce cadre que s'inscrit la réunion organisée par l'association francophone des autorités de protection des données personnelles[503]. Cette rencontre témoigne de la coopération des Etats surtout dans l'objectif d'une lutte efficace. De la sorte, il devient plus aisé de coordonner les sanctions contenues dans les différentes lois.

Dans les textes de protection des données à caractère personnel, quelles sanctions sont édictées en vue d'assurer une protection efficace ? Comparons ces sanctions entre Etats anglophones et francophones.

Quelles sanctions assurent la protection des données à caractère personnel ?

---

http://www.atrpt.bj/textedereference/telecom/loi/LOI_2009_09_PROTECTION_DES_DONNEES_PERSONNELLES.pdf

[502] Le site officiel de la CNIL au bénin est : http://www.cnilbenin.bj/.

[503] http://www.ambafrance-sn.org, rencontre tenue le 19 et 20 septembre 2011.

Dans la loi ivoirienne par exemple, l'article 22 de la loi du 08 Août 2013 dispose que « *est interdite et punie d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 10.000.000 francs CFA, la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telle prospection.* »

En plus des pratiques de « *broutage* » en Côte- d'Ivoire notamment, d'autres infractions contre les personnes sont commises : il s'agit des crimes ou de meurtres. La recherche de gain facile pousse certaines personnes à commettre des homicides volontaires qu'elles justifient par des considérations d'ordre mystique .En effet, l'exemple d'un jeune homme de 18 ans, qui, reconnu comme brouteur, tue un jeune enfant de 5 ans dont il était proche, sur les conseils d'un marabout (ou charlatan). Cette pratique était déjà le fait de pirates informatiques nigérians dans l'idée de sacrifice humain afin de toucher des trésors à la suite d'arnaques informatiques en direction d'Etats européens[504].

Sous quel régime peut-on classer ce type de dérive ? Comment les sanctionner ?

Il ne s'agit pas d'un homicide classique encore moins d'un meurtre simple. Il se trouve être en lien avec des fraudes informatiques effectuées de manière répétée avec des conséquences considérables. Il faudra créer une infraction spécifique pour ce type d'homicide compte tenu des circonstances. A moins que ces circonstances ne soient analysées en facteur aggravant la peine initialement encourue pour les homicides classiques.

Si dans l'ensemble des Etats francophones (du Bénin, du Burkina Faso, du Cap-Vert, de la Côte-d'Ivoire, de la Guinée, de la Guinée Bissau, du Niger, du Mali, du Sénégal, du Tchad, du Togo (y compris ceux qui n'ont pas spécifiquement des textes protégeant les données à caractère personnel) des sanctions sont édictées, ces sanctions relèvent soit des peines privatives de libertés soit des sanctions administratives ou encore des sanctions pécuniaires.

---

[504] www.abidjan.net, site d'informations en ligne en provenance d'Abidjan, en Côte-d'Ivoire.

Il convient de les classer en peine principale, complémentaire ou en mesure de sûreté. Mais avant tout, la sévérité des peines est à noter. A titre illustratif, certaines amendes au Sénégal vont de un million à cent millions (100 000 000) de F CFA. Cette somme n'est pas négligeable même s'il s'agit d'une personne morale qui doit la payer à titre de sanction pécuniaire pour n'avoir pas respecté certaines dispositions légales.
Au titre des peines principales, elles sont relatives de manière générale à la peine privative de liberté c'est-à-dire à l'emprisonnement.

Au Bénin, la loi de protection des données personnelles[505] prévoit une peine qui varie entre cinq et dix ans en fonction de la gravité du manquement pour lequel elle a été prononcée.

Au Nigéria, dès 2008, l'agence de protection des données est créée grâce à la loi instituant l'agence de la cyber-sécurité et de la protection des données en 2008: "cyber Security and Data Protection Agency (Establishment) Bill".

Les données personnelles n'étant pas l'unique terrain de chasse des cybercriminels, d'autres textes pourraient contenir des sanctions quant à la commission d'infractions de nature cybercriminelle. C'est le cas du secteur des télécommunications.

2. La régulation du secteur des télécommunications

Pour aboutir à une législation en phase avec les normes internationales, les Etats de l'espace économique ouest africain ont opté pour une réforme du secteur des télécommunications. Cette entreprise est louable et compréhensible dans la mesure où les textes législatifs de ce domaine sont obsolètes (dans la mesure où ils datent des années 90) et inadaptés aux évolutions technologiques sans cesse grandissantes. D'un autre point de vue, ce secteur est l'un des piliers en matière de cybercriminalité puisqu'il allie les technologies de l'information et de la communication à la consommation des populations urbaine et rurale.

[505] Cf. la loi n°2009-09 du 27 avril 2009 de protection des données personnelles

C'est dans ce cadre que l'Agence des Télécommunications de Côte-d'Ivoire (ATCI) a demandé à l'Etat ivoirien de se doter d'un cadre juridique et règlementaire à travers la prise de décrets sur l'identification des abonnés de téléphones mobiles et des usagers des cybercafés. Cette requête ayant pour but selon l'organisme de lutter efficacement contre le fléau de délinquance informatique[506]. Il est certain que ce genre de recommandation n'a réellement d'ampleur que lorsqu'elle est accompagnée de sanctions de la part des autorités régulatrice. Ainsi, même si la recommandation a pour objectif de motiver les abonnés des services de télécommunication à se faire identifier, le fait qu'il y ait une sanction en cas de non identification met une obligation de le faire. D'ailleurs, la pratique le démontre régulièrement. Refuser de procéder à son identification ne donne pas accès à un numéro de téléphone (mobile) et donc conduit à un refus d'accès au réseau. Cet appel de l'Agence des Télécommunications en Côte-d'Ivoire peut s'analyser en un stade embryonnaire de prise de conscience quant au fléau cybercriminel au niveau africain. Il en découle le caractère encore théorique des solutions africaines.

La théorie tend tout de même à s'estomper puisque les Etats mettent en place leurs législations.

D'une manière concrète, les Etats membres de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) ont décidé d'aligner sur les normes internationales, leurs textes relatifs aux secteurs des télécommunications.

α.Le Bénin

Plusieurs textes et décisions encadrent le secteur béninois des télécommunications. Par exemple, l'Ordonnance n°2002-002 du 31 janvier 2002 portant principes fondamentaux du régime des télécommunications en République du Bénin[507], le décret N°2008-507 du 08 septembre 2008 portant conditions d'acceptation et d'attribution des autorisations, des permis et des déclarations préalables pour l'exploitation des réseaux ou services des télécommunications en République du Bénin et

506 http://www.balancingact-africa.com/news/fr/editiion-en-fran-ais/136/infos-internetweb/c-te-divoire-lutte-c/fr

507 Ordonnance n°2002-002 du 31 janvier 2002 portant principes fondamentaux du régime des télécommunications en République du Bénin.

des décisions rendues par l'Autorité Transitoire de Régulation des Postes et Télécommunications (ATRPT) en République du Bénin instituée par le décret n° 2007-209 du 10 mai 2007[508].

Ces dispositions sont importantes dans la mesure où en plus d'encadrer les réseaux et les services de communications dans les attributions, elles contribuent à déterminer els degrés de responsabilités notamment des fournisseurs et des prestataires de service en cas de conflits ou de non-respect des obligations assorties aux différentes fournitures de services et prestations.

Une autre réalité en matière de sanctions contre la cybercriminalité en Afrique est l'insuffisance des actes législatifs existants. En soi, ce n'est pas que ces actes législatifs n'existent pas. Ils sont rédigés mais la pratique fait défaut dans la mesure où les décrets d'application sont pris trop tard au regard de la date de rédaction du texte de loi. Par conséquent, il semble impossible que ces décrets d'application soient pris un jour. Pour illustration, la loi béninoise sur la libéralisation du secteur des télécommunications a été votée en juillet 2002. Il a fallu attendre 2008 pour qu'un décret d'application de ce texte soit pris[509].

En effet, des cybercriminels appréhendés en Côte-d'Ivoire du fait de leurs malversations se sont vus relâchés « le juge ayant estimé que le cadre légal ne permettait pas de les condamner : motivation, le code pénal s'agissant des actes similaires ne prévoyait qu'une destruction des biens matériels, or en l'espèce, il y avait eu détournement de plusieurs fonds[510]». Il est dommage que le texte n'ait pas été complet. Toutefois, il se pose la question des preuves rapportées si le texte avait effectivement tout prévu.

La législation est en construction et les faits sus-relatés se sont déroulés en 2009.

En 2012, les autorités ivoiriennes avaient précisé que le code pénal ivoirien,

---

[508] Le décret n° 2007-209 du 10 mai 2007 portant création de l'autorité de de Régulation des Postes et Télécommunications (ATRPT) en République du Bénin, cf. site du gouvernement du Bénin.

[509] Voir le Rapport sur le cadre législatif des TIC au Bénin, *Cadre réglementaire et institutionnel pour le développement des technologies de l'information et de la communication au Bénin*, étude réalisée dans le cadre du programme de recherche « e-stratégie du Bénin » financé par le centre de recherches pour le développement international (CRDI) daté du 02 septembre 2010.

[510] Faits relevés par le directeur de l'Agence des Télécommunications en Côte-d'Ivoire au cours d'une conférence de presse : http://www.nordsudmedia.info et http://www.nordsudmedia.info

principalement l'article 403 serait étoffé pour se voir adjoindre des dispositions spécifiques à la cybercriminalité. En 2015, les dispositions complémentaires n'ont pas encore été rajoutées pour préciser les règles pénales.

Qu'en est-il du Ghana ?

β.Le Ghana

Pour mettre fin aux pratiques frauduleuses, le gouvernement ghanéen en général et le ministère de la communication en particulier a envisagé de reformer la législation des télécommunications en 2008. C'est dans ce cadre que ce ministère a mis en place une séance de travail avec pour thème « ICT4AD- création d'un environnement adapté-Cybercriminalité et les lois du Ghana »[511]. Le processus d'élaboration des lois en matière de cybercriminalité est encore en projet.

En parallèle, des entreprises privées étrangères signent des partenariats avec l'Etat ghanéen afin d'améliorer sa connectivité et ses moyens de communication mobiles. C'est le cas de HUAWEI, entreprise chinoise qui a pris l'initiative de la mise en place d'une plateforme dédiée au gouvernement ghanéen, appelée *e-gouvernement*[512].

D'autres Etats comme le Sénégal élaborent des réformes au niveau des règles relatives au secteur des télécommunications.

c. Le Sénégal

S'agissant du Sénégal, le chef de l'Etat et le gouvernement ont adopté le 17 décembre 2010, le projet de loi visant à s'aligner aux normes des directives de l'UEMOA et de la CEDEAO, relatives aux télécommunications.

A titre d'illustration, la Côte-d'Ivoire et le Sénégal ont mis en place des projets de loi adoptant la directive, de manière à être en phase avec l'harmonisation ouest africaine des législations amorcée.

Outre ces deux Etats, d'autres comme le Niger ont entamé dans la foulée des réformes

[511] La version originale est "Creating the enabling environment – Cyber crimes and the laws of Ghana ».

[512] Cf. **LEMARCHAND H**. et **LOUIS-SIDNEY B**., Cybersécurité des pays émergents, Livre blanc, les notes stratégiques, Compagnie Européenne d'Intelligence Stratégique.

dans le secteur des Télécoms également. C'est ainsi que plusieurs textes en vue de combler le vide juridique en la matière ont été adoptés. Il en va ainsi du projet d'ordonnance modifiant et complétant l'ordonnance n° 99-045 du 26 octobre 1999, portant réglementation des Télécommunications, adopté le 16 décembre 2010[513].

Le secteur des télécommunications et de la protection des données à caractère personnel sont par rapport à la cybercriminalité des vecteurs de transmission. Ils sont donc régis par des règles propres et distinctes de la cybercriminalité. La cybercriminalité, est, elle-même un domaine spécifique et particulier qui appelle un corpus législatif distinct des composantes de la communication et des données.

B- L'adoption des lois relatives à la cybercriminalité

L'initiative de l'élaboration des textes encadrant la répression de la cybercriminalité est clairement exprimée lors de la Conférence extraordinaire de l'Union Africaine des Ministres en charge de la Communication et des Technologies de l'Information à Johannesburg le 05 novembre 2009. L'expression de cette volonté de lutter contre la cybercriminalité a évolué grâce à plusieurs déclarations[514] que sont la Déclaration d'Abidjan du 22 février 2012, la Déclaration d'Addis-Abeba du 22 juin 2012 adoptant le projet de loi sur l'harmonisation des cyber-législations en Afrique et la déclaration de Khartoum AU/CITMC-4/MIN/Décl.(IV) du 06 septembre 2012.

La mise en œuvre de ces différentes déclarations a permis d'appréhender la répression de la cybercriminalité sous la forme d'une Convention sur la cyber-sécurité dont le projet UA-01/09/2012 sur la cyber-sécurité en Afrique est la première version. Le projet contient plusieurs objectifs dont les principaux sont *l'élaboration d'une politique d'adaptation des incriminations nouvelles spécifiques aux technologies de l'Information et de la Communication, la mise en place des sanctions et l'adaptation du régime de*

---

[513] Cf. http://www.balancingact-africa.com/news/fr/edition-en-fran-ais/149/infos-telecoms/niger-d-but-de-r-for/fr

[514] Les différentes déclarations sont consultables sur le site de l'Autorité Francophone des Données Personnelles

responsabilité pénale en vigueur. Ce projet de Convention est en phase de ratification depuis 2014. Et la Commission européenne a participé activement à cette élaboration grâce à son partenariat avec l'Union Internationale des Télécommunications. D'ailleurs, cette aide s'insère dans le cadre de la coopération UE-ACP[515].

En effet, les chefs d'Etats et de gouvernement de l'Union africaine ont adopté la Convention de l'Union Africaine sur la cyber-sécurité et la protection des données à caractère personnel, lors de la réunion des 26 et 27 juin 2014 à Malabo en Guinée équatoriale. Concernant la répression de la cybercriminalité, la Convention contient des dispositions relatives au droit pénal procédural, au droit substantiel et a pour objectif principal diverses adaptations grâce à la modernisation des instruments de répression. L'initiative de l'Union Africaine se poursuit dans les diverses autres institutions et organismes économiques africains. Les Etats eux-mêmes se mettent à jour dans ce sens.

C'est pourquoi il est important de savoir dans quelles conditions sont adoptées les lois sur la cybercriminalité au plan régional (a) et au niveau des Etats (b).

a- L'approche régionale

La cybercriminalité est un facteur perturbateur des zones économiques prises dans leur ensemble. C'est en cela que la Communauté des états de l'Afrique de l'Ouest (CEDEAO), espace non seulement à portée économique mais également politique s'est engagée à lutter sérieusement contre ce fléau. Certains Etats ouest-africains, comme le Nigéria ou encore la Côte-d'Ivoire sont estampillés comme des réseaux cybercriminels.

Face à cette alerte, qui a pris une dimension mondiale, le premier sommet ouest-africain sur la cybercriminalité s'est tenu du 30 novembre au 02 décembre 2011 à Abuja au Nigéria et traitait de la lutte contre la cybercriminalité relativement à son impact

[515] Cf. L'UIT consolide l'alliance mondiale contre les cybermenaces in *ITU NEWS, Cybersécurité*, n° 2, 2014.

économique sur la région ouest-africaine[516]. Il est organisé par la Commission des crimes financiers et économique (du Nigéria), de l'Organisation des Nations Unies en charge de la lutte contre la Drogue et les crimes (en anglais United Nations office on Drugs and Crime UNODC) et la CEDEAO en collaboration avec Microsoft.

Ces échanges[517]traitant de la question des sanctions contre les comportements répréhensibles des cybercriminels. Or, ces échanges ne sont pas rapidement concrétisés dans la mesure où il y a, à ce jour, très peu d'Etats ouest-africains qui répriment réellement les actes cybercriminels. La plupart du temps, c'est à partir de ces Etats que les criminels commettent les infractions. Et ils ne sont pas sanctionnés compte tenu des difficultés pour les appréhender.

Dans les faits, il n'est pas aisé pour les autorités de police judiciaire sur place, d'arrêter les délinquants ; les actes cybercriminels (notamment hacking, usurpation de données ou fraudes informatiques ou encore spamming) sont effectués dans des cyber-cafés, des espaces qui, jusqu'en 2011 n'étaient ni encadrés encore moins contrôlés. Il devient dès lors difficile d'apprécier un éventuel impact des sommets organisés en vue de lutter contre la cybercriminalité.

Ce sommet a permis certes de soulever les difficultés liées à la lutte contre la cybercriminalité en Afrique, mais il a également été l'occasion de soumettre l'idée d'une coopération multilatérale. Cette idée est non négligeable dans la mesure où l'infraction cybercriminelle prise dans sa globalité touche plusieurs territoires à la fois : elle n'a généralement aucune frontière. Or, édicter des textes, des sanctions et même prendre des mesures sans tenir compte de cet aspect, voue la lutte à l'échec.

---

[516] Cf. **Henry Osborn Quarshie1, Alexander Martin-** Odoom, Fighting Cybercrime in Africa, *Computer Science and Engineering* 2012, 2(6): 98-100. Le sommet avait pour thème en version d'origine : The Fight against Cybercrime: Towards Innovative and Sustainable Economic Development.

[517] Cf. par exemple le 44è sommet de la CEDEAO à Yamoussoukro dès le Vendredi 28 Mars 2014, La CEDEAO installe des équipes d'intervention contre la cybercriminalité, Agence de presse africaine, journal du 15 mai 2014.

Autre exemple : la 23ème Session Ordinaire du Sommet de l'Union Africaine, les 26 et 27 juin 2014 sur la cybersécurité et la législation : disponible sur le site de l'Association francophone de la protection des données : *www.afapdp.org/archives/2701*

C'est pourquoi la coopération multilatérale qu'on peut aussi appeler la mutualisation des efforts est un choix de taille.

En comparaison des solutions concrètes employées par les Etats de l'Union Européenne, ceux de l'Afrique de l'Ouest sont réellement, à ce jour, au stade de réflexion.

Avant 2010, il était possible d'affirmer que l'absence d'un arsenal juridique communautaire favorisait la commission d'actes cybercriminels en toute quiétude. Il n'existait pas. A cette date, cette affirmation peut être nuancée. De ce point de vue, il faut noter que les relations internationales et les accords de partenariats existant entre la plupart des pays ouest-africains et les pays de l'Union Européenne les poussent à mettre en conformité leurs législations avec les normes internationales existantes.
De la sorte, les différents sommets revêtent une utilité notamment dans le secteur des télécommunications, qui est en réel mouvement de réformes au sein de chaque Etat membre de l'UEMOA et de la CEDEAO.

C'est au moyen de la directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace CEDEAO, que la Communauté encadre de manière explicite la lutte contre la cybercriminalité. A la lecture de la directive portant lutte contre la cybercriminalité élaborée par les Conseils des ministres des Etats membres de la cybercriminalité, il se dégage un constat général : une multitude de textes visés dans des domaines différents, convergent vers le thème central de la cybercriminalité. La directive a un champ d'application large contenu à l'article 3 qui se décline en deux volets : d'une part elle concerne les infractions relatives à la cybercriminalité et d'autre part les infractions pénales dont la constatation requiert une preuve électronique. La directive définit d'abord dans les articles 4 à 25 les infractions spécifiques aux technologies de l'information et de la communication. Elle classe ensuite dans une seconde catégorie les adaptations des infractions classiques aux technologies de l'information et de la communication et le fait dans les articles 26 à 29.

L'approche est spécifique en ce qu'elle aborde les incriminations par exemple, de manière simple. Ce qui n'est pas le cas des textes de la Convention de Budapest, qui, bien qu'élaborés de façon riche et précise, tendent à trop complexifier les termes des infractions. Ces difficultés ne les rendent pas forcément accessibles. Il faut encore d'autres textes expliquant ce qui est visé. La volonté de pédagogie des Ministres de la CEDEAO doit, de ce fait, être mise en relief. A la suite de la directive 06/11 sur la lutte contre la cybercriminalité dans l'espace de la CEDEAO[518], les Etats sont sommés de prendre des mesures nécessaires afin d'adapter leur législation surtout leurs codes pénaux en vue d'une harmonisation du droit dans cette zone d'échanges monétaires. Quelle est dès lors l'approche nationale de la lutte contre la cybercriminalité ?

b- L'approche nationale de la lutte contre cybercriminalité

L'approche nationale diffère selon que les Etats sont membres du Commonwealth ou non.

1. Dans les Etats membres du Commonwealth

En Afrique de l'Ouest, sont membres du Commonwealth : le Nigéria, le Ghana, la Gambie et la Sierra Léone.

En matière de cybercriminalité, il existe une coopération entre le Conseil de l'Europe et ces pays. C'est en ce sens que se réunit depuis 2011, un groupe de travail réfléchissant avec le Conseil de l'Europe à l'application de la convention de Budapest selon le modèle législatif du Commonwealth[519]. Sur la base des travaux de ce groupe, l'ensemble des législations applicables est élaboré et les entités habilitées à leur application sont spécifiées. Les pays concernés pour l'Afrique de l'Ouest sont : le Ghana, le Nigéria, la Gambie.

---

[518] Directive CEDEAO 06/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, Abuja Juin 2011 et la directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO signée à Abuja les 17-19 Août 2011.

[519] Cf.: The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law Council of Europe contribution to the Commonwealth Working Group on Cybercrime, Data Protection and Cybercrime Division Strasbourg, 27 February 2013.

α. Le Ghana

La cybercriminalité est connue au Ghana sous la dénomination de « Sakawa crime »[520].

Plusieurs moyens sont mis en œuvre par les cybercriminels pour atteindre leurs objectifs et dans ce cadre, l'un des procédés le plus utilisé spécialement au Ghana est le morcellement des ordinateurs de seconde main, exportés des pays étrangers et généralement de l'Europe ou de l'Amérique. L'opération consiste à désagréger un ordinateur de manière à pouvoir atteindre les données contenues ou stockées sur le disque dur ou sur la mémoire interne. Une fois ces informations obtenues, les cybercriminels les utilisent pour obtenir des sous grâce à des chantages via internet.

Il existe depuis 2008, au Ghana, la loi sur les transactions électroniques appelée « the Electronic Transaction Act » du 18 décembre 2008. Au titre des sanctions contenues dans ce texte, l'article 141 de cette loi ghanéenne autorise les agences de sécurité informatique de l'Etat à confisquer l'accès aux réseaux informatiques, aux cyber-fraudeurs. Cette autorisation de confiscation de l'accès au réseau est une sanction technique exercée par les agences de sécurité informatique. Le problème avec cette autorisation conférée par la loi est que ces agences sont en général des entreprises privées. Dès lors, sur quels fondements une agence de sécurité informatique (organisme de droit privé) peut-elle confisquer l'accès au réseau à un citoyen ? C'est la question des preuves à établir qui est sous-jacente. La loi ghanéenne a-t-elle prévu les conditions de qualification d'un cyber-fraudeur ?

Les actes cybercriminels épousent diverses formes particulières notamment les arnaques en ligne à l'encontre des ghanéens vivant en dehors du Ghana (et appelé la Diaspora), les vols d'identité et les trafics d'investissement en or et autres produits de valeur.

---

[520] Cf. **JASON WARNER**, "Understanding Cyber-crime in Ghana: A view from Below, in International Journal of Cyber Criminology, July 2011, Vol. p. 736-749 et http://www.ghanabusinessnews.com/2009/08/19/ghana-to-set-up-cyber-crime-response-team/

Il faut à cet effet souligner une infraction importante qui mérite à tout point de vue une incrimination particulière : c'est le craquage des anciens ordinateurs récupérés pour en extraire des données par la suite utilisées sur les réseaux numériques. En effet, le Ghana est l'un des Etats de l'Afrique de l'ouest dans lequel plusieurs ordinateurs en provenance des Etats comme les Etats Unis ou d'autres pays développés sont envoyés. C'est la pratique des Etats développés de se débarrasser de leurs anciens appareils électroniques dans certains pays dits pauvres. Les ordinateurs par exemple, sont « *jetés* » et se retrouvent en circulation parce que récupérés par des personnes qui, par la suite, en font un usage illicite c'est-à-dire cybercriminel. Ainsi, une fois en possession des vieux ordinateurs, les jeunes ghanéens s'adonnent au craquage et à la récupération des informations stockées dans les disques durs de ces appareils[521]. Les données récupérées leur servent par la suite à retrouver leurs propriétaires grâce à internet et à organiser des chantages financiers ou affectifs ou encore pour des vols d'informations bancaires pouvant servir à des détournements de fonds. Quel encadrement légal est prévu pour ces infractions ? Sont-elles toutes incriminées ?

Pour l'heure, il n'existe pas encore de législation spécifique à ces agissements. Ils sont régis par le droit pénal commun. Il faut à cet effet souligner qu'au Ghana, le *sakawa* a l'air d'un culte. Il y a du mysticisme qui est lié à l'activité des cybercriminels, et des meurtres peuvent même être commis. Les incriminations devront de ce fait tenir compte non seulement de la dimension de vols des activités illicites pratiquées mais également du volet pénal et des circonstances aggravantes.

Il faut noter que les lois de lutte contre la cybercriminalité, en ce qui concerne les Etats du Commonwealth, sont votées dans le cadre du projet global de législation contre la cybercriminalité. Ce projet initié avec le Conseil de l'Europe notamment du 9-11 juillet 2008 à Cotonou et lors de la Conférence panafricaine en novembre 2008 en Côte-d'Ivoire à Yamoussoukro.

---

[521] Cf. **JASON WARNER**, "Understanding Cyber-crime in Ghana: A view from Below, in International Journal of Cyber Criminology, July 2011, Vol. p. 736-749 : dans cet article, il décrit dans le détail cette pratique de récupération des données sur des disques durs d'anciens ordinateurs en provenance des Etats d'Europe et d'Amérique surtout.

A la suite de la première phase, s'est tenue une seconde étape sous l'égide du premier sommet ouest-africain sur les Fraudes informatiques du 2 au 3 février 2010, à Abuja, Nigeria.

β. Le Nigéria

S'agissant de ce grand Etat, le Nigéria, reconnu mondialement pour son rang pétrolier, le processus est long et il débute en 2005 avec la loi sur la sécurité informatique et l'arsenal de protection des informations sensibles dite "Computer Security and Critical Information Infrastructure Protection Bill" de 2005, présentée au Parlement mais dont l'approbation a échoué avant l'expiration du délai en 2007. En ce sens, le Nigéria a participé à plusieurs activités organisées par le Conseil de l'Europe de 2007 à 2012. Poursuivant ses objectifs, le Nigéria se dote d'une loi sur le piratage électronique : "Computer Misuse" de 2009.

Avant 2011, il est impossible pour les tribunaux nigérians d'admettre des preuves générées par les ordinateurs encore moins les preuves électroniques. Grâce à la loi relative aux preuves de 2011, ce problème est désormais réglé. La volonté de lutte contre la cybercriminalité du Nigéria est claire.

En témoigne le discours du Président Jonathan GOODLUCK le 19 juillet 2011 dans son discours[522] prononcé lors de sa rencontre avec le Premier Ministre britannique David Cameron.

Dès 2004, le gouvernement fédéral nigérian crée le groupe de travail nigérian (Nigeria Cyber Working Group) pour lutter contre la cybercriminalité.
Dans cet Etat, les autorités en charge de la lutte contre les actes cybercriminels se fondent sur la recherche du gain économique de ces activités frauduleuses. C'est pourquoi, l'appréhension se fait d'un point de vue monétaire via la création de taxes liées aux fraudes. Le modèle est différent des Etats francophones.

En 2006, au Nigéria, est mis en place un texte Advance Fee Fraud and other Offences Act of 2006, appelé loi contre la cybercriminalité. La cybercriminalité est

perçue comme un frein à l'économie nigériane[523] et c'est pour cette raison qu'elle est traitée sous cet angle. Il faut cependant souligner le caractère très général de ce texte qui concerne généralement les infractions financières et à caractère économique[524].

Au niveau des mesures à prendre, elles sont d'une part des mesures financières et économiques en ce que les actes commis par les cybercriminels ont essentiellement pour but de soutirer des fonds à leurs victimes et d'autre part les dispositions prévues pour lutter contre la cybercriminalité prennent la forme de dispositifs de sécurité notamment informatique.

Le Nigéria fait des efforts, depuis 2007, en vue de mettre sa législation à jour et en adéquation avec la Convention de lutte contre la Cybercriminalité.[525]

En 2011, est votée la loi sur la Cyber-sécurité. Cet acte comporte les dispositions encadrant l'élaboration des preuves électroniques. D'ailleurs, il est possible d'y retrouver les incriminations et les sanctions des vols d'identité, du *cyber-squatting* ou encore du cyber-terrorisme notamment.

Si l'approche législative des Etats du Commonwealth se fonde sur les travaux de groupe notamment ceux qui sont effectués dans le cadre de la coopération avec le Conseil de l'Europe, comment la lutte contre la cybercriminalité prend-t-elle forme dans les législations des autres Etats non membres du Commonwealth ?

2. Dans les autres Etats

---

[522] Discours du Président nigérian, cf. http://ukinnigeria.fco.gov.uk/en/news/?view=PressR&id=632784582

[523] **NUHU RIBADU**, Cybercrime and Commercial Fraud: A Nigerian Perspective, Congress to celebrate the fortieth annual session of UNCITRAL, Vienna, 9-12 July 2007.

[524] Cf. **ADOMI** Security ans Software for cybercafes, IGI, 2008, p. 228 ; **Uchenna Jerome ORJI**, Legal Governance of Information Technology in Nigeria and African States: An Assessment of Responses to Computer Security, University of Ibadan, Nigeria, May 2010.

[525] Communiqué de presse - 413(2007) de la division de la presse du Conseil de l'Europe à la suite de la conférence du 13 juin 2007 à Strasbourg sur la promotion de la Convention de lutte contre la cybercriminalité.

Les autres Etats sont ceux qui ne font pas partis du Commonwealth c'est-à-dire le Bénin, la Côte-d'Ivoire, le Burkina Faso, le Mali, le Niger, le Sénégal, le Togo, et le Tchad.

α. La Côte-d'Ivoire

Le 14 mai 2013 et sur présentation du Ministre des Postes et des télécommunications, l'Assemblée Nationale ivoirienne a adopté le projet de loi relatif à la loi sur la cybercriminalité[526]. Ce texte, tant attendu de la part des victimes de « brouteurs »[527] mais aussi des acteurs des différents secteurs économiques, sanctionne de 1 à 20 ans de prison tout acte cybercriminel et de 500 à 100 000 FCFA d'amende. Il est publié au journal officiel de la République de Côte-d'Ivoire depuis le 12 août 2013 dans une édition complémentaire. La Côte-d'Ivoire a désormais un texte de loi national contre la cybercriminalité. Cette démarche est salutaire dans un état cité comme « un paradis pour les cybercriminel ».

C'est d'ailleurs la référence légale qui faisait défaut puisque récemment, dans le cadre de la coopération internationale, le FBI a arrêté deux ivoiriens cybercriminels avec la coopération des services de police et surtout avec le travail de la plateforme de lutte contre la cybercriminalité[528]. Les textes de loi encadrant la lutte contre la cybercriminalité se mettent en place petit à petit. Cette mise en place progressive permet l'activité judiciaire dans les états de l'Afrique de l'Ouest. Les magistrats ont, de la sorte, une base légale plus pertinente et adéquate pour régler les questions de sanctions contre les actes cybercriminels. Avant ces lois, les textes de références étaient ceux de droit pénal traditionnel comme les dispositions sanctionnant le vol, les recels ou autres escroqueries et abus de confiance.

---

[526] Cf. article de l'Agence de Presse Africaine et la Loi n° 2013-451 relative à la lutte contre la cybercriminalité publiée au Journal Officiel de la République de Côte-d'Ivoire édition complémentaire n° 32 du lundi 12 août 2013.

[527] Le terme « brouteur » est employé couramment en Côte-d'Ivoire pour designer des personnes s'adonnant à des actes d'intrusions frauduleuses et principalement d'arnaques financières via internet.

[528] Cf. le site de la plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire : http://cybercrime.interieur.gouv.ci/

β. Le Bénin

Le cas du Bénin est très particulier. Les dispositions légales traitant des sanctions contre la cybercriminalité figurent au chapitre 5 de la loi portant lutte contre la corruption[529]. Ce chapitre 5 traite des infractions cybernétiques et informatiques. Il est dommage qu'un problème récurrent comme la corruption soit mêlé aux actes de cybercriminalité, la corruption étant un fléau aussi important que la cybercriminalité. Il aurait été intéressant et plus judicieux de scinder les deux dispositifs compte tenu de l'ampleur et de l'évolution des deux phénomènes, particulièrement en Afrique. La corruption est une ancienne plaie de ce continent et même s'il est louable que des sanctions pénales soient prévues à cet effet, elles ne doivent pas être combinées à des actes cybercriminels, qui exigent également des sanctions particulières et dans un autre dispositif légal.

Dans le cadre de l'implantation de la cyberstratégie, le Conseil de l'Europe travaille avec le Bénin, le Sénégal et le Nigéria. Ces trois Etats sont particulièrement avancés au niveau de la lutte contre la cybercriminalité.

La législation sénégalaise et surtout l'activité judiciaire née de l'application de cette législation en est une preuve. En ce qui concerne le Bénin, le cadre législatif quelque peu discutable sur la cybercriminalité, notamment les sanctions qui y figurent, souligne les efforts effectués dans le domaine.

§2- Les impacts de la législation sur l'appareil judiciaire

---

[529] Cf. loi n°2011-20 du 12 octobre 2011portant lutte contre la corruption et autres infractions connexes en République du Bénin, publiée au Journal Officiel sous le numéro spécial 05 bis du 06 mars 2012 avec plusieurs décrets d'application :

1°) - décret n°2012-338 du 02 octobre 2012 portant modalités d'application des articles 3 et 10 de la loi n° 2011-20 du 12 octobre 2011 portant lutte contre la corruption et autres infractions connexes en République du Bénin ;

2°) - décret n°2012-336 du 02 octobre 2012 portant attributions, organisations et fonctionnement de l'Autorité Nationale de Lutte contre la Corruption, publié au Journal Officiel sous le n° 02 du 15 janvier 2013 ;

3°) - décret n°2013-122 du 06 mars 2013 portant conditions de protection spéciale des dénonciateurs, des témoins, des experts et des victimes des actes de corruption, publié au Journal Officiel sous le n° 14 du 15 juillet 2013 ;

4°) - décret n° 2013-241 du 08 mai 2013 portant nomination des membres de l'Autorité Nationale de Lutte contre la Corruption.

L'appareil judiciaire est le meilleur outil pour mesurer l'impact des législations mises en place aussi bien au niveau régional que national. C'est une phase intermédiaire obligatoire à la mise en œuvre de la répression contre la cybercriminalité contenue dans les textes de loi. Les différentes conséquences observées permettent ainsi de qualifier les lois de suffisantes ou non. Elles sont le moyen de vérifier l'importance d'éventuelles adaptations nécessaires.

C'est à la lumière de la jurisprudence se fondant sur les textes édictés que sera étudiée l'activité judiciaire (A).

Le caractère récent des législations punissant les comportements cybercriminels en Afrique en général et dans les Etats ouest-africains en particulier démontre une longue période d'impuissance des gouvernements face à ce fléau pourtant grandissant. Il convient cependant à la lumière des textes récents édictés et des cas de jurisprudence d'analyser l'application des normes au niveau des juridictions par exemple. Passer en revue les textes visés par la directive portant lutte contre la cybercriminalité ainsi que les domaines pointés montre une approche légèrement différente du problème par rapport à l'Union Européenne (B).

A- L'activité judiciaire

L'activité judiciaire en matière de cybercriminalité est marquée par la rareté des décisions de justice. Jusqu'à une date très récente (milieu des années 2008), les juges fondent leur décision sur le droit pénal traditionnel. Il en résulte des décisions de justice peu adaptées au contexte de l'efficacité des sanctions contre la cybercriminalité. Une application prospective des jurisprudences africaines pourrait être le support adéquat pour mesurer l'adaptation des normes édictées au fléau cybercriminel en territoire africain. Cette faible quantité de décisions conduit à une approche différente de l'activité judiciaire.

a- La jurisprudence africaine peu foisonnante en matière de répression de la cybercriminalité

Plusieurs raisons expliquent le nombre peu important des décisions de justice en matière de criminalité organisée liée à la haute technologie.

La première raison résulte de la cible visée par les cybercriminels africains.

En effet, sur un plan africain, la cybercriminalité s'analyse plus en termes d'infractions des locaux vers d'autres sites étrangers et souvent européens. C'est en cela que la jurisprudence offre à titre d'exemple des cas de répression de cybercriminels africains ayant perpétré des actes à destination de sites européens. En témoigne l'affaire du Spam Nigérian, dont a eu à connaître la Cour d'appel de Rennes[530]. Les faits à l'origine de cette décision sont les suivants : plusieurs individus se sont faits passer pour diplomate, afin d'extorquer des fonds à un ressortissant européen héritier ayant besoin d'aide pour le transfert de fonds et personnes en attente de ce transfert

La seconde raison est liée à la construction même de l'arsenal juridique, support des décisions de justice. Cet état de la jurisprudence tient compte du caractère récent de la législation spécifique en la matière. Du fait du manque de textes spécifiques, il n'est pas étonnant de voir des affaires de cybercriminalité jugées en s'appuyant sur des règles de droit commun alors que la cybercriminalité devrait avoir pour support des règles pénales spéciales. Ce n'est que depuis 2004 que la plupart des Etats se sont dotés de législations sur la protection des données par exemple. C'est l'exemple du Burkina Faso ou de la Côte-d'Ivoire ou encore avec le Sénégal.

Dans ce sens, les Etats comme le Sénégal ou la Côte-d'Ivoire rendent des décisions de justice sanctionnant des actes relevant de la cybercriminalité.

Au Sénégal par exemple, la répression par les décisions de justice a réellement débuté dès 2009. En effet, par son jugement n° 3375 du 29 juillet 2009, le tribunal Hors Classe du Sénégal a statué sur une tentative d'escroquerie par le biais d'un système informatique. En l'espèce, une personne utilisait un site Web et des SMS[531] pour proposer des relations sexuelles en contrepartie d'une offre d'emploi[532]. Le tribunal a condamné

---

[530] Cour d'appel de Rennes, 3ème chambre, 20 novembre 2007, Ministère public, F., G. / MM. A. B. C. D. E., disponible en ligne sous le lien : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2291

[531] Acronyme désignant les messages écrits transférés par voie de téléphone mobile, SMS est issu de l'anglais et correspond à Short Message Service qu'il est possible de traduire par Service de court message.

[532] Jugement du Tribunal Hors Classe du Sénégal n° 3375 du 29 juillet 2009.

ces agissements en réglant la question de l'escroquerie de service. Il a par contre exclu les « relations sexuelles » du champ d'application des services visés par l'article 379 bis du Code pénal. Selon cet article en effet, l'article 379 bis du code pénal sénégalais[533] : « Quiconque aura reçu des avantages ou des commodités matérielles, des prestations ou se serait fait fournir des services en employant soit des manœuvres frauduleuses, quelconque, soit en soit en faisant usage de faux nom ou de fausses qualités, sera puni des peines prévues à l'alinéa premier de l'article précédent »[534].

A la lumière de ces articles et surtout du cadre de commission des infractions, il aurait été plus constructeur pour le législateur sénégalais d'intégrer une disposition plus spécifique quant aux faits reprochés. Cette remarque permet de mettre en exergue le fait que des sanctions traditionnelles continuent d'être appliqués à des actes susceptibles de la qualification cybercriminelle, surtout lorsque ces pratiques sont répétitives. Sanctionner les délinquants ne sera efficace que si les décisions font jurisprudence avec une acuité particulière.

D'un autre point de vue, les lois relatives à la cybercriminalité n'ont été votées au Sénégal qu'en 2008. Il est de ce fait possible d'estimer que les juges n'ont pas encore suffisamment de recul sur ce genre d'activités criminelles, au moment de la commission des exactions.

Il faut tout de même constater une évolution de la jurisprudence entre 2008 et 2012 avec la mise en place des textes spécifiques à la cybercriminalité.

b- L'évolution de la jurisprudence à la lumière des textes de lois

---

[533] Cette disposition a été introduite au code pénal grâce à la loi n° 99-05 du 29 janvier 1991.

[534] C'est-à-dire l'alinéa premier de l'article 379 du même code qui dispose que : « *Quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges, et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui, sera puni d'un emprisonnement d'un an au moins et de cinq ans au plus, et d'une amende de 100.000 à 1.000.000 francs CFA ».*

Cette évolution est positive et est marquée par un foisonnement des décisions de justice grâce à l'élaboration des corpus juridiques. L'exemple du Sénégal permet d'illustrer le propos.

En 2010, le Tribunal Hors Classe s'adonne de nouveau à l'exercice dans une affaire du 21 janvier 2010 en application de l'article 431-16 de la loi sur la cybercriminalité. Cette fois, le texte est spécifique. En l'espèce, il s'agit d'un réseau anglophone de cybercriminels démantelé à la suite d'enquêtes de la Division des investigations criminelles. Des messages avec pour contenu des transactions financières fictives sont émis par les délinquants. Ils abusent de la sorte de la crédulité de certaines personnes pour les attirer dans des pièges et leur soutirer de l'argent. Ces actes sont incriminés au Nigéria sous l'appellation de *scam* 419, du numéro de l'article du code pénal nigérian correspondant. C'est l'avantage qu'aurait tiré le délinquant, en soutirant les sommes, qui est le critère de réalisation de l'infraction, selon l'appréciation du juge. Il est dommage que les officiers en charge de l'enquête n'aient pas révélé les éléments constitutifs pour corroborer les faits. Il ressort des faits de l'espèce que, le juge saisi ne disposait pas de suffisamment de preuve pour condamner les délinquants appréhendés. Le problème est réellement que la loi sur la cybercriminalité n'a pas prévu de sanction en cas de tentative. Comme le souligne le docteur Mouhamadou LO[535], docteur en droit au Sénégal et Juriste à l'Agence Informatique de l'Etat au Sénégal[536], ces dispositions relatives à la tentative et surtout à sa sanction devront être prévues et intégrées lors des reformes de la loi sur la cybercriminalité, qui, soulignons-le, est encore jeune. Ce n'est qu'avec les différentes applications des juges qu'elle montrera ses insuffisances.

---

[535] Cf. **LO Mouhamadou** dans son article publié sur les premières décisions en matière de cybercriminalité au Sénégal : http://www.pressafrik.com/La-lutte-contre-la-cybercriminalite-les-premieres-decisions-de-la-justice-senegalaise_a40664.html. La contribution de Docteur LO a été considérable en ce qui concerne la jurisprudence sénégalaise sur la question. Compléter avec **P. A. TOURE**, Le traitement de la cybercriminalité devant le juge: l'exemple du Sénégal, éditions l'HARMATTAN, 2014 : dans cet ouvrage spécifique à la justice sénégalaise, l'auteur détaille des faits des décisions de justice récemment rendues par le juge contre des actes cybercriminels notamment en 2012 et 2013.

[536] Agence Informatique de l'Etat au Sénégal créée par le décret n° 2004-1038 du 23 juillet 2004.

Il appartient par ailleurs aux juges d'établir la jurisprudence en l'espèce. Toutefois, s'agissant d'une matière pénale, il sera question pour les juges pénaux de formuler de manière explicite les motifs justifiant les relaxes, comme c'est le cas avec l'espèce soumise au juge du Tribunal Hors Classe du Sénégal.

La jurisprudence de la cybercriminalité est en construction dans les Etats de l'Afrique de l'Ouest. Les décisions sont encore au stade de tâtonnements normaux du fait du caractère récent des législations. Les Etats comme la Côte-d'Ivoire n'ont pas encore réellement mis à disposition du public les décisions de justice. La documentation sur ce plan est difficile à acquérir et les plateformes en ligne des entités judiciaires ne sont pas encore dotées à l'instar des Etats européens de décisions en ligne pour l'instant même si les TIC commencent à entrer dans les habitudes administratives.

En l'absence de décisions de justice foisonnante, l'activité judiciaire doit être basée sur des fondements solides à savoir la cohérence et d'éventuelles adaptations des applications textuelles au contexte ouest-africain.

B- Les fondements d'une bonne politique de lutte: cohérence et adaptation

Bien que naissant, l'arsenal juridique se met en place et s'érige en vecteur de prise en compte des problématiques comme la nécessité d'une autorité indépendante régionale pour coordonner l'action des Etats ouest-Africains (a).

D'ailleurs, en s'appuyant sur ces applications factuelles, les perspectives d'adaptation des textes aux réalités du terrain (b) se dessinent. En cela, l'aspect théorique des solutions n'empêche pas de s'interroger sur l'efficacité des accords existant en la matière entre les Etats africains et les Etats membres de l'Union européenne. Ces actes multilatéraux du fait de leur dimension territoriale pourraient certainement contrecarrer la théorie des propositions émises via les organismes. Ils pourraient ainsi favoriser une amorce de lutte dans les territoires africains et remédier au retard de ce continent dans la recherche d'éradication de la cybercriminalité.

a- La nécessité d'une autorité administrative indépendante

Qu'il s'agisse de la Côte-d'Ivoire ou d'un autre Etat quelle que soit sa situation géographique, l'autorité en charge du contrôle de l'application des normes liées aux TIC

doit avoir une certaine indépendance. En cela, il est permis de citer le ministre ivoirien des Technologies de l'Information qui a fait remarquer l'importance d'une indépendance de cette autorité. Ce qui fait réellement la force de décisions d'une autorité c'est son indépendance et son autonomie entière par rapport aux pouvoirs publics ou étatiques en place. En 1992, par exemple au Bénin, ADJOVI décrit la lenteur dans la mise en place de l'instance de régulation audiovisuelle au Bénin. Il révèle les difficultés pour les autorités de régulation d'avoir une réelle indépendance par rapport aux gouvernements en place. Et le cas béninois n'est pas isolé[537].

Dès lors, se pose aujourd'hui, la question de l'autorité en charge de l'application des lois relatives à la lutte contre la cybercriminalité. Est-ce la compétence des autorités de régulation des télécommunications ou celle de nouvelles autorités ? La réponse à cette interrogation est variable suivant l'Etat.

En Côte-d'Ivoire, la mission de protéger les données à caractère personnel est confiée à l'Autorité de la Régulation des Télécommunications par l'article 46 de la loi du 19 juin 2013 relative à la protection des données à caractère personnel[538]. Selon les dispositions de cet article, *les missions de l'autorité de protection des données à caractère personnel sont confiées à l'autorité administrative indépendante en charge de la régulation des télécommunications et des Technologies de l'information et de la communication.*

Pour une gestion efficace, confier la protection, le contrôle des données à caractère personnel à l'autorité en charge de la régulation des télécommunications est risqué.

En effet, les télécommunications comprennent la Télévision, les radios et même si en Côte-d'Ivoire ces moyens de télécommunications ne sont pas en nombre trop important, une seule institution ne saurait à elle seule avoir les deux types de charges: d'une part la régulation des télécommunications et d'autre part l'usage adéquat de ces

---

[537] **ADJOVI Emmanuel V.,** Les instances de régulation des médias en Afrique de l'Ouest, le cas du Bénin éditions KHARTALA- FES, Paris, 2003.

[538] Cf. Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, JORCI du 08 août 2013.

télécommunication et d'autres technologies nouvelles que sont les réseaux numériques. L'attribution des compétences de régulation uniquement aurait été plus sage.

D'un autre point de vue, l'attribution de la régulation et du contrôle de la protection peut se défendre dans la mesure où, pour le cas de la Côte-d'Ivoire, le champ d'application de ces régulations n'est pas trop étendu. Le nombre des acteurs clés n'étant pas excessif.

A qui est confié le contrôle ou la gestion de la lutte contre la cybercriminalité ?

La lutte contre la cybercriminalité est confiée en Côte-d'Ivoire à la Plateforme de Lutte contre la Cybercriminalité au niveau de la réception des plaintes des victimes et de la sensibilisation des populations dans l'usage des technologies de l'information et de la communication. Mais en termes de contrôle de l'application des lois relatives à la cybercriminalité, la législation est muette.

Dans des Etats comme le TOGO, la question est réglée depuis qu'il existe la Cellule de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (CLCTIC). Cette entité a pour *mission de mener les investigations sur les infractions liées à la cybercriminalité, de collecter et d'analyser les informations liées à cette infraction*[539].

En plus de ce partage de compétences, l'attribution des noms de domaine reste un autre problème majeur à résoudre au plan de l'Afrique.

C'est le lieu de faire le lien avec la remise en cause de l'autorité de l'ICANN[540] par rapport à l'administration américaine. En effet, cette autorité d'envergure mondiale à qui a été confiée l'affectation des noms de domaine voit son indépendance sans cesse remise en cause notamment par l'Union européenne. Ce doute est surtout dû aux liens étroits que l'ICANN entretient encore avec l'administration américaine. D'où il suit qu'une structure rendant des décisions en matière de commission d'infractions

[539] Cf. La lettre de l'Ambassade de France au TOGO Janvier 2012 - n°2.

[540] Cf. **CHEVALIER J**., L'Etat régulateur, Revue française d'administration publique, 2004/3 no111, p. 473-482.

numériques serait plus crédible en Afrique notamment, si elle a une parfaite indépendance tant dans son fonctionnement que dans sa prise de décisions.

Dans le cadre de l'attribution des noms de domaine, d'une certaine manière, l'ICANN participe pour une part importante du succès de la lutte en matière de cybercriminalité.

L'ICANN est présente en Afrique sous le nom de l'AFRINIC, agence de gestion des noms de domaines. Cette agence de gestion a les délégations de l'ICANN. Elle représente l'organisme au plan de l'Afrique. Mais il n'existe pas suffisamment en Afrique de représentants. Seuls certains Etats comme le Nigéria par exemple, ont entamé les démarches pour avoir une gestion plus claire des noms de domaine notamment avec le Nigerian Internet Registration Association (NIRA) instituée le 23 mars 2005.

L'Afrique recevra un nom de domaine panafricain une fois que l'ICANN aura évalué les offres pour administrer le nouveau ***.africa*** (se lit dotAfrica) top level domain (TLD) des différents opérateurs registraires. L'un des enjeux majeurs de la mise en place de structures sur le terrain africain traitant directement de l'attribution des noms de domaine est une ébauche de solution pouvant mettre fin à de nombreuses pratiques comme les spams. Il faut à cet effet souligner que lorsqu'une personne reçoit un mail dont elle ne connaît,pas l'expéditeur, la racine attachée est souvent *.gmail* ou *.it,* ou *.hotmail*. Or, le fait d'adresser les noms de domaines obligerait ces spammeurs à se soumettre à la certification et à avoir leurs propres noms de domaine.

Cette technique est une autre forme de contrôle qui reste à explorer davantage. Au titre des illustrations de l'encadrement ou de structure indépendante allant dans le sens de mettre fin le phénomène de la cybercriminalité, une meilleure coordination des services de l'Etat. C'est l'exemple d'un état avancé comme le Bénin notamment dans le cadre de ses télécommunications.

Le 10 Mai 2007, l'Autorité Transitoire de Régulation des Postes et Télécommunications (ATRPT) est créée, par décret N°2007-209 du Ministère Délégué Chargé de la Communication et des Technologies de l'Information et de la Communication auprès du Président de la République du Bénin.

Cet établissement public indépendant (financièrement) a provisoirement pour mission la

régulation du secteur des télécommunications et des TIC. Elle comprend le Conseil Transitoire de Régulation et le Secrétariat Exécutif qui est essentiellement chargé de préparer et d'exécuter les décisions prises par le Conseil.[541]

Par ailleurs, il existe une autorité indépendante en l'institution de la Haute Autorité de l'Audiovisuel et de la Communication (HAAC). Elle est instituée par la Loi Organique, n°92-021 du 21 Août 1992[542].

S'agissant du domaine de la téléphonie, l'attribution des fréquences radioélectriques est faite par le Ministère en Charge des télécommunications. Quant au contrôle de ces fréquences, une fois attribuées, c'est l'autorité de Régulation qui en a la charge. Les fréquences des radiodiffusions et de la télévision sont attribuées par la HAAC.

Il se trouve qu'il s'agit des mêmes fréquences.

Il faut reconnaître au continent européen et principalement aux Etats membres de l'Union européenne leur force : la volonté manifeste de mettre fin à la cybercriminalité par une politique commune et soudée. Et pourtant, il faut souligner l'existence de défauts et des failles à cette politique.

Outre les échecs et les défaillances, la stratégie de lutte n'est certainement pas adaptée dans son intégralité aux réalités africaines. Il convient de mettre un point d'honneur sur cette remarque puisque d'une manière générale les Etats africains oublient souvent d'adapter à leurs vécus respectifs les normes européennes copiées. Certes, le fait de prévoir des lois en adéquation avec les systèmes européens, ou encore le fait d'aligner leur législation dans un but de sécurité juridique poursuit un but d'efficacité des normes. Mais, il faut tenir compte des échecs de certaines techniques ou politiques et en tirer des leçons pour éviter de reproduire et perpétuer les erreurs du passé.

---

[541] cf. Revue de Performance du Secteur des TIC Benin 2009/2010, dossier réalisé par **CHABOSSOU Augustin** ; voir en complément **TCHENG H.** et al. « Télécoms et développement en Afrique», Futuribles : Analyse et prospective, février 2009, n°349, page 39-52.

[542]Cf. Loi Organique, n°92-021 du 21 Août 1992 Relative à la Haute Autorité de l'Audiovisuel et de la Communication (H.A.A.C.).

A l'instar de la mise en place en Europe d'organismes en charge de la lutte contre la cybercriminalité, les Etats africains s'inspirent et se mobilisent tout en prenant le soin d'adapter les problématiques aux réalités de leurs territoires.

Si le système de nommage des domaines est l'un des secteurs à privilégier et à assainir pour une réelle indépendance de l'internet et des réseaux numériques en Afrique, le secteur bancaire est l'autre dimension à privilégier. En dépend l'efficacité de la lutte contre les diverses et multiples fraudes exercées à l'encontre des comptes bancaires quelle qu'en soit la situation (les comptes bancaires qui font l'objet d'actes cybercriminels pouvant se situer n'importe où dans le monde). Ce qui conduit à analyser le secteur bancaire au niveau de l''espace UEMOA et de celui de la CEDEAO.

b- Le secteur bancaire au sein de l'UEMOA et de la CEDEAO

Si les bases de données, les interfaces de communication des données bancaires sont encadrées en Europe, elles le sont également au niveau international et également dans les Etats Africains. Le domaine bancaire est l'un des secteurs les plus règlementés dans les zones UEMOA et CEDEAO. On peut mentionner ici l'ensemble des dispositifs mis en place tels que la directive relative aux transactions électroniques dans l'espace UEMOA, ainsi que la directive 07/2002/CM/UEMOA touchant à la lutte contre le blanchiment des capitaux dans les Etats membres de l'UEMOA[543].

Il faut dans ce domaine mentionner comme illustration l'accord BALE du 12 décembre 1988, qui est une déclaration internationale exigeant des institutions bancaires de collecter les données lui permettant d'identifier tous ses clients, spécialement les titulaires de comptes et de coffres afin de pouvoir garantir la sécurité des prestations fournies à ces derniers.

Les accords BALE 2 ont été signés par les banques centrales en vue d'établir une nouvelle règlementation bancaire tenant compte du niveau de capitaux propres pour

[543] Directive relative à la lutte contre le blanchiment de capitaux dans les Etats membres de l'UEMOA : Directive n°07/2002/CM/UEMOA du 19 septembre 2002 disponible sur la base de donnéss des textes de la BCEAO sous le lien suivant : http://www.bceao.int/Directive-No07-2002-CM-UEMOA.html.

accorder des prêts ou des crédits[544]. Cet ensemble Bâle 2 est un dispositif établi en juin 2004 et correspond à une adéquation des fonds propres à la solvabilité des banques. Ces accords sont entrés en vigueur le 31 décembre 2006. Ces accords Bâle 2 sont transposés en droit européen grâce à deux directives : **directive 2006/48/CE du Parlement européen et du Conseil du 14 juin 2006 concernant l'accès à l'activité des établissements de crédit et son exercice**[545] et **la directive 2006/49/CE du Parlement européen et du Conseil du 14 juin 2006 sur l'adéquation des fonds propres des entreprises d'investissement et des établissements de crédit**[546].

Les transactions font l'objet d'encadrement, les flux transfrontières et tous les transferts de fonds également. Les encadrements légaux mis en place visent à éviter les techniques de blanchiment de fonds, qui sont très courantes en Afrique[547].

Il existe des partenariats entre les Etats notamment certains Etats européens, comme la Norvège et des Etats africains. Ces pays participent de manière active à l'amélioration de la lutte contre la cybercriminalité à travers des projets de collecte et de traitement des informations statistiques par les nouvelles technologies de l'information et de la communication. C'est dans ce cadre que la Norvège soutient certains Etats africains (Ethiopie, Ghana, Mozambique, Ouganda et Sénégal) dans le projet SCAN-ICT. Ce projet vise à contribuer au renforcement de leurs capacités dans la collecte, le traitement et la diffusion des statistiques sur les TIC et leur étendue[548].

---

[544] Cf. : http://acpr.banque-france.fr/international/les-grands-enjeux/les-accords-de-bale/bale-ii.html, sur le site de l'Autorité de Contrôle Prudentiel et de Résolution de la Banque de France. Les accords Bale II sont rédigés par le Comité de Bâle sur le contrôle bancaire. Pour une version de ces accords, cf. la Banque des règlements internationaux et pour une version en ligne, consulter : http://www.bis.org/publ/bcbs128fre.pdf.

[545] Cf. Directive 2006/48/CE du Parlement européen et du Conseil du 14 juin 2006 concernant l'accès à l'activité des établissements de crédit et son exercice publiée au Journal officiel de l'Union européenne, L 177, 30 juin 2006.

[546] Cf. Directive 2006/49/CE du Parlement européen et du Conseil du 14 juin 2006 sur l'adéquation des fonds propres des entreprises d'investissement et des établissements de crédit publiée au Journal officiel de l'Union européenne, L 177, 30 juin 2006.

[547] Cf. **I. DIALLO**, « *Un profil des marchés criminels à Dakar* », in Rapport de l'Institute for Security Studies n° 264 du 4 Août 2014.

[548] Informations recueillies sur http://www.UNECA.org et le Rapport sur les indicateurs en matière de technologies de l'information et des communications et l'impact de la technologie de l'information et des

Ces initiatives sont à féliciter car elles permettent aux deux espaces d'échanger et de se compléter d'un point de vue de la lutte contre la criminalité contre la haute technologie.

---

communications au niveau des pays, rapport E/ECA/DISD/CODI 3/15, Mai 2003 du Conseil Economique et Social des Nations Unies, Commission Economique pour l'Afrique. Compléter avec http://www.osiris.sn/-1-Presentation-du-projet-.html.

CONCLUSION DE LA PREMIÈRE PARTIE

La mise en place d'une politique de lutte contre la cybercriminalité exige plusieurs étapes de réflexion et de tests quant aux résultats des réflexions sur la pratique. Ces différents paliers sont franchis peu à peu par les Etats de l'Union Européenne au fur et à mesure des avancées technologiques. Or, ces avancées impliquent la perfection des auteurs des actes cybercriminels dans leur pratique et dans leur quête de percer les mystères des systèmes informatiques institutionnels, étatiques ou privés.

De nombreuses imperfections ressortent des textes théoriques et il revient à la pratique de les corriger ou les adapter à la réalité ; les prévisions théoriques souffrant toujours des aléas du concret. Les textes se perfectionnent, se précisent davantage au contact des structures qui les appliquent au quotidien. Tandis que les infractions traditionnelles sont remplacées et corrigées en ce qui concerne les incriminations, la difficulté de sanctionner les infractions cybercriminelles s'accentue avec la naissance de nouvelles attitudes à encadrer au plan normatif. C'est pourquoi, il est possible de suggérer que la mise en œuvre des politiques stratégiques de répression de la cybercriminalité mettra certainement à jour les zones abstraites des prévisions de lutte contre ce phénomène.

Pour sa part, l'Afrique de l'Ouest hérite non seulement de ces technologies mais également des dérives qui en naissent. Avec les relations internationales croissantes, cette partie du monde n'a d'autre alternative que de se plier aux exigences de la mise à jour des normes. C'est la raison pour laquelle la lutte contre la cybercriminalité est une autre part de l'héritage européen, mondial mais surtout technologique. Mais il ne peut être question de copier purement et simplement les systèmes européens. A sa façon et à son rythme, l'Afrique de l'Ouest met en place et développe sa politique de coercition à l'encontre de la criminalité contre la haute technologie. Cette mise en place des sanctions en Afrique de l'Ouest est lente, elle bénéficie dans certains cas des collaborations des institutions internationales et européennes.

D'autres problématiques liées à la sanction de la cybercriminalité sont source de difficulté : la multiplicité ou la diversité des domaines en cause. La cybercriminalité intéresse certes les réseaux électroniques et numériques mais elle embrasse divers domaines : les communications, le domaine bancaire, celui de la santé, celui des

consommations. Bref, toutes les composantes de la vie humaine sont touchées. C'est ce qui accentue la complexité à prévoir des dispositions légales et règlementaires sur tous les plans.

Si la mise en place de la politique est l'occasion de réflexions, ses applications permettent de la tester pour mesurer ses résultats et ce quel que soit le continent considéré.

DEUXIEME PARTIE :

LA MISE EN ŒUVRE DU DISPOSITIF REPRESSIF CONTRE LA CYBERCRIMINALITE

L'effectivité de la répression mise en place pourra se mesurer à la mise en œuvre des sanctions dans une acception pratique et technique. La technicité des sanctions et toutes les précautions qui les accompagnent témoignent des réelles difficultés à punir la cybercriminalité. Il en ressort que l'efficacité de la sanction appliquée à la délinquance informatique pourra être jugée et remise en cause en s'appuyant sur les moyens utilisés.

En pratique, il est revenu aux législateurs de raisonner selon deux pistes : soit la cybercriminalité est réprimée selon que l'ordinateur est l'outil de commission de l'infraction, soit l'ordinateur est la cible des cybercriminels[549]. La problématique qui découle de cette catégorisation dans la sanction est celle d'appréhender les difficultés que rencontrent les agents de police judiciaire notamment lors de perquisitions, de réquisitions, d'ordinateurs notamment pour recueillir des preuves de l'infraction commise.

Toutes ces interrogations quant aux preuves des infractions cybercriminelles nécessitent le recul professionnel des praticiens. Grâce à leurs expériences professionnelles, ces agents mettent le mieux en exergue la double analyse de la répression de la cybercriminalité : il s'agit du contrôle a priori (l'aspect préventif) et du contrôle a posteriori (volet punitif) de la politique de lutte contre la délinquance informatique. La répression ne recouvre donc pas uniquement la sanction. Elle implique des mesures particulières de protection qui revêtent dès lors le caractère préventif. Le propos est de viser la protection en amont de la cybercriminalité afin de justifier de la proportionnalité de la sanction qui suivra pour l'hypothèse où des actes cybercriminels seront posés en dépit de toutes précautions prises pour les empêcher. En ce sens, la protection a pour objectif de se prémunir contre des infractions. Ce n'est donc qu'en partie, que l'aspect protecteur contre la cybercriminalité est sous-jacent à sa coercition.

L'examen du dispositif coercitif de la cybercriminalité suppose l'analyse des protections préventives (chapitre 1) avant d'aborder la perspective de la sanction à proprement parler (Chapitre 2).

CHAPITRE 1 : LA PROTECTION CONTRE LA CYBERCRIMINALITE

Traiter de la protection contre la cybercriminalité permet de préciser l'ensemble des mesures techniques particulières mises en œuvre pour éviter la commission des infractions cybercriminelles. Ces techniques sont-elles efficaces dans leur application ?

En termes d'efficacité, il faut mentionner le fait que les législations anciennes sont renouvelées et adaptées aux époques actuelles. Il en va ainsi de la loi de 1991[550] relative à la liberté de communication qui prévoit des règles propres à l'interception des communications ordonnées par l'ordre judiciaire.

Il est possible de souligner une adaptation notable de cette loi à l'ère numérique puisque depuis le 14 mars 2011, le législateur français envisage le sort des perquisitions opérées en matière informatique. Cette loi qui n'est pas sans reproche soulève l'épineuse question des garde-fous des interventions ; elle s'intéresse également à l'encadrement des modes de preuve. Dès lors, les nouvelles dispositions, si elles s'alignent sur le système des écoutes téléphoniques telles que prévues depuis la loi de 1991 seront-elles suffisamment adaptées pour réprimer la cybercriminalité ?

Il serait intéressant de ce point de vue de s'attarder sur la collecte des moyens de preuve, les modes d'investigation utilisés par les officiers et agents de police judiciaire à travers les mesures techniques (Section 1).

Une fois ces techniques et leurs pratiques analysées, se pose la question cruciale de leur efficacité. Pour ce faire, l'efficacité s'apprécie de manière globale mais surtout en fonction des mesures et des moyens pris dans leur individualité (Section 2).

Section 1 : Les mesures techniques préalables

Par mesures techniques préalables, il faut entendre les opérations de terrain effectuées sur les réseaux numériques. Des exigences, comme la tenue de registres sont

des préalables pour une mise en œuvre effective des législations définies dans les politiques de lutte.

Par la suite, d'autres précautions comme les cyber- patrouilles vont être menées ainsi que des mises en demeure de retrait. Ces actions sont préventives.

En effet, elles peuvent être perçues comme des sanctions dans la mesure où elles interviennent avant même la commission des infractions par les délinquants. Dans cette hypothèse, ces mesures techniques empêcheront les délinquants de commettre leurs actes. Ces actes sont dès lors de tentative ou souvent d'infraction préliminaire à d'autres actes répréhensibles. A titre d'illustration, les pédophiles qui se connectent à des sites dans l'optique de faire des propositions indécentes à des mineurs pourront être pris certes en flagrant délit sur internet. Mais l'acte fondamental pour lequel ils ont effectué cette connexion ne pourra pas être commis s'ils sont appréhendés à la suite de la conversation via internet avec le mineur interlocuteur (qui est dans le cadre des *cyber patrouilles* un agent de gendarmerie connecté sous un faux pseudonyme et se faisant passer pour un mineur).

Dans une autre hypothèse, il est possible de percevoir l'aspect coercitif de la *cyber patrouille* avec les gendarmes. Ceux-ci sont avertis grâce aux signalements de certaines connexions à destination de mineurs exclusivement, par certains internautes. Ces mesures ont, entre autres, pour but de constituer des preuves grâce aux connexions et adresses repérées. L'illustration de la pédopornographie paraît simple mais est-ce le cas des autres infractions ?

La pédopornographie est un excellent exemple pour montrer que prendre des dispositions en amont est efficace. Mais dans certaines autres hypothèses, les cybercriminels installent des logiciels sur des postes de manière à désactiver les connexions illégales dès l'instant où les officiers de la gendarmerie ou tous autres agents spécialisés dans le domaine numérique parviennent à détecter ces activités anormales sur les réseaux numériques. Cette pratique des cybercriminels est un frein à l'efficacité de l'action de terrain menée par les agents en charge de la lutte contre les réseaux criminels. Quelles mesures sont mises en œuvre dans ces cas ?

Enfin, la question se pose de savoir en quoi les cyber patrouilles réussissent le mieux dans la lutte contre le fléau ? A la suite des cyber patrouilles, des mises en demeure de retrait sont effectuées et des actes de cryptologie sont mis en place. Qu'en est-il réellement de ces pratiques au plan de la coercition effective ?

§1- Les précautions particulières de prévention

Par précautions particulières, il faut comprendre toutes les dispositions pratiques mises en place afin d'éviter la commission des infractions cybercriminelles. Il faut inclure dans cet ensemble, les opérations techniques réalisées en vue d'empêcher la commission d'attaques informatiques ou tout autre dérivé. Il s'agit des opérations d'adressage de noms de domaine (A) mais aussi des mesures directement installées sur les outils informatiques et les réseaux (B) et enfin de l'éducation des individus (C) compte tenu de l'apparente prise de conscience quasi-nulle des internautes.

A- Les opérations d'adressage

Les opérations d'adressage concernent les abonnements de téléphone mais également d'internet (a). Il s'agit également des noms de domaines, qui nécessitent une intervention spécifique d'organismes de certification et d'enregistrement (b).

a- L'adressage des abonnés téléphoniques et internet

C'est dans ce cadre notamment que la CNIL impose aux utilisateurs de bases de données de publicité ou de marketing de procéder à des déclarations préalables des diverses utilisations et surtout des personnes concernées par ces usages.

C'est dans ce même esprit qu'il est possible de considérer que la lutte contre la cybercriminalité est enclenchée en Côte-d'Ivoire. En effet, les réseaux de téléphonie mobile sont plus en vogue et plus utilisés que les réseaux internet. Or, cette branche de la communication est aussi touchée par les menaces cybercriminelles, les piratages et autres méfaits sont exercés au moyen ou à partir des outils et les technologies de l'information et de la communication. C'est pourquoi une vaste opération d'identification des abonnés de service de téléphonie mobile mais aussi utilisateurs d'internet a été lancée. C'est surtout la traçabilité qui a rendu utile cette identification des abonnés. Cette initiative est l'œuvre du ministère des postes et des technologies. Ce ministère s'est assigné pour

objectif d'identifier les utilisateurs et les usagers afin de faciliter les éventuelles recherches mais surtout de mettre fin aux actes impunis comme le « broutage [551]», les escroqueries via internet.

Cette vaste opération a pour objectif d'assurer la traçabilité des puces de téléphonie mobile. A ce stade, il convient de faire des précisions : le niveau d'implantation des réseaux numériques est moins développé que celui de la téléphonie. Si bien qu'il y a plus d'utilisateurs de mobiles que de services internet en ligne ou via l'ADSL. Par ailleurs, il existe un réel problème d'état civil non seulement dans les administrations publiques mais également dans les habitudes commerciales du secteur privé. Il découle de ces deux facteurs qu'il n'est pas automatique (contrairement aux Etats européens) pour un vendeur de se préoccuper de l'identité de celui qui se procure une puce de téléphone. Cet échange est plus proche de l'achat de cigarettes par un fumeur pressé. Or, le fait pour un revendeur de puces téléphoniques de remettre contre paiement et sans aucune précision sur l'identité de l'acheteur, ne facilite pas la remontée vers cet utilisateur en cas de problème.

L'ensemble de ces précisions permet de prendre conscience de l'importance d'opérations comme la traçabilité exigée par l'Agence des Télécommunications de Côte-d'Ivoire (ATCI). Cette opération peut s'analyser en une base essentielle de la lutte.

A cette procédure est combinée la mise en place d'un répertoire des cybercafés, qui sont désormais tenus de s'identifier d'une part et d'autre part de dresser une liste de leurs clients quotidiens.

Ces deux meures constituent une innovation colossale dans la lutte contre la cybercriminalité en Afrique de l'ouest. Les autorités ont de la sorte décidé de prendre le problème à *bras le corps* et surtout de trouver des solutions pratiques adéquates et adaptées au fléau cybercriminel.

b- L'adressage des noms de domaine

[551] Le broutage est le terme ivoirien pour désigner les fraudes bancaires via les réseaux numériques.

Le nom de domaine est une base de données dont l'un des principaux objectifs est de se décentraliser[552].

Le fait d'exiger une tenue de registres journaliers par les gérants des cybercafés facilitera la création d'adresse IP par utilisateurs. Cette technique n'existait pas auparavant et les brouteurs ou autres pirates se faufilaient en toute quiétude après la commission de leurs forfaits. Le Commandant DJAHA, en poste au CENTIF a souligné[553] l'utilité de cette identification : la traçabilité mais surtout l'adressage pour répertorier les utilisateurs des différents réseaux. Des adresses IP pourront ainsi être établies et permettront de retrouver en cas de recherches les personnes connectées à un moment précis. D'une manière plus précise, une adresse IP, norme américaine, est le lien par lequel l'ordinateur communique. Elle est délivrée par le Dynamic Host Control (ou Configuration) Protocol (DHCP), qui lui, est le serveur. Cette attribution se fait soit manuellement, soit automatiquement. L'adresse est dite « dynamique » pour les postes de travail d'une entreprise notamment et, ce, parce qu'elle change au bout d'un certain temps. Elle peut également être dite « statique » et c'est le cas des adresses IP des serveurs. Le DHCP a un nombre limité d'adresses IPv4 qu'il peut délivrer. Il faut savoir qu'il existe deux catégories d'adresse IP : l'adresse IPv4 et l'adresse IPv6. L'adresse IPv4 est actuellement saturée parce qu'elle est épuisée d'un point de vue de la diffusion. Elle couvre toutes les opérations via internet. L'adresse IPv6 a été créée à la suite de la saturation des adresses IPv4.

Pour prévenir des actes de cybercriminalité (ou mieux les éviter) tout l'ensemble décrit par le DHCP et l'adresse IP doivent être sécurisés. En clair, le serveur et les adresses qu'il diffuse doivent être protégés puisqu'ils peuvent faire l'objet d'intrusion et servir les actes de cybercriminalité. Il faut intégrer des alertes dans les architectures de supervision

[552] Cf. ALBITZ Paul et LIU Cricket traduction de Giles CARRÉ, DNS et BIND, Adminstration système et réseau, O'Reilly & Associates, 4ème edition, Paris 2001.

de chaque système d'information des entreprises. Ces alertes permettent de dénoncer automatiquement les intrusions dès qu'il y en a.

Au niveau de l'Afrique, l'adressage des noms de domaine reste encore un vaste chantier.

En effet, l'ICANN a des représentants au niveau de chaque continent et pour ce qui est de l'Afrique, plusieurs organismes comme l'African Regional At Large organisation (AFRALO) et l'AFRINIC interviennent.

L'attribution des noms de domaines aussi bien pour les particuliers que pour les entreprises et les administrations n'est pas tout à fait bien organisée au niveau de l'Afrique. Le secteur est encore en défriche, le contrôle n'y est pas encore tout à fait installé puisqu'à l'heure actuelle, seuls 5 registraires sont réellement accrédités pour procéder à l'enregistrement des noms de domaines. La raison à cet état de l'adressage des noms de domaine est la date de la prise de décision tardive de l'Union Africaine quant à l'instauration d'un nom de domaine exclusivement dédié à l'Afrique *.africa* ou dotafricat, en avril 2012 lors du Sommet sur l'Innovation à Addis-Abeba.

Il faut éclaircir la question des adressages des noms de domaine au niveau du continent africain et en rendre le contrôle possible pour en faciliter la gestion. Si ces exigences ne sont pas remplies, il devient impossible de résoudre les questions de répartition et de sécurisation des systèmes. Les normes de generic top- Level Domain (gTLD) sont-elles appliquées ? Et si oui, les conditions d'attribution des noms de domaine sont-elles un gage de sécurité quand on observe la multiplicité des noms de domaines à l'origine des mails frauduleux ou des mails créés spécifiquement pour commettre des infractions cybercriminelles en bande organisée ?

Les noms de domaine en Afrique de l'Ouest connaissent plusieurs niveaux à assainir : la répartition des rôles entre registraires, registrar et registry. *Un Registry est une organisation responsable de la gestion d'un domaine de niveau supérieur*[554]. Le *registraire (registrar en anglais) ou bureau d'enregistrement* a en charge de réaliser

[554] Cf. ALBITZ Paul et LIU Cricket traduction de Giles CARRÉ, DNS et BIND, Adminstration système et réseau, O'Reilly & Associates, 4ème edition, Paris 2001.

l'interface entre le registry et le client c'est-à-dire qu'il se charge de l'enregistrement de domaine et fournit des services. Par exemple, Network Solution Inc. Est un registry exclusif et un registraire pour les domaines .com, .net, .org et .edu.

Plusieurs niveaux pour les noms de domaine, les premières catégories (et il y en a sept) sont les noms de domaine de premier niveau[555] : .com (pour les activités commerciales), .edu (pour l'éducation), .gov (pour les gouvernements), .int (pour les institutions internationales), .mil (pour les militaires), .org (pour les organisations) et .net.

Les secondes catégories de domaine sont les Country Code Top Level Domain (ccTLD) ou les noms de domaines utilisant les codes des pays. Il s'agira par exemple de .ng pour le Nigéria et enfin, la dernière catégorie est constituée par les generic Top level domain (gTLD) ou nom de domaine générique.

Où en est-on- concrètement au niveau de l'Afrique ?

Beaucoup d'hésitations et de tâtonnements. A l'heure actuelle, les pays d'Afrique s'organisent pour établir une politique autour de la question des noms de domaine. Pour l'instant, une coordination n'est pas encore trouvée quant à la régulation de ce secteur. Certains pays sont plus organisés que d'autres. C'est l'exemple du Nigéria où la Nigerian Nigerian Internet Registration Association (NIRA) instituée en 2005 se charge de la gestion des noms de domaine.

L'attaque du système informatique des studios *SONY pictures*[556] a contribué à empêcher la diffusion dans les salles obscures[557] du film de Seth Rogen et Evan Goldberg, intitulé « The Interview » traduit en français *l'interview qui tue* »[558] produit par l'enseigne américain SONY attendu au cinéma en France le 11 février 2015 et prévu aux Etat- Unis à Noël 2014.

---

[555] Cf. **DREYFUS N.**, Marque et internet, protection, valorisation, défense, collection A Lamy Axe droit, Wolter Kluwer, France 2011.

[556] Voir : http://rue89.nouvelobs.com/2014/12/22/affaire-sony-kim-jong-est-tigre-papier-256694;

[557] C'est à dire le cinéma

[558] Le film a pour sujet Kim Jung-un, le maître de Pyongyang.

En effet, les cybercriminels (en cause) ont menacé SONY Pictures de représailles si SONY pictures diffuse ce film ayant pour sujet Kim Jung-un, le maître de Pyongyang, une région de la Corée du Nord. La localisation pourrait très bien être changée pour l'Afrique, où il n'y a que 5 registraires en charge de l'adressage des noms de domaine. Ce type d'attaque devrait inciter à accélérer la mise en place rapide d'une attribution contrôlée et mieux gérée des noms de domaine en Afrique. L'objectif étant d'éviter la répétition de telles infractions d'envergure internationale.

En plus des opérations d'adressage, les mesures techniques directes sont des précautions particulières à prendre en compte.

B- Les mesures techniques directes

Les mesures dont il est question sont dites directes parce qu'elles interviennent sur les supports pouvant être menacés de risque de contournement des droits des auteurs. Elles sont opérées également sur les plateformes de commission des infractions comme la cyber pédophilie et d'autres infractions dont l'appréhension nécessite une intervention ponctuelle pour en assurer le succès. Ces mesures particulière sont la gestion des droits numériques ou Digital Rights Management en abrégé DRM (a) ou le recours aux cyberpatrouilles (b). A côté de ces moyens légaux techniques employés, il existe les assurances, autre mesures techniques de prévention qu'il convient d'adjoindre aux deux premières (c).

a- Les Digital Rights Management

Les Digital Rights Management (DRM) constituent la Gestion des Droits numériques.

Ce sont des mesures de protection et sont considérées comme étant efficaces dès lors qu'elles sont un moyen de contrôle des contenus par leurs propriétaires via des codes d'accès d'une part. D'autre part, ces DRM constituent des outils de blocage des contenus relativement aux personnes tierces c'est-à-dire autre que les auteurs[559].

[559] cf. Circulaire de la DACG nº 2007-1/g3 du 3 janvier 2007 jusd0730001c présentant et commentant les dispositions pénales de la loi nº 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins

C'est la loi du 1er août 2006[560] qui a permis de transposer la directive de 2001 protégeant ces mesures. Plusieurs dispositions protectrices sont contenues dans cette loi notamment pour l'encadrement de ces mesures techniques. A titre d'illustration, des peines délictuelles ont été prévues aux nouveaux articles du code de la propriété intellectuelle (articles 22, 23 et 29 de la loi) L. 335-3-1 et L. 335-3-2 pour les droits d'auteur, L. 335-4-1 et L. 335-4-2 pour les droits voisins, L. 342-3-1 et L. 342-3-2 pour les bases de données[561], afin de réprimer :

1° Toute importation, fabrication ou activité de diffusion ou de promotion en faveur de procédés technologiques conçus ou spécialement adaptés pour porter atteinte à une mesure technique de protection ou à un dispositif d'information sur le régime des droits (six mois d'emprisonnement et 30 000 euros d'amende - L.335-3-1 II et L. 335-3-2 II pour les droits d'auteur/L. 335-4-1 II et L. 335-4-2 II pour les droits voisins/L. 342-3-1 et L. 342-3-2 pour les bases de données) ;

2° Toute importation ou distribution d'œuvres dont un élément d'information relatif au régime des droits a été supprimé ou modifié dans le but de porter atteinte à un droit d'auteur ou à un droit voisin, de dissimuler ou de faciliter une telle atteinte (même peine - L. 335-3-2 III pour les droits d'auteur/L. 335-4-2 III pour les droits voisins/L. 342-3-2 pour les bases de données) ;

3° L'atteinte portée aux mesures techniques de protection ou aux dispositifs d'information sur le régime des droits, par une intervention personnelle réalisée autrement que par l'usage de moyens déjà existants conçus ou spécialement adaptés à cette fin (amende de 3 750 euros - L. 335-3-1 I et L. 335-3-2 I pour les droits d'auteur/L.

---

dans la société de l'information et d'action publique dans le domaine de la lutte contre les atteintes à la propriété intellectuelle au moyen des nouvelles technologies informatiques, publié au bulletin officiel du ministère de la justice nº 2007-1 du 28 février 2007.

[560] Loi nº 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information et d'action publique dans le domaine de la lutte contre les atteintes à la propriété intellectuelle au moyen des nouvelles technologies informatiques, publiée au JORF du 03 Août 2006.

[561] Les bases de données sont définies à l'article L. 112-3 al. 2 du Code de la Propriété Intellectuelle comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen »

35-4-1 I et L. 335-4-2 I pour les droits voisins/L. 342-3-1 et L. 342-3-2 pour les bases de données).

Les DRM servent à protéger des données enregistrées sur des supports CD et DVD.

Ils peuvent également couvrir des données diffusées par le réseau à condition que la diffusion passe par un chiffrement et des signatures[562]. Ce qui renvoie aux techniques de cryptographie.

Etymologiquement, *crypto* vient du grec *kruptein* et signifie caché[563]. La cryptographie est un code graphique déchiffrable par l'émetteur et le destinataire seulement[564]. Il s'agit surtout d'une technique d'encodage par l'intermédiaire de codes mathématiques[565] et chiffrés. La technique est vieille d'avant les guerres mondiales dans la mesure où elle était déjà employée dans l'art militaire[566]. En droit français, la loi pour la confiance dans l'économie numérique[567] définit en son article 29 la cryptologie comme « *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'information ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ils garantissent la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité*». Cette définition complétée trouve ses origines dans le Guide

---

[562] cf. **BLOCH L.** et **WOLFHUGEL C.**, Sécurité informatique : principes, méthodes à l'usage des DSI, RSSI et administrations, 3è édition, Eyrolles, Paris, 2011

[563] cf. Dictionnaire le Robert, p. 400

[564] idem.

[565] **BECKETT Brian**, Introduction aux méthodes de la cryptologie traduit de l'anglais par Philippe Béguin, Philippe Klein et Éric Hénault, publié à Paris, Milan, Barcelone : Masson, collection Logique, mathématiques, informatique, 1990. **BENSOUSSAN Alain** et **LE ROUX Yves** dans « Cryptologie et signature électronique mentionne que la technique a été développée dans les années 1920 par les Hollandais avec la machine Enigma, machine utilisée par les nazis durant la seconde guerre mondiale, cf. p.13 de l'ouvrage.

[566]Cf. **JOSSE Henri** (Marie-Léopold-Henri), la cryptologie et ses applications à l'art militaire, Paris : L. Baudoin, 1885.

[567] Loi LCEN, loi n° 2004-575 du 21 juin 2004, op.cit.

pratique élaboré par le Service central de la sécurité des systèmes d'information (SCSSI) et le Secrétariat d'Etat à l'Industrie[568].

Les mesures de cryptographie, sont propres aux droits d'auteurs. Elles sont des moyens de protéger mais constituent également des gages de contournements des actes éventuels de cybercriminalité. Elles permettent de contrôler l'usage des bases de données, des supports lorsqu'ils sont utilisés.

En plus de constituer des outils de protection, les Digital Rights Management sont une sanction indirecte. Ce sont des espèces de filtres qui acceptent ou refusent l'accès des internautes selon leur qualité d'auteur (ayant accès) ou non (à qui l'accès est refusé). Cet outil revêt dès lors la double fonction de protection et de sanction.

Le bémol est que l'usage des chiffrements qu'exige leur diffusion peut constituer un frein à leur efficacité.

C'est pourquoi dans des domaines plus sensibles comme la protection des mineurs d'autres moyens techniques directs seront utilisés. Il s'agit des cyber-patrouilles organisées par les gendarmes d'une manière générale.

b- Les cyber-patrouilles

Les cyberpatrouilles consistent dans des filatures virtuelles sur Internet par des gendarmes de la Division de lutte contre la cybercriminalité.

Les cyber patrouilles interviennent sous plusieurs formes et consistent dans une surveillance des sites par des spécialistes de la police et de la gendarmerie.

Il est question pour des analystes, des spécialistes en *monitoring*[569], des juristes de filtrer les contenus des sites présents sur la toile. Le Plateau d'Investigations Cybercriminalité

[568]Cf. Guide pratique élaboré par le Service central de la sécurité des systèmes d'information (SCSSI) et le Secrétariat d'Etat à l'Industrie La règlementation française en matière de cryptologie, juin 1998.

[569]Le monitoring est selon le Centre National de Ressources Textuelles et Lexicales, l'ensemble de techniques permettant d'analyser, de contrôler, de surveiller soit, en électronique, la qualité d'un enregistrement, soit, en médecine, les réactions physiopathologiques d'un patient, disponible en ligne : http://www.cnrtl.fr/definition/monitoring

et Analyses Numériques (PICyAN) du Pôle Judiciaire de la Gendarmerie a en charge les investigations sous pseudonymes. Il s'agit de surveillance des sites de manière générale en fonction de la gravité et de la sensibilité des infractions. D'un point de vue criminalistique, cette structure réalise à la demande des magistrats ou des juges d'instruction ou des juges des libertés et de la détention des expertises et des examens techniques relatifs à la preuve électronique notamment.

A titre d'illustration, en France, le ministère des Finances (les Douanes et les services de la Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes (DGCCRF) sont organisés pour repérer quotidiennement des produits illégalement proposés à la vente sur internet. Il s'agit là du domaine de la contrefaçon en ligne[570].

La pédopornographie est un autre domaine dans lequel les agents de la gendarmerie infiltrent les sites, forums de discussion réseaux, blogs. En effet, ils se font passer pour des enfants, l'objectif étant de démasquer les prédateurs. Cette couverture est employée par plusieurs (220 enquêteurs) agents de la gendarmerie du service.

Les services de gendarmerie dédiés à ces activités sont dotés de structures permettant d'analyser les images qu'ils reçoivent mais également les autres contenus. C'est la tâche confiée au Centre d'Analyse d'Images Pédopornographiques (CNAIP)[571].

Il faut souligner que c'est conjointement que gendarmerie et police travaillent. Plusieurs services sont affectés à cette tâche et sont précisés par le code de procédure pénale, par le décret n°2005-274 du 24 mars 2005 portant organisation générale de la gendarmerie nationale[572], et par l'arrêté du 30 mars 2009[573]. Il s'agit des offices centraux de police

[571]cf. Circulaire interministérielle n° CRIM-2010-7/E6 du 22 mars 2010 relative aux investigations sous pseudonyme sur Internet et au rôle du centre national d'analyse des images de pédopornographie, Bulletin Officiel du Ministère de la Justice, Loi n° 2010-02 du 30 avril 2010.

[572] Cf. Décret n° 2005-274 du 24 mars 2005 portant organisation générale de la gendarmerie nationale, JORF n°72 du 26 mars 2005 page 5123 texte n° 16.

[573] Cf. Arrêté du 30 mars 2009 relatif à la répression de certaines formes de criminalité informatique et à la lutte contre la pédopornographie, JORF n°0078 du 2 avril 2009 page 5818 texte n° 5.

judiciaire (office central pour la répression des violence aux personnes, office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, à l'office central pour la répression de la traite des êtres humains, office central pour la répression de trafic illicite des stupéfiants), du service technique de la recherches judiciaires et de la documentation de la gendarmerie nationale, des directions interrégionales et régionales de la police judiciaire et des services de recherches de la gendarmerie nationale.

Quel que soit le service concerné, les dispositions pratiques s'accompagnent de plusieurs mesures dont les mises en demeure de retrait.

Les mesures de retrait sont effectuées à la suite de perquisitions des officiers de police judiciaire. Elles peuvent être opérées via des injonctions délivrées à la suite d'avertissements restés sans réponse de la part des cybercriminels.

A côté de ces mises en demeure de retrait il peut être procédé à des opérations de cryptographie. En ce qui concerne ces dernières, la loi française octroie ce pouvoir uniquement aux institutions étatiques et par conséquent, il est strictement interdit aux particuliers de procéder à des cryptages de leurs échanges par exemple.

En quoi ces opérations sont-elles des sanctions de la cybercriminalité et quelle est la portée de telles coercitions ?

Les mesures de retrait comme les actes de cryptographies sont des préliminaires techniques mis en place pour prévenir la coercition qui pourrait succéder à un acte cybercriminel.

Les cyberpatrouilles et les mesures de retrait sont des prétextes pour signaler l'importance des systèmes d'information d'une manière générale. C'est la protection même des systèmes d'information d'une manière globale qui doit être recherchée et assurée. C'est pourquoi, la protection des systèmes d'information en France par exemple a été érigée en point d'intérêt privilégié de sécurité nationale. Et c'est dans le livre blanc

de la Défense[574] que les pouvoirs publics civils et militaires ont souligné cet aspect fondamental. En clair, la cyber sécurité est en amont de la protection des systèmes d'information et permet ainsi d'assurer la sécurité du cyberespace de l'Etat, et par ricochet des citoyens. Le fait pour les autorités militaires et étatiques d'insister sur la cyber-sécurité comme composante de la sécurité nationale est symptomatique des différentes actualités vécues. Les Etats ont été attaqués via leurs systèmes d'information (exemple de l'Estonie qui a été le premier été attaqué de manière directe en 2007 en matière de cybercriminalité). Les récentes affaires liées aux virus informatiques *Stuxnet* paralysant des centrales nucléaires d'Uranium, les écoutes généralisées ou des affaires d'espionnage industriels et informatiques, sont des cas réels qui traduisent l'importance de la protection des systèmes d'information. La responsabilité de l'Etat est dès lors engagée ou à engager[575].

A l'instar des pratiques publiques légales, se développent d'autres moyens préventifs qu'on pourrait qualifier de privé du fait de leur champ de compétence : il s'agit des assurances. Les assurances sont un gage à exploiter.

c- Les assurances comme mesure préventive

Les assurances se développent dans tous les domaines et il serait curieux de voir qu'elles sont absentes dans un domaine aussi sensible que la prévention contre la cybercriminalité. Qu'est-ce qu'une assurance et comment la définir dans le cadre de la cybercriminalité ? Que couvre-t-elle ? Peut-elle être efficiente dans ce secteur ?

Le dictionnaire définit l'assurance comme le contrat par lequel un assureur garantit à l'assuré, moyennant une prime ou une cotisation, le paiement d'une somme convenue en

[574]Le livre Blanc de la Défense sur la cyber sécurité, cf. : http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf. Voir également le communiqué de presse de l'ANSSI sous le lien suivant : http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/la-cybersecurite-au-coeur-du-nouveau-livre-blanc-sur-la-defense-et-la-securite.html

[575] Comme le soulignent **O. KEMPF** et ses coauteurs **DOSSE S. et MALIS C.** dans l'ouvrage collectif, le cyberespace: nouveau domaine de la pensée stratégique Centre de recherche des écoles de Coëtquidan Alliance géostratégique, 2013 lorsqu'ils relèvent la question de l'engagement de la responsabilité conjointe de l'Etat et de ses concitoyens dans des cas de cybercriminalité comme celui dont a eu à connaître l'Estonie en 2007.

cas de réalisation d'un risque déterminé[576]. Dans tous les domaines faisant intervenir le risque, comme la santé, la vie quotidienne, le véhicule, les individus personnes privées comme les entreprises, personnes morales, quel que soit le secteur d'activité prennent des assurances. Le secteur de la sécurité informatique n'échappe pas à cette habitude de se prémunir surtout avec les risques réels liés aux pertes de données, ainsi qu'activités sur internet et notamment la cybercriminalité.

Ainsi, les Directions de Systèmes d'Information, dans toutes les sociétés prennent le soin de prévoir des lignes couvrant non seulement le matériel informatique mais aussi les systèmes complets d'information contre la cybercriminalité. Si la cybercriminalité expose des risques aux entreprises, aux particuliers et aux administrations, force est de reconnaître que ces risques ont simplement mué. En effet, dès 1990, dans sa thèse sur la contribution à l'identification des risques informatiques et à la proposition des méthodologies de correction, Monsieur RAOUH relève le problème de la maîtrise des risques liés à l'informatique. Il propose déjà la coordination effective des connaissances en informatiques, des savoirs techniques et du domaine des assurances afin de mieux proposer des correctifs aux dommages liés aux systèmes d'information pris dans leur ensemble[577]. Le marché du risque numérique n'est pas nouveau en soi mais les évolutions technologiques survenues depuis favorisent la complexité des dommages à couvrir et à indemniser. C'est donc un marché avec de nouvelles attentes, qui se développe pour les entreprises de prestation d'assurance. Dans le domaine de la santé par exemple, il est conseillé aux hôpitaux de prendre des assurances dans cette optique préventive afin de pallier les éventuelles pertes de données ou de fausses communications de dossiers de patients. A ce propos, le dossier médical personnalisé relance la question des assurances dans la prévention des éventuelles dérives de l'usage d'internet par les établissements publics et privés de santé.

---

[576] Cf. Dictionnaire Le Robert, p. 103.

[577] Cf. **RAOUH D.**, Contribution à la recherche sur l'identification, la typologie, la problématique et les méthodologies correctives des erreurs en matière de risques informatiques : application au problème de l'assurance, Université de Paris 2, 12 juillet 1990 sous la direction de M. J. DONIO.

D'une manière générale dans le domaine des assurances, c'est le risque numérique qui sera couvert par les sociétés d'assurances. Quel est le contenu de ce concept ? Par risque numérique, la plupart des services commencent par proposer aux entreprises des prestations leur permettant d'évaluer les degrés d'exposition aux délits informatiques. C'est l'affaire SONY de 2011[578] qui est à l'origine de la diffusion des offres d'assurance couvrant les risques numériques. Les faits de l'espèce sont relatifs au piratage des logiciels SONY via des sites britanniques. En effet, le hacker GeoHot HOTZ a réussi à contourner, en ligne, des mesures techniques de protection du *jeu Plastation* Network 3 créé par la firme japonaise SONY. Il met en place une méthode de ce contournement et le publie via un site internet en libre accès au public. Le but de la manœuvre étant de permettre un téléchargement gratuit de la version de la PSN. L'entreprise SONY saisit dès lors la justice américaine et obtient en 2011 une ordonnance restrictive à l'encontre du hacker. Par cette ordonnance du 1er Mars 2011, le Juge ordonne au hacker de « livrer à Sony l'intégralité des informations demandées à savoir tous les logs de serveurs, les adresses IP, le informations sur les comptes utilisateurs, l'enregistrement des accès aux comptes, aux applications et aux formulaires d'enregistrement ainsi que toute autre information permettant d'identifier des personnes ou des machines ayant accédé ou téléchargé des fichiers hébergés en rapport avec www.geohot.com, mais également le fichier geohot.com/jailbreak.zip. Les conséquences du piratage des données d'une entreprise par des hackers ne se limitent pas aux retombées économiques sur cette dernière. En effet, les utilisateurs des services ou clients (comme c'est le cas pour l'entreprise SONY) de cette enseigne se retrouvent lésés. En témoigne la publication des données dérobées comme les données bancaires sur des sites publics et mis en vente libre dans les réseaux de cybercriminels ou autres contrefacteurs et détourneurs de fonds[579]. On comprend dès lors l'inquiétude des utilisateurs ou des titulaires de compte de PSN en ligne de s'attaquer à SONY du fait de cette défaillance technique. D'ailleurs, la sanction de la part de la justice britannique traduit la gravité d'une telle défaillance de la part de la

[578] Cf. Sony Computer Entertainement America LLC v Hotzn et al. Case n° C-11-00167 SI (N. D. Cal), United States District of Court Northern District of California Courtroom A, 15th Floor.

[579] Cf. **S. FALLETIN**, Le piratage de Sony touche les données bancaires, Le figaro du 03 mai 2011.

firme japonaise : SONY est condamnée à verser une amende de 290 000 £ soit presque 300000 euros du fait de ce piratage, qui selon l'Information Commissioner's Office aurait pu être évité si SONY avait mis en place suffisamment de garanties techniques[580]. Pour pallier à ce type de risque, plusieurs organismes d'assurance réfléchissent à des polices d'assurance adaptées aux nouvelles technologies.

En guise d'illustration, l'année 2013 en France a été l'occasion pour des grands groupes comme AON, AXA et AGCS de lancer leurs produits contre la cybercriminalité à leurs clients[581].

Le risque numérique a fait l'objet d'un rapport du sénat[582] en France présenté par Messiers Bruno SIDO, sénateur, et Jean-Yves LE DÉAUT, en date du 26 juin 2013. Le rapport ROBERT émet plusieurs recommandations s'agissant de la cybercriminalité comme par exemple, la protection des internautes.

Les moyens de prévention contre la cybercriminalité exigent également une communication accrue en direction des populations non seulement sur les usages des moyens de télécommunication et d'internet, mais une véritable éducation sur les risques liés à la cybercriminalité doit être faite.

C- L'éducation des populations

En matière de cybercriminalité, le mot victime fait souvent penser aux victimes de cyber-pédopornographie et donc indirectement aux enfants. Il faut souligner en ce qui

---

[580] Cf. **Julien L**, *Sony légèrement sanctionné en Angleterre pour le piratage de PSN*, Magazine Numerama du 24 janvier 2013.

[581] Cf. **BAUME Thomas**, « Aon diagnostique les risques liés à la cybercriminalité pour les risk-managers » publié le 09 octobre 2013 et « Axa Corporate Solutions dévoile le volet assurance de son offre cyber » mis en ligne le 18 octobre 2013 sur le même site : *http://www.argusdelassurance.com/cybercriminalite/*. Pour compléter la version cyberassurance, le groupe Allianz propose un contrat Cyber Protect couvrant les sites, les liens en plus du matériel informatique, cf. : https://www.allianz.ch/public/fr/a_notre_propos/espace_media/communiques_de_presse/communiques_de_presse_2013/05.09.13_cyber_protect.html

[582] Cf. Le risque numérique : en prendre conscience pour mieux le maîtriser, Rapport n° 721 (2012-2013) de MM. **Bruno SIDO**, sénateur et **Jean-Yves LE DÉAUT**, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 3 juillet 2013.

concerne le traitement de la cybercriminalité par l'éducation, que la Commission européenne a initié en 1999 un plan d'action Safer Internet. Il a pris la forme d'un programme pluriannuel grâce à la décision 854/2005/CE du Parlement européen du 11 mai 2005 instituant un programme pluriannuel visant à promouvoir une utilisation plus sûre de l'internet et des nouvelles technologies en ligne. Ce programme a pour objectif d'encadrer les enfants mais également les parents dans l'utilisation qu'ils font de l'Internet. Il s'étend de l'ordinateur à d'autres supports comme les jeux vidéo. Aujourd'hui ce programme prend la forme d'espace dédié aux jeunes. Sont ainsi organisés des espaces d'expression, des campagnes de sensibilisation, des ateliers. Pour consulter le site dédié aux activités des jeunes dans ce cadre, il est possible de regarder l'adresse suivante : http://www.saferinternet.fr/.

Certes, les enfants font partie des premières victimes mais ce ne sont pas les plus nombreux. Ils arrivent loin derrière les victimes de fraude de cartes bancaire ou même des victimes d'usurpation d'identité. En effet, la pratique permet d'observer que les intrusions dans les systèmes informatiques et les usurpations d'identité facilitent énormément les vols de données bancaires. De ce fait, il serait intéressant en terme de prévention à ces risques d'éduquer les potentiels victimes et les rendre plus responsables notamment dans l'utilisation des informations personnelles ou même des données susceptibles de faire l'objet d'actes cybercriminels.

Cela peut paraître anodin pour l'ensemble des populations mais le simple fait de retirer de l'argent au distributeur automatique de billets et de jeter dans la rue, par la suite le reçu imprimé du distributeur est un acte qui pourra facilement servir les intérêts de n'importe quel pirate, ou voleur de données ou tout autre cybercriminel.

L'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP) a établi son 7ème rapport en 2011[583]. Ce document a permis à ses auteurs après une analyse de la jurisprudence de souligner la rareté des sanctions prononcées par les juges en matière cybercriminelle d'une part, et d'autre part le niveau insuffisant de ces

sanctions. Les auteurs du rapport, membres de l'INHESJ et de l'ONDRP en ont déduit qu'il faut une autre approche de la répression de la cybercriminalité. Ils préconisent de sécuriser davantage l'identité numérique grâce à une généralisation de l'usage des certificats individuels, à la formation en amont des services de justice, qui seraient alors des services bien plus spécialisés du fait des formations des utilisateurs et à une responsabilisation des acteurs du secteur.

Au titre des pratiques entreprises par les internautes victimes d'arnaques, ou d'autres actes cybercriminels du même type, il faut spécifier l'organisation des victimes pour éviter que les actes concernés se reproduisent[584].

En effet, il est frustrant pour des victimes d'actes cybercriminels de se rendre compte qu'elles n'ont aucun moyen d'action que la plainte déposée auprès des services de police. Hormis l'attente des actes de procédure qui vont suivre le dépôt des plaintes (notamment les actes d'enquête et l'arrivée d'autres plaintes concernant les mêmes acteurs), les victimes se retrouvent impuissantes. C'est pour lutter contre l'impunité des cybercriminels que certaines victimes s'érigent en justiciers avec la création de sites parallèle aux sites escrocs en ligne. Ces sites sont souvent des forums organisés soit pour expliquer davantage les processus d'arnaques en ligne, soit pour prévenir soit encore pour contrecarrer les plans de ces cybercriminels.

Ces initiatives de la part des victimes ne sont pas légales dans la mesure où elles ne sont encadrées par aucun texte législatif. Le fait de créer un faux site pour que les cybercriminels se livrent en communiquant avec ses concepteurs permet aux initiateurs d'obtenir des adresses électroniques des cybercriminels puis les mots de passe correspondant.

C'est une technique utilisée par une victime qui a créé un site dans ce but. La manœuvre facilite l'intrusion dans ces boîtes mails afin de détecter des arnaques commis ou encore celles qui se préparent. La technique pourrait s'analyser en une pratique frauduleuse car

la concernée, la victime, qui s'érige en justicier des victimes de telles attaques, n'a d'une part aucune qualité (elle n'est pas désignée par loi, encore moins policiers spécialiste en matière de cybercriminalité) pour le faire et d'autre part, elle commet une infraction au sens de l'intrusion frauduleuse qui est une infraction passible de prison. En outre, on pourrait arguer qu'elle viole le principe du respect de la vie privée.

Bien que cette pratique et l'ensemble des initiatives dans ce sens emportent la critique sur le plan juridique et l'encadrement, elles sont efficaces et évitent dans certains cas à des potentielles victimes de tomber dans les pièges des cybercriminels. Elles facilitent dans une certaine mesure la rééducation des internautes notamment les consommateurs qui achètent fréquemment sur les sites de ventes en ligne.

A l'inverse, les victimes justicières, ne sont pas à l'abri de menaces de mort et cela favorise un autre type de criminalité à la solde de la lutte contre la cybercriminalité.

Un autre aspect de l'éducation des populations mais également des entreprises passe par les code de conduite. Ces ouvrages de référence ou guide sont des supports d'éducation et surtout des bases d'exemples plus concrets. Leur usage est d'une utilité remarquable. Ces supports sont souvent désignés comme des chartes de bonne conduite des entreprises face à l'usage des technologies de l'information et de la communication.

A côté des entreprises et des administrations, les familles et les foyers sont éduquer autrement à utiliser ces technologies. Ainsi, grâce au décret du 8 décembre 2013, est créée la Délégation aux usages de l'internet qui a pour rôle d'éduquer les familles, les foyers démunis à se servir intelligemment des réseaux informatiques[585].

Au niveau des entreprises encore, la pédagogie des salariés est un travail à effectuer par les responsables informatiques.

En Afrique de l'Ouest par exemple, ce n'est souvent pas de mauvais augure qu'une personne en possession d'un ordinateur de bureau (sur son lieu de travail) utilise

[585] Nouvelle entité relevée par le Rapport Robert du 16 février 2014 sur la lutte contre la cybercriminalité, Rapport présentée au Sénat : cf. http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

ce dernier à des fins personnelles. C'est le contexte d'un salarié qui utilise le matériel informatique de l'entreprise pour des aides matérielles de proches (par exemple aider à lire une clé USB personnelle pour en extraire ou imprimer des documents) sans intention de nuire. Ce comportement qui paraît dépourvu de toute intention d'infiltrer un système informatique et surtout accompli dans l'ignorance est un moyen de compromettre la sécurité du système informatique de l'entreprise. C'est pourquoi à tous les niveaux des salariés dans les entreprises et dans les administrations, un code de conduite doit être enseigné.

En outre, la sécurité informatique dans les entreprises inquiète également. Cette inquiétude revêt une importance capitale puisqu'il ne faut pas exclure les intrusions informatiques du fait des connexions anarchiques des salariés. Ces connexions sans aucun rapport avec les taches professionnelles sont des portes d'entrée des cybercriminels dans les systèmes informatiques des entreprises concernées. De ce fait, le niveau de sécurité des systèmes informatiques peut constituer un frein à la coercition des cybercriminels.

En somme, la protection par les moyens techniques contre la prolifération des actes cybercriminels découle également des comportements et des habitudes des internautes aussi bien dans leur vie quotidienne domestique que professionnelle. C'est pourquoi les bonnes pratiques professionnelles doivent être associées à l'éducation des populations face à l'utilisation des réseaux numériques.

L'ensemble des précautions prises en amont permet par la suite d'évaluer ou de mesurer l'efficacité des protections et des sanctions techniques édictées pour l'hypothèse où des actes cybercriminels seraient commis.

§2 : L'efficacité des sanctions techniques

Les sanctions techniques sont constituées par l'ensemble des opérations réalisées soit à distance soit directement sur les ordinateurs ou les supports contenant des données. Il sera de ce fait question pour les agents de police ou de gendarmerie de procéder à des filtrages, à de l'infiltration mais aussi à des méthodes préventives et pédagogiques.

Ces mesures peuvent prendre d'autres tournures plus audacieuses par l'intéressement des cybercriminels eux-mêmes. Il s'agira à cet effet de faire d'eux les nouveaux acteurs de la lutte contre le fléau cybercriminel.

Au titre de l'efficacité des sanctions techniques, il faut souligner la standardisation via les normes aussi bien de sécurité que de protection. D'un autre côté, on peut également relever le fait que les institutions européenne et internationale aient recours aux experts, quels que soient les domaines de compétence. Par le passé, les juges avaient recours à des dires d'experts pour fonder leur décision notamment dans des domaines techniques comme celui de l'informatique. Désormais, l'habitude devient systématique : le recours à des experts non pas uniquement par les juges mais également par les institutions comme le Conseil de l'Europe ou même l'Union européenne.

La rédaction des rapports, de guides de bonnes pratiques, des recommandations traduit l'expertise qui se développe en la matière tant pour les moyens de lutte que pour les techniques de protection contre les attaques. C'est pourquoi, le filtrage et l'infiltration des systèmes informatiques sont des techniques à coupler pour une efficacité des sanctions en matière de répression de la cybercriminalité (A).

D'autres mesures nécessaires et indispensables relèvent aussi de l'expertise dans la matière : il s'agit des preuves. Les preuves sont particulièrement délicates à manier en matière informatique dans la mesure où elles sont susceptibles pour la plupart d'être virtuelles même si certaines restent matérielles. C'est pourquoi, elles exigent une acuité en ce qui concerne leur collecte mais également leur traitement. D'ailleurs, elles sont encadrées par les textes de loi (B).

A- Le filtrage et l'infiltration

Le filtrage et l'infiltration sont des mesures techniques mises en place dans le cadre de la sécurisation des réseaux informatiques en général et pour les services internet en particulier. Pris uniquement, le filtrage ne suffit pas d'où sa remise en cause (a). Pour être efficace, il est complété par une autre mesure qu'est l'infiltration dans les systèmes informatiques concernés (b).

a- La remise en cause du filtrage pris uniquement

L'une des premières mesures de la Loi LOPPSI a été d'insérer dans le code pénal un article destiné à régir la technique du filtrage sur internet. L'objectif de cette technique étant de bloquer l'accès des sites diffusant des images et des contenus pédophiles. Elle prévoit la modification de l'article 6 de la loi pour la confiance dans l'économie numérique de 2004 pour y insérer les mentions suivantes : « *lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant des dispositions de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux fournisseurs d'accès à internet les adresses internet des services de communication au public en ligne entrant dans les prévisions de cet article et auxquelles ces personnes doivent empêcher l'accès sans délai*». Il découle de cette disposition que le filtrage nécessite une décision de l'autorité administrative. Il s'agit en réalité d'une autorisation qu'accordent la Commission Nationale d'Informatique et Libertés en ce qui concerne la France.

Le filtrage n'est donc pas une mesure automatique qui se met en place ipso facto ou en raison de téléchargements intempestifs par exemple. Cette technique semble être une solution aux pratiques illégales sur internet mais elle est remise en cause. Il convient de s'interroger sur les raisons.

Dans sa décision Scarlett du 24 novembre 2010, la Cour de Justice de l'Union Européenne remet en cause la technique du filtrage préventif et général des communications en vue de lutter contre les téléchargements illicites de fichiers[586]. A la suite de cette décision des auteurs ont pu écrire que le filtrage en lui seul ne suffit pas. Il faudrait y adjoindre d'autres pratiques voire lutter autrement conte les infractions commises via internet. Parmi ces auteurs, monsieur Bigot suggère d'allier l'ICANN à la lutte afin de dépolluer internet à la source.

Mais en quoi consiste cette technique de protection ?

A son évocation, le terme du filtrage semble être une technique simple de filtre d'internet. Il n'en est pourtant rien. En effet, le filtrage recouvre un ensemble de mesures

[586] Arrêt Scarlett c. Sabam, 3e chambre CJUE, 24 novembre 2011, Affaire C 70/10.

techniques complexes. C'est un moyen de contrôle technique[587] qui emprunte plusieurs formes[588].

Le filtrage se fait par la technique de liste noire dont le contenu est filtré. C'est le filtrage des pages web. C'est la technique de la *block- list*. A ce jour aucune institution nationale n'a encore d'habilité à générer les listes noires. Mais EUROPOL et INTERPOL sont actifs en la matière.

Le filtrage peut encore passer par le canal d'une identification automatique. Il s'agit alors d'une analyse automatique des contenus, des images, des textes ou des vidéos cibles et ce en utilisant des logiciels modernes sophistiqués.

Le filtrage peut enfin être réalisé par système de classification (Rasting System). Cette technique a pour appui une classification des contenus internet, faite de manière individuelle ou par une tierce partie. Dans une étude réalisée par des spécialistes de la question en Europe, il a pu être démontré que le filtrage est facilement contournable, d'où la nécessité de l'associer à d'autres options techniques comme l'infiltration.

Il faut souligner que le filtrage fait référence à la surveillance du réseau d'une manière générale par le fournisseur d'accès. L'article 15 §1 de la directive « commerce électronique » interdit d'obliger le Fournisseur d'accès Internet (FAI) à se livrer à une surveillance de communications. C'est sur ce fondement que l'Union européenne refuse un filtrage général. La raison évoquée c'est que le filtrage est à l'encontre du respect des données personnelles. En effet, filtrer le réseau de manière générale sans restriction reviendrait à incorporer dans cette surveillance tous les contenus, tous les échanges et toutes les connexions qu'ils soient licites ou non. Or, cette optique nuirait indubitablement au respect des données des personnes abonnées sur ledit réseau. C'est en

---

[587] Par exemple, la technique du contrôle parental est une forme de filtrage pour éviter l'accès des enfants à des contenus illicites comme des sites pornographiques.

[588] Cf. la note n° CERTA-2005-INF-006 du 10 janvier 2006 du CERTA dans laquelle le centre gouvernemental de veille d'alertes et de réponse aux attaques informatiques détaille les techniques et les différentes formes de filtrages avec leurs avantages et inconvénients. La note est consultable en ligne : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001

illustration de cette donne que la Cour de Justice de l'Union européenne a refusé un filtrage général dans un arrêt l'Oréal II de la Grande Chambre en date du 12 juillet 2011[589]. En effet, dans cet arrêt, les faits sont relatifs à plusieurs ventes des produits de marque L'Oréal constatées par l'enseigne via différents sites européens d'eBay sans l'accord de l'Oréal. S'estimant victime de contrefaçons, l'Oréal a assigné EBay devant les tribunaux. C'est l'enseigne anglaise qui a été traduite en justice. C'est à la suite des investigations de la High Court of Justice du Royaume Uni que plusieurs précisions factuelles ont été apportées. Parmi elles, la plus importante est le fait que eBay ait fait installer des filtres sur les mots clés afin de constate qu'eBay a installé des filtres *afin d'identifier les annonces qui pourraient contrevenir aux conditions d'utilisation du site*.

Quelques mois après cette décision, la Cour rend un autre arrêt Scarlett contre Sabam le 24 novembre 2011 précisant que le filtrage général va à l'encontre de la liberté d'entreprise des fournisseurs d'accès internet. Dans le cadre de cette affaire, un litige oppose la société Scarlet Extended SA, un fournisseur d'accès internet, à Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) La Scarlet Extended SA propose des prestations d'accès à internet à ses clients sans autre service du type téléchargement. Dans cet objectif, elle est sollicitée par la SABAM de mettre en place un système de filtrage des communications électroniques au moyen de logiciels d'échange d'archives (dits «peer-to-peer»), afin d'empêcher l'échange des fichiers portant atteinte aux droits d'auteur. La société Scarlet refuse et la SABAM la fait citer devant la justice en vue de faire analyser la faisabilité de cette requête au regard des différentes directives européennes à savoir la directive 2000/31 dite directive sur le commerce électronique» [590], la directive 2001/29 du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société

---

[589] Cf. Cour de justice de l'Union européenne Grande chambre Arrêt du 12 juillet 2011, L'Oréal et autres / eBay international et autres, Affaire C-324/09, publiée au Recueil de jurisprudence 2011 page I-06011.

[590] Cf. Directive du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») publiée au JO L 178, p. 1

de l'information[591], la directive 2004/48 du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle[592], la directive 95/46 du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[593] et la directive 2002/58 dite directive vie privée et communications électroniques[594]. Devant le juge, ces dernières méritent une interprétation afin de savoir si elles autorisent le filtrage généralisé des communications électroniques pour empêcher les téléchargements illicites portant atteinte aux droits d'auteur, principalement d'œuvres musicales.

En analysant la décision, il ressort que le filtrage limité en temps et en portée est toléré. Le filtrage général n'est pas toléré par la Cour européenne de justice[595]. Dans une décision opposant la société *Netlog* à la société SABAM, la Cour de Justice a confirmé sa décision dans un arrêt du 16 février 2012[596] en estimant que *la mise en place d'un dispositif de filtrage général sur le contenu de la plateforme de Netlog serait disproportionnée.*

Le filtrage en tant que technique répressive des fraudes informatiques est selon les tenants de cette thèse un frein à la liberté d'expression et constitue une violation de la vie privée en ce qu'il obligerait les fournisseurs d'accès internet à passer en revue sans tri de ce qui serait illicite et licite de l'ensemble des communications et échanges.

---

[591] Cf. Directive du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information publiée JO L 167, p. 10.

[592] Cf. Directive du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle publiée au JO L 157, p. 45, et rectificatif JO L 195, p. 16.

[593] Cf. Directive du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données publiée au JO L 281, p. 31.

[594] Cf. Directive du Parlement européen et du Conseil, du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques publiée au JO L 201, p. 37.

[595] Cf. Arrêt Scarlett c. SABAM, CJUE du 24 novembre 2011, aff. C 70/10.

[596] Cf. Arrêt Netlog c. SABAM, CJUE du 16 février 2012, aff. C C-360/10

D'un autre côté, le filtrage est remis en cause dans la mesure où il semble ne pas suffire dès lors qu'il est effectué sans but précis. C'est pourquoi il est couplé à des pratiques comme l'infiltration. Il est alors question de parler de complémentarité des deux techniques.

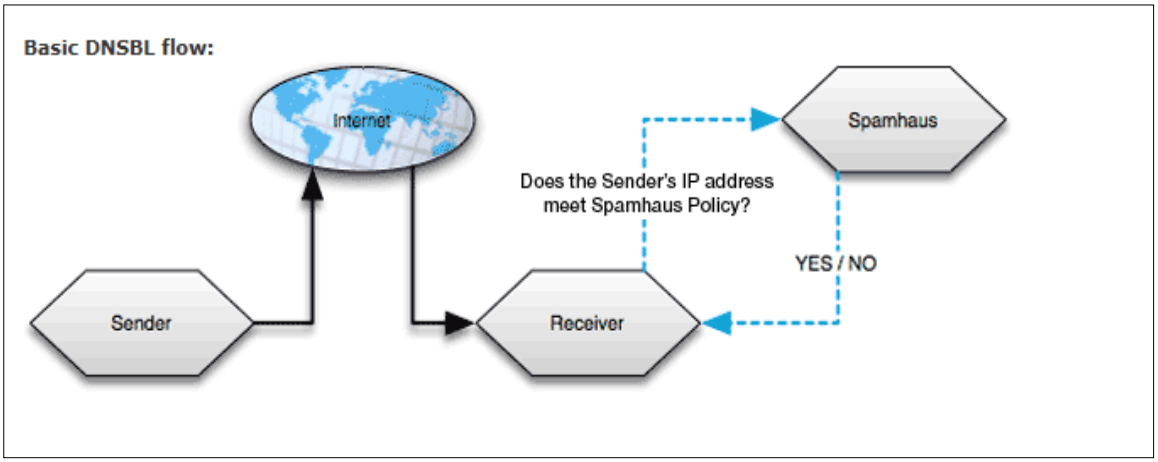
b- La nécessaire complémentarité du filtrage et de l'infiltration

En matière d'infiltration, il convient non seulement de considérer les infiltrations organisées par les agents ou officiers de police ou de gendarmerie en charge des infractions informatiques ou spécifiques d'une part et d'autre part les infiltrations déguisées opérées par des organismes privées comme le Spamhaus par exemple.

S'agissant des opérations d'infiltration du fait de la police ou de la gendarmerie, elles sont encadrées par les codes pénaux et de procédure pénale. C'est dans ce cadre que le code de procédure pénale français définit l'opération d'infiltration à l'article 706-81 en ces termes « *l'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs…* ». L'article 706-83 précise que l'infiltration est autorisée par écrit et spécialement motivée. Il ressort de ce second texte que l'infiltration n'est pas le principe pour les infractions d'une manière générale. Elle est une opération exceptionnelle. Mais en cas de cybercriminalité, peut-on en dire autant vu la complexité des opérations effectuées pour parvenir à appréhender des cybercriminels notamment le démantèlement des réseaux mis en place via les voies numériques ?

En ce qui concerne les organismes privés, le cas de spamhaus permet de souligner la part contributive d'institutions autres qu'étatique dans la lutte contre les infractions contenues dans la cybercriminalité. En l'espèce, qu'est-ce que le Spamhaus et quelle infraction particulière prévient-il ?

Le Spamhaus est fondé en 1998 et basé à Genève et à Londres. Cet organisation non gouvernementale intervient dans dix pays et a pour but de lutter contre les courriers indésirables. Pour ce faire, le Spamhaus est composé de spécialistes inforensiques[597], d'enquêteurs et d'ingénieurs informatiques. Il travaille en collaboration avec le FBI et le National Cyber-Forensics and Training Alliance. Son mode opératoire est de filtrer les mails reçus dans les boîtes mails des structures ou entreprises qui ont souscrit à ses abonnements. Le Spamhaus opère ainsi une traque contre les groupes de spammeurs et les vers malveillants à travers le monde. Le schéma suivant explique le mécanisme de base d'envoi d'un mail. C'est sur la base de ce système que Spamhaus opère le de filtrage de mails reçus.



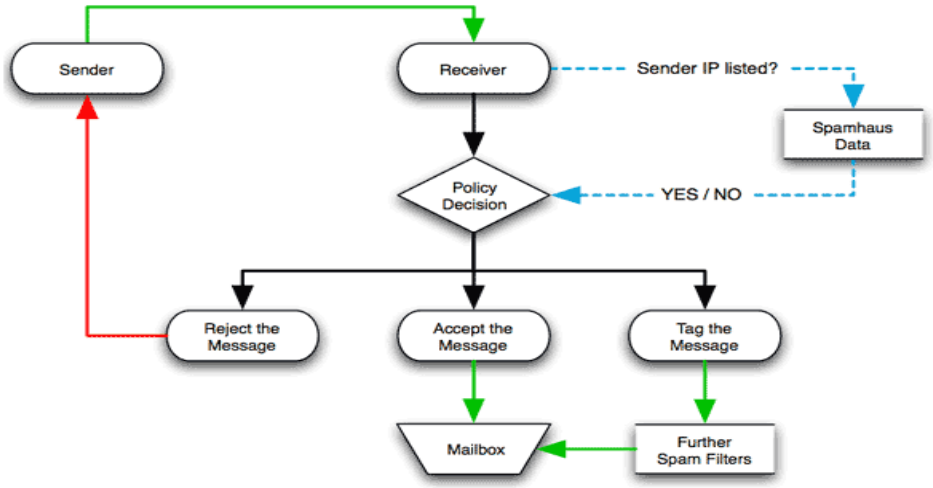
Cette illustration provient du site officiel du Spamhaus[598].

En fonction des standards compatibles ou non des mails envoyés, le mail sera reçu ou bloqué par le destinataire qui aura adhéré aux conditions de protection de *Spamhaus*. Ce sont ces standards qui déterminent de la nature de désirable ou d'indésirable du mail

[597] C'est-à-dire d'informatique légale : voir SANG, Fernand Lone, NICOMETTE, Vincent, et DESWARTE, Yves. Attaques par entrée-sortie et contremesures. *Actes de la Journée Sécurité des Systèmes & Sureté des Logiciels (3SL)*, p. 11-13.

[598] Cf. http://www.spamhaus.org

envoyé. Le schéma suivant en est l'illustration exacte : il décrit le processus d'acceptation ou de refus des mails non sollicités dans la boîte de courriels du destinataire, adhérent au système de protection *Spamhaus*.



Il faut adhérer au système de protection de Spamhaus Project pour bénéficier de la protection accordée et pour que sa boîte mail soit filtrée. Il est permis de parler d'infiltration puisqu'il ne peut y avoir filtrage sur une boîte mail que si cette dernière est en partie contrôlée (ou gérée pour le tri des mails) par l'organisme en charge de son nettoyage ou encore du classement en mail indésirable ou non des divers courriels envoyés. L'adhésion est ouverte aussi bien aux particuliers qu'aux professionnels. Le consentement est d'une certaine manière sollicité plusieurs fois : par exemple, le filtrage de base n'est opéré que parce que le propriétaire de la boîte mail a adhéré au système du Spamhaus Project. C'est la première étape de consentement. La seconde étape intervient au moment où un message est reçu et que la boîte mail destinatrice est par exemple saturée, le message est alors *tagué* c'est-à-dire estampillé d'une marque particulière le classant automatiquement dans la catégorie de courrier indésirable à moins que le propriétaire ne l'accepte et n'en fasse un courrier désiré.

Les techniques d'infiltration et de filtrage sont des pratiques spécifiques mais la preuve revêt une importance capitale en matière d'infraction. La cybercriminalité n'échappe pas à cette règle procédurale pénale fondamentale.

B- L'importance des preuves

La collecte des preuves en matière de cybercriminalité est délicate mais importante. En effet, ce sont les preuves qui permettront d'établir la réalité des faits dont sont accusées les personnes appréhendées par les services de police ou de gendarmerie en charge de lutte contre la cybercriminalité.

Le domaine des supports numériques étant affranchi de la matérialité des données, il est tout à fait aisé de modifier ou d'altérer les preuves récoltées. C'est en ce sens que la Commission européenne a mis en place le projet C-TOSE (Cyber-Tools On-Line Search for Evidence). Ce projet établit une procédure particulière de récolte des preuves en la matière.

Une fois les supports de preuve collectés, ils devront être analysés ou traités afin d'en tirer le maximum d'informations pour prouver ou désapprouver les actes cybercriminels. Il existe une science spécifique à ce domaine de traitement des preuves : c'est l'inforensique.

L'importance des preuves en matière de cybercriminalité exige de connaître cette science précise dans la mesure où elle est un pilier de ce domaine particulier.

Le droit s'est adapté à la collecte des éléments probants dans le domaine informatique. De ce fait, des moyens spécifiques comme la signature électronique, les certificats électroniques ou encore les techniques de cryptage sont utilisés[599].

Il convient d'appréhender également d'autres supports susceptibles d'être pris en compte au titre des éléments de preuve. C'est toute la question des vidéosurveillances, des empreintes génétiques et de tout autre moyen capable d'éclairer sur des faits cybercriminels aussi bien pour le juge que pour les autorités en charge des enquêtes.

Dès lors, les techniques de collecte de preuves, leur encadrement juridique ainsi que les acteurs qui interviennent, révèleront l'importance de la preuve qu'elle soit numérique ou autre.

---

[599] Cf. **A. HOLLANDE et X. LINANT DE BELLEFOND**, Pratique du droit de l'informatique et de l'Internet, 6e édition Delmas, Toulouse, Septembre 2008.

a- Les techniques de collecte

Pour réprimer des criminels sur le fondement d'une décision de justice suppose de rassembler des preuves attestant de la commission des actes qui leur sont reprochés. Dans le cas de la cybercriminalité, il s'agit d'actes commis soit sur des fichiers, soit sur des logiciels ou encore sur des réseaux ou des outils informatiques.

C'est pourquoi les preuves rapportées seront des connexions retraçant les chemins d'accès aux sites ou aux moyens de communication piratés, des adresses IP retrouvées avec des traces des actes commis notamment des horaires et les attaques effectuées. Il pourrait également s'agir de mails échangés ou de codes secrets « craqués ».

L'ensemble de ces éléments techniques collectés obéit à un traitement particulier selon les textes de lois.

C'est dans ce cadre que l'article 20 de la Convention de Budapest dispose relativement à la collecte en temps réel des données relatives au trafic que : « *chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à collecter ou enregistre par l'application de moyens techniques existant sur son territoire er à obliger les fournisseurs de service, dans le cadre de ses capacités techniques existantes (…)*». Cet article montre que la convention accorde certes une importance à la production des preuves mais il souligne surtout la latitude laissée aux Etats de tenir compte de leur niveau d'avancement technologique quant à l'établissement des preuves des infractions en matière de cybercriminalité.

La **directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999** sur un cadre communautaire pour les signatures électroniques[600] encadre les transactions électroniques. Elle a été prise en application des nouveaux moyens de preuve notamment la preuve électronique. Il faut ajouter que plusieurs moyens de preuve peuvent servir de supports. Il s'agit des vidéoconférences (puisque ce sont des captations d'images et de sons) utilisant la voie des multimédias, les empreintes laissées mais également et surtout des preuves en lien direct avec les supports informatiques. A ce titre, la technique de la

[600] J.O.C.E., n° L 013 du 19 janvier 2000, p. 12 et s.

signature électronique et des certifications se classent sous cette directive quant à leur régime juridique.

La signature électronique obéit à divers processus de sécurité et par conséquent, en matière de cybercriminalité, elle n'est pas un aspect négligeable. C'est même l'un des points saillants de la sécurité informatique.

1-La signature électronique

Elle est encadrée la **Directive 2003/511/CE du Parlement européen et du Conseil du 14 juillet 2003** relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/511/CE du Parlement et du Conseil du 13 décembre 1999[601]. La signature électronique est une forme de preuve mais est également un moyen de protection des actes accomplis via des supports informatiques.

Selon la directive, elle emprunte deux formes à savoir d'une part la signature électronique simple c'est-à-dire celle émise par les techniciens et la signature électronique avancée d'autre part, émise par les juristes. A différence entre ces deux formes est que la première ne présente aucune dimension juridique puisqu'elle est totalement dépersonnalisée, tout ordinateur pouvant la réaliser. A l'inverse, que la seconde est déterminée par le droit interne[602]. Il faut souligner qu'en dépit du fait que la signature électronique simple ne revête pas pleinement de dimension juridique, elle constitue un fait juridique et peut dès lors être utilisée comme moyen de preuve ; c'est pourquoi l'article 5 de la directive mentionne cette catégorie de signature.

S'agissant de la signature électronique avancée, la directive européenne exige plusieurs caractéristiques que sont : son lien uniquement au signataire, le fait qu'elle permette d'identifier ce dernier, sa création par des moyens que le signataire puisse garder sous son contrôle exclusif et enfin la signature électronique avancée doit être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données

[601] J.O.C.E., n° L. 175 du 15 juillet 2003, p. 45

[602] Cf. **PIETTE-COUDOL Thierry**, La signature électronique, éditions Litec, Paris, 2001, p. 3

soit détectable. Ces critères sont contenus dans l'article 2 de la directive sur la signature électronique. Ces critères cumulatifs favorisent une authentification et une vérification de l'auteur de la signature. C'est un moyen de personnaliser les signatures et ainsi de mettre fin aux signatures génériques créées par un ordinateur ou des robots informatiques comme ça peut être souvent le cas pour la signature électronique simple.

2-Le certificat électronique

Qu'est-ce qu'une certification ? Quels intérêts présente-t-elle en matière de preuve surtout pour la cybercriminalité ?

La certification peut se définir comme un procédé de signature électronique qui consiste à signer numériquement un message en ajoutant à une signature numérique une clé publique. Plus clairement, le certificat est délivré par un prestataire de certificat électronique habilité à cet effet. Le décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par es produits et les systèmes des technologies de l'information[603] encadre les conditions d'agrément des prestataires de certification. Madame Feral-Schuhl précise que ce certificat est en quelque sorte la carte d'identité électronique qui accompagne le message électronique et qui permet d'établir un lien entre la personne et sa signature électronique[604].

Le premier intérêt lorsque la certification accompagne un message électronique, c'est de laisser subsister des traces tangibles des échanges entre les interlocuteurs[605].

Le second intérêt de ce mécanisme est d'assurer l'impartialité de celui qui établit l'élément de preuve. Aucun des interlocuteurs n'est directement l'auteur du certificat électronique ; c'est en effet le prestataire de certification qui le fait. Et il en découle une égalité des parties en cas de litige.

---

[603] Décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par es produits et les systèmes des technologies de l'information publié au JO 19 avril 2002, p. 6944.

[604]Cf. **FERAL-SCHUHL C.**, Cyberdroit, le droit à l'épreuve de l'internet, 6e éditions DALLOZ, 2010, p. 706.

[605] Cf. **OUATTARA Aboudramane**, la preuve électronique, étude de droit comparé Afrique, Europe, Canada, collection horizons juridiques africains, éditions PUAM, 2011, p. 130

A côté de la certification des produits technologiques, existe la certification des entreprises et plus précisément la certification des sites internet des entreprises. Ce mécanisme n'existe pas réellement en Europe mais un dispositif l'encadrant est en réflexion notamment en Allemagne avec la *Datenschutzauditgesetz*[606]. C'est un label selon lequel l'entreprise agirait en conformité avec la loi de protection des données à caractère personnel En France, à l'heure actuelle, il n'existe de trace de cet encadrement que dans le code de la consommation.

Les normes informatiques sont un autre moyen de collecte des preuves en matière de preuve dans les infractions cybercriminelles. Qu'en-est-il réellement ?

3- Les normes informatiques

Les normes sont définies comme : « un document qui définit des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services » [607]. Elles sont d'une manière générale élaborées par l'Organisation Internationale de Normalisation, appelée ISO[608]. Elle se compose de plusieurs experts issus d'organismes nationaux et qui réfléchissent à la mise en place des spécifications techniques de pointe adéquates et adaptées dans divers secteurs de l'économie et de la technologie mondiale. L'informatique n'échappe pas à cette règle. C'est dans ce cadre que des normes informatiques sont établies au plan mondial.

Il en existe plusieurs et les principales normes informatiques internationales sont les normes dites internationales ISO-27035, les normes de réseau, et les normes 27001 pour les services de support et les Datacenter.

---

[606] Cf. **KOSSI A. V.,** La protection des données à caractère personnel à l'ère de l'Internet, impact sur l'évolution du cadre normatif et nouveaux enjeux, Etat des lieux en France et en Allemagne.

[607] Cf. http://www.iso.org/iso/fr/home/standards.htm

[608] ISO vient du grec *Isos* qui signifie égal. C'est dans cette optique que les fondateurs de l'ISO ont opté pour cette abréviation à la place de OIN pour Organisation Internationale de la Normalisation : http://www.iso.org/iso/fr/home/about.htm.

La norme ISO-27035 vient remplacer la norme ISO CEI 18044 de 2004 précédemment mise en place. L'avantage de la nouvelle norme de 2011 est de s'adapter à la taille des entreprises quelles qu'elles soient mais elle a surtout le mérite de couvrir la gestion des risques liés aux technologies de l'information, elle comprend des techniques de sécurité et englobe enfin des systèmes de management de la sécurité de l'information[609].

Quant à la norme 27001, elle est réservée au management des systèmes d'information c'est-à-dire les données financières, les documents relatifs à la propriété intellectuelle. Elle sert surtout à gérer les risques de la sécurité de l'information que sont l'intégrité des données et leur confidentialité ainsi que le suivi de leur mise à jour[610].

Les normes informatiques font l'objet d'encadrement au niveau européen afin de garantir la sécurité des transactions et de toutes les opérations par le biais de l'interopérabilité des systèmes d'informations. C'est l'objectif de l'harmonisation des règles juridiques encadrant ces systèmes qui est pris en compte. En réalité ces normes (comme S/MIME) contribuent à crypter des messages en y ajoutant des signatures numériques. En cela, elles sont des clés, des solutions contre les actes des cybercriminels notamment pour les données à caractère personnel dans le domaine des banques ou d'autres échanges aussi importants. Elles permettent en effet de contenir certains abus grâce aux risques évalués. C'est le cas de la norme ISO/IED27005 qui traite la confidentialité dans le cadre de risque pouvant conduire à la perte de confidentialité[611]. Ces normes ne sont pas toujours complètes et suffisantes. C'est pourquoi, d'autres référentiels techniques s'y ajoutent. Par exemple la méthode EBIOS c'est-à-dire Evaluation des Besoins et Identification des

---

[609] Cf. http://www.iso.org/iso/fr/home/standards/management-standards/iso27001.htm

[610] Cf.: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr; voir pour un détail des normes informatiques et leurs liens avec le risque **REFALO P-L**., La sécurité numérique de l'entreprise, l'effet papillon du hacker, Eyrolles, Paris, 2012.

[611] Cf. **REFALO P-L,** précité, p 165.

Objectifs de Sécurité (produite par l'ANSSI) ou encore le référentiel général de sécurité publié par arrêté du Premier ministre[612].

En matière de preuve juridique, elles peuvent très bien être un moyen efficace, à condition que les OPJ ayant recours à ces moyens soient suffisamment formés. C'est le cas en ce qui concerne les officiers des unités spécialisées de lutte contre la cybercriminalité au sein de l'Union Européenne (par illustration, les officiers de l'OCLCTIC ou de la BEFTI)[613].

Si les techniques de collecte paraissent particulières du fait de la technicité du domaine de la cybercriminalité, elles sont encadrées légalement.

b- L'encadrement des preuves numériques

Les preuves numériques sont encadrées aussi bien dans leur collecte que dans leur traitement. Les acteurs habilités à les recueillir doivent dès lors respecter les conditions prévues par les lois et les règlements du droit pénal des preuves.

1- Les conditions de collecte des preuves numériques

Plusieurs acteurs sont habilités par la loi à collecter les preuves en matière numérique. Cette collecte est soumise à diverses exigences légales. Au titre des personnes autorisées, Sont visés non seulement les officiers de police judiciaire qui procèdent à la collecte des preuves mais également les auxiliaires de justice tels les huissiers. Ainsi, dans le cadre d'une procédure d'enquête, les juges de la chambre criminelle de la Cour de cassation ont estimé, dans un arrêt du 5 Janvier 2005 que « *la production des fichiers temporaires retrouvés sur un poste d'ordinateur ne permet pas d'établir une preuve suffisante de l'infraction parce que leur enregistrement est automatique et ne peut donc pas caractériser une intention de copier de la part de la personne poursuivie.* »[614]

---

[612] Cf. Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques publié au JORF n°0113 du 18 mai 2010 page 9152 texte n° 1.

[613] Cf. **Rapport ROBERT** sur la cybercriminalité, de juillet 2014.

[614] Cf. Crim. 5 Janv. 2005, n° 04-82.524, Bull. Crim. n° 176.

Dans le même esprit, la Chambre criminelle estime que les preuves recueillies doivent respecter les garanties d'un procès équitable dans son arrêt du 7 févier 2007[615]. Dans cet arrêt, la chambre criminelle a jugé que : « *constitue une provocation policière, qui rend irrecevables les indices recueillis parce que méconnaissant les garanties du procès équitable et le principe de la loyauté dans la recherche des preuves, le fait, pour un service de police, même étranger, d'offrir aux internautes la connexion à un site pédo-pornographique*».

Il faut souligner que l'application de la Convention Européenne des Droits de l'Homme a considérablement modifié les modes d'administration de la preuve pénale[616]. C'est ce qui ressort des différentes applications notamment les sanctions adressées à la France notamment en matière d'écoutes téléphoniques avec les arrêts KRUSLIN et autres.

Les éléments de preuve recueillis par exemple par des officiers de police judiciaire dans le cadre d'une enquête pour l'usage frauduleux de cartes bancaires obéissent à certaines règles de prélèvement. De la sorte, *la bande magnétique copiée qui aura servi de supports aux vols sur les comptes bancaires ainsi que les cartes usagées trafiquées ou falsifiées dans cet objectif, devront être saisies en possession dudit fraudeur ou de ses complices ou encore à son domicile*.

Sur le point de l'encadrement légal des moyens de preuve, l'arrêté du 21 juin 2011 sur la signature électronique ou numérique en matière pénale modifiant le code de procédure pénale[617] mérite une attention particulière. Il encadre de manière détaillant la sécurité des moyens ou supports utilisés dans le cadre de la signature électronique ou numérique. Il

---

[615] Cf. Crim, 7 févr. 2007, n° 06-87.753, FS-P+F, Cyril C. : Juris-Data n° 2007-037763, décision commentée par **J. BUISSON** dans la Revue internationale de droit pénal, Numéro 3/4 2006 - Volume 77 et Revue Procédure, juin 2007, n°6.

[616] Cf. DELMAS-MARTY, 1992 citée par JOBARD et SCHULZE-ICKING dans l'étude « Les preuves hybrides, étude réalisée par sur l'administration de la preuve pénale en Europe », p. 10.

[617] Cf. Arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale publié au JORF n°0146 du 25 juin 2011 page 10796 texte n° 12.

explicite les conditions d'homologation de la signature électronique utilisée, des organes de certification ainsi que les conditions de l'archivage électronique.

Ces problématiques permettent de s'intéresser au traitement des preuves numériques avec l'*inforensique.*

2- Le traitement des supports de preuve par l'inforensique.

L'inforensique ou analyse forensique ou criminalistique informatique[618] est l'étude ou la pratique relative aux procédés légaux ou à l'argumentation. Il s'agit de l'extraction ou de l'examen des preuves à partir de supports informatiques ou électroniques[619].

Dans son ouvrage Computer Forensic, Robert Newman définit l'inforensique informatique comme le fait pour cette science d'utiliser les technologies digitales informatiques pour développer ou produire des preuves d'investigation en vue de prouver ou désapprouver des allégations[620]. Cette science a essentiellement pour but d'acquérir, de retrouver, de préserver ou de présenter des données fournies ou enregistrées à partir d'un média informatique[621].

L'inforensique permet de garantir la fiabilité des données produites en vue des preuves notamment des actes cybercriminels. Dans ce contexte, la Direction Nationale du Renseignement douanier et des Enquêtes Douanières (DNRED) [622] comporte en son sein une Cellule de Recueil de la Preuve Informatique (CRPI) dont le rôle est de détecter les transactions illicites sur internet pour les transmettre après instruction aux services

---

[618] Cf. **J-P. PASSEMARD**, Cybercriminalité, nouvel enjeu sécuritaire du xxi[e] siècle, in Revue *Sécurité Globale* 2013, n°24, p 59-65.

[619] Pour une définition, voir **FARGEAUD**, Pierre. *La preuve informatique en droit français: les aspects juridiques de l'inforensique*. 2007. Thèse de doctorat. Limoges.

[620] Cf. **NEWMAN (R),** Computer Forensic, Evidence collection and Management, Routledge, 2007, p. 4.

[621] Idem, p. 5.

[622] Cf. la Direction a été créée par l'Arrêté du 29 octobre 2007 portant création d'un service à compétence nationale dénommé " direction nationale du renseignement et des enquêtes douanières, publié au JORF n°270 du 21 novembre 2007, texte n ° 34.

d'enquêtes approfondies[623]. Mais avec les nouvelles problématiques liées au mode de stockage dans les systèmes de *cloud computing*, se posent les questions relatives à la preuve. Comment les officiers de police judiciaire par exemple pourraient procéder à des perquisitions informatiques en présence de données délocalisées et stockées en dehors des Etats de commission des infractions de piratage notamment ou des transferts de fonds liés à des activités de détournement de données informatiques ?

En réponse à cette importante interrogation, l'article de JUHAN Virgile publié au Journal du Net du 1er décembre 2010 relatif à la résolution des affaires de cybercriminalité contient une interview d'un commandant de l'OCLCTIC. Il en ressort en substance que plusieurs moyens sont combinés pour parvenir à la réunion de preuves en cas d'informations ou de traces stockées via le système du cloud computing : les logs de connexion[624] analysés avec les heures de connexion et les images de vidéosurveillance. Tous ces éléments sont des supports qui, jumelés permettent d'établir les preuves numériques.

En dehors de ces recours légaux, la collaboration des cybercriminels comme moyen de répression pourrait être envisageable. Réprimer revient à punir un acte contrevenant les législations pénales en place. Mais sanctionner signifie également trouver des mesures adéquates pour éviter la commission des actes répréhensibles. Quelle pourrait être la portée d'une telle acception en ce qui concerne la cybercriminalité ?

De manière concrète, les nombreuses législations mises en place au sein de l'Union européenne ainsi que les mesures pratiques prises pour punir les cybercriminels arrivent à être contournées de manière continuelle par ces derniers. Il apparaît dès lors que ces délinquants numériques ont une avance technologique considérable sur les agents des structures de police et de gendarmerie. Il y a certainement une autre solution que légiférer et essayer de les capturer ou de les dissuader de commettre leurs forfaits. D'une part, il est possible pour les Etats de concevoir eux- mêmes des systèmes d'exploitation avec des

[623] Cf. Rapport ROBERT du 1er Juillet 2014, p 39 et suivantes.

[624] C'est à dire les identifiant et mot de passé grâce auxquels une personne se connecte à un ordinateur dans un cybercafé par exemple.

moyens de cryptage particuliers. Cette hypothèse a déjà été envisagée et a réellement montré ses limites en pratique. Les failles sont continuellement insérées et les cybercriminels parviennent à pénétrer les systèmes en décryptant les codes secrets et autres combinaisons confidentielles. D'autre part et cette proposition est très délicate à envisager : il faudrait donner la possibilité aux cybercriminels de gérer une plateforme de l'Etat de sorte à les mettre du côté des partisans de la lutte. Il s'agit ici de contrecarrer les plans par la collaboration ou leur contribution à la lutte. Ils changent ainsi de camp et se retrouvent être confrontés à leurs anciens complices délinquants. Cette approche se veut délicate et particulièrement risquée. Elle répond cependant à un objectif de démantèlement des réseaux et des mafias cybercriminels. La collaboration devient dès lors un parfait alibi pour lutter contre la cybercriminalité dans ses racines profondes. D'autres supports ou preuves collectées peuvent permettre d'établir les preuves en matière d'infraction cybercriminelle. Il s'agit des empreintes digitales traitées ultérieurement.

Les empreintes digitales ou encore les images issues des vidéosurveillances sont des supports de preuve facilitant la confrontation des cybercriminels à leurs actes et leurs victimes. S'agissant des empreintes digitales, dès lors que les malfaiteurs sont fichées par les services de police criminelle, il apparaît aisé de retrouver les concernés. La difficulté commence quand ces personnes ne sont inscrites dans aucun fichier des services de police. Dès lors, la technique qui pourrait être de mise est celle des recoupements avec d'autres réseaux notamment mafieux étant entendu que la cybercriminalité est un type de crime commis en bande organisée (c'est une criminalité organisée à l'échelle de la haute technologie).

Toutes les techniques mises en place pour faire la lumière sur les actes cybercriminels sont délicates. Elles sont spécifiques vue la complexité des maniements technologiques et informatiques qui en découlent. C'est ce qui rend la mise en place des moyens techniques de protection spéciaux, en amont. De plus, cette technicité appelle des encadrements législatifs stricts. Or, l'appareil judiciaire accuse toujours un retard par rapport aux activités illicites des cybercriminels.

A côté de toutes les mesures préalables prises par les autorités étatiques la répression impose certes de punir les coupables, responsables d'actes cybercriminels mais elle suppose aussi d'encourager les victimes à travers un soutien psychologique. Cet encouragement peut susciter de la part des victimes la volonté de faciliter le suivi de leurs plaintes notamment. C'est dans ce cadre que l'Union européenne a édicté la Directive 2012/29 UE du Parlement européen et du Conseil du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil[625].

La Directive entre dans le cadre d'une justice réparatrice et a pour vocation générale de permettre à toute victime d'être entendue, de participer à la procédure pénale, de faire valoir ses droits et de pouvoir se faire assister, aider, écouter. Elle garantit les droits fondamentaux et pour ce faire, les Etats membres de l'Union ont jusqu'au 16 novembre 2015 pour la transposer. Cette démarche met l'accent sur le fait que la répression ne suffit pas, encore faut-il permettre aux victimes d'éviter d'être à nouveau des cibles. Dans le cadre de la cybercriminalité cet aspect est important dans la mesure où les conséquences psychologiques des préjudices subies peuvent se répétées. Toutefois la présente directive pèche par son caractère trop général. C'est d'ailleurs ce que souligne le rapport ROBERT lorsqu'il traite de la protection des internautes. Il précise que cette directive ne cible pas suffisamment la cyber-victime. En effet, souligner la particularité des victimes de la cybercriminalité aurait apporté une véritable nouveauté à la directive puisqu'elle vient remplacer une décision cadre, donnant de la sorte une force contraignante à l'ensemble des dispositions qu'elle contient. Sur ce point, il faut espérer que la directive soit révisée et adaptée à la réalité.

Tous ces facteurs sont révélateurs des difficultés qui existent dans la répression de la cybercriminalité. De manière plus précise, de quels ordres sont ces difficultés ? Entachent-elles l'efficacité des sanctions élaborées ?

---

[625] Cf. Directive 2012/29 UE du Parlement européen et du Conseil du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil, publiée au Journal officiel de l'Union européenne, L 315, 14 novembre 2012.

Section 2 : Les difficultés d'une répression efficace

La première difficulté à trouver une répression légale efficace à la cybercriminalité est la technologie en elle-même[626].

En effet, toutes les entités étatiques cherchent à encadrer un espace non limité, et qui répond à une construction sans frontière, d'architecture technologique[627].

En ce qui concerne l'harmonisation des moyens de lutte, elle est une autre source de complication.

L'harmonisation est selon le vocabulaire juridique, l'opération législative consistant à mettre en accord des dispositions d'origine (et souvent de date) différente, plus spécialement à modifier des dispositions existantes afin de les mettre en cohérence avec une réforme nouvelle. Il s'agit d'unifier des ensembles législatifs différents par élaboration d'un droit nouveau empruntant aux uns et aux autres[628].

Il est possible d'ajouter que l'harmonisation est la prédisposition des autorités judiciaires de plusieurs Etats dans un espace géographique considéré, à faire coexister leurs droits nationaux c'est-à-dire à s'entraider entre elles de manière à favoriser l'exercice des compétences respectives[629]. Et l'un des objectifs principaux de l'harmonisation en droit pénal est de lutter contre l'impunité[630].

C'est dire qu'en matière de répression, les législations des Etats de l'Union européenne, doivent aboutir à une coordination des textes réprimant la cybercriminalité. Or, cette

---

[626] Et sur ce point **Nicolas ARPAGIAN** souligne dans son ouvrage sur *la cybersécurité*, les difficultés technologiques (par exemple les différences d'analyses normatives des ordinateurs) et juridiques liées à la lutte contre la cybercriminalité, difficultés perçues dès 1997 par les Etats membres du G8 c'est-à-dire l'Allemagne, le Canada, les Etats-Unis, la France, l'Italie, le Royaume-Uni et la Russie), p. 81 et 82.

[627] C'est dans ce sens que **Thomas SCHULTZ** considère que la contrainte architecturale du cyberespace est technologique, cf. Réguler le commerce électronique par la résolution des litiges en ligne, édition Bruylant, p.348.

[628] Cf. **Gérard CORNU**, Vocabulaire juridique, Association Henri Capitant, P. 503.

[629] Cf. **C. de JACOBET de NOMBEL**, « est-il nécessaire d'harmoniser pour coopérer ? », *in* Juge national, européen et droit pénal, collection Actes et études, p. 11à et s. et également **WEYEMBERGH A.**, Coopération judiciaire pénale.

[630] Idem.

harmonisation suppose une mise au point de chacun des Etats sur ce qui est incriminé par la Convention sur la Cybercriminalité par rapport à la pratique réelle sur le terrain.

Sur un plan international, c'est-à-dire au regard des normes existant déjà en Afrique ou dans des Etats tiers qui échangent notamment des données avec l'Union européenne, il serait intéressant de procéder à un toilettage des textes et des pratiques de lutte. En clair, la contribution de la régulation est importante à la réalisation des objectifs fixés face à la cybercriminalité. Dans cette optique, il faut s'interroger sur les réelles barrières à des incriminations communes ou à des incriminations ayant une base commune.

Qu'est ce qui est le plus efficace en termes de répression ? L'objectif recherché n'est pas d'éliminer ou de supprimer un système existant. Le but à atteindre est de faire reculer considérablement la cybercriminalité, voire l'anéantir. Cela suppose de trouver les obstacles à la régulation utile et adaptée aux mutations sans cesse évolutives de la cybercriminalité. Fort des constats précédents, la première réelle difficulté au niveau des textes est l'harmonisation de la régulation d'une manière générale (§1).

Ces freins émanant des entités étatiques de lutte contre le fléau cybercriminel favorisent d'autres entraves de la part des délinquants. En réalité, les textes non harmonisés, créent un désordre considérable qui joue en faveur des cybercriminels.

De plus, les innovations technologiques sans cesse croissantes s'y ajoutent.

Dans la mesure où les cybercriminels ont constamment une longueur d'avance sur les législateurs et s'adaptent facilement aux évolutions, il se crée un fossé. En cela, cette adaptation rapide contribue à entraver l'efficacité de la lutte contre la cybercriminalité.

A cette complication, s'ajoute la question de la détermination des niveaux de responsabilité en cas d'infractions cybercriminelles. Une fois que les lois incriminent des faits comme faisant partie de la cybercriminalité et par conséquent punissables, les légiférants n'ont pas tout à fait élucidé toute la répression dans la mesure où définir les degrés de responsabilité reste à préciser. Cette complexité s'inscrit au rang des subtilités de la répression de la cybercriminalité (§2).

§1- La difficulté d'harmonisation des incriminations et des peines

La question de l'harmonisation doit être analysée à la lumière des textes fondateurs des espaces communautaires considérés (c'est-à-dire d'une part l'Union Européenne et d'autre part les Etats de l'Afrique de l'Ouest).

La difficile harmonisation des règles répressives de la cybercriminalité prend sa source dans le foisonnement des textes en vigueur au sein de l'Union Européenne d'une part et dans le retard de l'édiction des normes coercitives en Afrique de l'Ouest d'autre part.

Comment s'analyse cette difficulté d'harmonisation ? Pourquoi trouver une lutte commune à la cybercriminalité apparaît impossible ? Les incriminations au sein de la Convention sur la cybercriminalité devraient pourtant permettre aux Etats de légiférer aisément sur la question. Il suffirait d'adapter les textes aux pratiques et aux cultures de chaque Etat. Cette solution n'est pourtant pas une évidence dans la pratique. Quelles sont les justifications d'une telle complication législative favorisant la commission des infractions cybercriminelles ? Si les systèmes pénaux de l'Union européenne sont difficiles à harmoniser comment est abordée la question au niveau de l'Afrique de l'Ouest ?

La régulation est certainement aussi complexe à élaborer sur les deux continents. Ou du moins si le continent européen qui a des avances en la matière n'arrive pas à coordonner ses solutions sera-t-il évident pour les Africains d'organiser leur lutte contre la délinquance numérique ? Ces interrogations nous conduisent à analyser les incriminations de part et d'autre et la pratique qui en découle dans l'optique d'une harmonisation des systèmes pénaux spéciaux. Les problématiques liées à l'harmonisation sont relatives aux difficultés textuelles d'harmonisation (A) mais également aux complications créées par la pratique (B).

A- Les harmonisations législatives

L'harmonisation des sanctions contre la cybercriminalité au sein de l'Union Européenne doit être envisagée à la lecture de l'article 2 du Traité de l'Union Européenne : faut-il une harmonisation générale (et ce, dans ce cas l'harmonisation n'a

pour objet que la convergence des législations des Etats membres de l'Union) ou faut-il préférer une harmonisation infraction par infraction et dans ce cas s'agit-il d'une harmonisation spéciale ?

a- Le choix entre l'harmonisation générale et l'harmonisation spéciale des incriminations

L'harmonisation générale d'un point de vue pénal (puisque la cybercriminalité relève essentiellement de ce domaine) repose pour ce qui est de l'Union européenne sur l'objectif de faire de l'Union un Espace de Sécurité, de Justice et de Liberté[631].

Cet objectif signifie que chaque citoyen européen soit dans un espace qui garantisse à la fois sa sécurité sur tous les plans mais lui permette également de faire valoir ses droits quel que soit l'Etat de l'Union dans lequel il se trouve.

S'agissant de la spécialité de l'harmonisation, il faut prendre les infractions au cas par cas et en définir les éléments de constitution sans disparité d'un Etat à l'autre. C'est en ce sens que BERNARDI considère que les catégories d'infractions sont l'un des facteurs à prendre en compte dans les techniques d' l'harmonisation pénale dans le champ européen[632].

Les difficultés d'harmoniser les incriminations des infractions cybercriminelles résultent de la diversité des cultures juridiques propres aux Etats membres de l'Union Européenne.

1- La diversité des cultures juridiques comme critère de choix

Si certaines infractions sont communes et ont dès lors les mêmes éléments constitutifs, d'autres sont difficilement conciliables. La Convention de Budapest est un premier canevas dans cette perspective. Il n'est certes pas un instrument juridique limité à l'Union européenne mais, il est reconnu par l'Union comme ayant vocation à régir le domaine de la cybercriminalité.

---

[631] L'espace de Justice et de Liberté est l'un des piliers de l'harmonisation pénale au sein de l'Europe et cet objectif est prévu par le programme de Stockholm du 11 décembre 2009, J.O. C 115, 4 mai 2010.

[632] Voir pour les techniques d'harmonisation A. BERNARDI, Stratégies pour une harmonisation des systèmes pénaux européens in Archives de politique criminelle 2002/1 n°24, p.197.

De ce point de vue, les propositions que présente la Convention méritent d'être approfondies au niveau européen dans le sens d'une coordination des différents ordres juridiques.

En outre, l'absence de frontière dans le cyberespace ne facilite pas la détermination des compétences territoriales. A titre d'illustration, quel est le tribunal compétent pour connaître d'une intrusion informatique ?

2- L'absence de frontière dans le cyberespace comme second critère

Le contrôle du cyberespace échappe aux Etats et la casuistique régulière des infractions commises le révèle : il n'est pas toujours aisé de classifier une infraction. Cette classification prend du temps notamment pour remonter les filières par exemple en cas d'interception du site d'une institution d'envergure comme l'OCDE par des pirates sans aucune trace, ni suppression de documents internes.

Les difficultés normatives à réprimer la cybercriminalité sont liées à la conception qu'ont les législateurs du cyberespace (considéré en tant que réseau).

En effet, cet espace est tridimensionnel et les incriminations tant européennes qu'africaines ne rassemblent pas toujours ces trois dimensions. Les réseaux comme le précise Arnaud DUFOUR comportent une partie matérielle (ordinateurs, terminaux, cartes d'interfaces, réseau, câbles etc.), une partie logicielle (applications, programmes de gestion de réseau, de système de sécurité) et une composante « humaine », constituée d'une part de gestionnaires chargés de la mise en œuvre du réseau, d'autre part de clients du réseau, c'est-à-dire des utilisateurs bénéficiaires des services offerts par le réseau.

C'est de cette dimension tridimensionnelle dont doivent tenir compte les Etats pour légiférer quant aux infractions commises dans le cyberespace.

Il découle de l'absence de coordination des textes que les cyber-délinquants en profitent. Ils commettent ainsi des actes en tenant compte de l'incrimination de l'Etat dans lequel ils se trouvent.

Ce qui rend difficile les harmonisations législatives qu'il s'agisse de l'Union Européenne ou de l'Afrique de l'Ouest, ce n'est pas tant l'absence des textes que la difficulté d'adapter les textes incriminant des faits aux cultures juridiques mais plus le

refus d'abandon pour chaque Etat en cause, de sa souveraineté étatique. Or, le droit pénal est par essence un droit souverain. Et la cybercriminalité relève de ce domaine.

Pour résoudre la question, Jean Jacques LAVENUE propose[633] la souveraineté informationnelle : c'est-à-dire « *assurer le contrôle du patrimoine informationnel* ». C'est une prospection qui permet de réaliser que les Etats dits forts sont finalement ceux qui maîtrisent les flux communicationnels ou plutôt les flux d'échanges des informations : quelles informations seront divulguées ? Quelles autres seront tues, cachées, protégées et éviteraient ainsi d'être mises à nue par d'éventuels pirates, en proie de données transitant par les canaux numériques. Loin de copier les Etats totalitaires, la protection des informations, et par conséquent des données semblent obéir à ce principe compte tenu de l'effritement des maillons du cyberespace.

Mais, il faut souligner que tous ces facteurs profitent aux cybercriminels, qui occasionnent le ralentissement des procédures et des enquêtes. Ils emploient dès lors deux pratiques à savoir l'empilage et le forum shopping qui favorisent un ralentissement des procédures en cours ou paralysent les enquêtes menées.

Par l'empilage, le cybercriminel brouille les pistes en ayant recours à des intermédiaires techniques dans divers Etats non coopératifs[634]. Quant au forum shopping, il s'agit d'une pratique empruntée au droit international privée qui consiste pour l'auteur de localiser son acte malfaisant dans un Etat où l'acte n'est pas réprimé. C'est d'ailleurs dans ce cadre que se classent les infractions à caractère raciste qui, outre Atlantique sont couverts par le premier amendement de la Constitution américaine[635].

D'un autre point de vue, la mise en place de législations et leur mise en œuvre prennent du temps. Ce qui pose réellement la difficulté de la répression de la

---

[633] Cf. **LAVENUE J. J**., Cyberespace et droit international: pour un nouveau jus communicationis, *Droit prospectif-Revue de la recherche juridique*, 1996, p. 811-844.

[634] Etats dits non coopératifs dans la mesure où ils n'ont pas signé la convention de lutte contre la cybercriminalité, et par conséquent ne sont pas soumis à cette règlementation.

[635] Cf. 1st Amendement (1791) interdit au Congrès de voter une loi ayant pour but l'établissement d'une religion ou interdisant son libre exercice, ou encore aucune loi contraignant la liberté d'expression, de religion ou de presse.

cybercriminalité c'est l'impossibilité matérielle des textes de loi à s'appliquer aux situations concrètes que posent les cybercriminels. Les législateurs ont tendance à vouloir laisser les juges établir la loi à travers les casuistiques mais dans la mesure où très peu de cas font l'objet de plainte et aboutissent, il devient complexe de créer cette jurisprudence et partant de légiférer à l'issue de la jurisprudence encore en construction.

Parallèlement à l'Union européenne, l'Afrique en générale, et singulièrement l'Afrique de l'Ouest est en phase d'élaboration de sa charpente législative. Elle bénéficie de ce fait, l'expérience européenne dont, elle pourrait tirer des leçons.

Réfléchir à la manière de créer les textes réprimant la cybercriminalité de manière commune paraît profitable à cet espace en construction. C'est l'option choisie puisque l'élaboration du projet de loi quant à l'harmonisation des textes relatifs à la cybercriminalité a fait l'objet d'un sommet des chefs de gouvernements des Etats membres de l'UEMOA en 2010. Ce cap est gardé et a favorisé l'aboutissement de ce projet avec la Convention de l'Union Africaine sur la cyber-sécurité et la protection des données à caractère personnel, adoptée par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014.

Ce nouvel outil juridique élaboré attend d'être transposé dans les différents corpus juridiques des Etats membres de l'Union Africaine. L'efficacité des sanctions édictées et le recul de la cybercriminalité en Afrique de l'ouest en dépendent.

De par sa nature transfrontière, la cybercriminalité exige de la part des Etats de trouver des politiques applicables à cette criminalité organisée. Cette criminalité numérique renferme tous les caractères d'une criminalité organisée : les *brouteurs* ou criminels numériques sont des membres de réseaux de criminels (blanchiment de fonds, fabrication de faux billets, dealers de drogue …) d'une manière générale et ce cas n'est qu'un exemple.

La complexité des infractions cybercriminelles est un aspect qui exige d'harmoniser les textes d'incrimination des actes. Cette complexité rend difficile leur répression.

En effet, ces infractions - et on vise certaines en particulier comme le spam - en génèrent d'autres. Ainsi, les spam générés par les cybercriminels ont pour objectif de favoriser des

processus de blanchiment d'argent. Ce qui conduit à une superposition des faits criminels qu'il faut clairement qualifier. On passe de la génération d'un simple courrier indésirable (infraction contre la communication électronique libre consentie et éclairée) à un crime d'ordre financier qu'est la volonté de dissimuler des fonds frauduleusement acquis.

A côté de la superposition des incriminations à dissocier et à expliciter, la traçabilité de certains actes est également source de difficulté de la répression des actes de cybercriminalité. Dans le système de trading de haute fréquence, cette complication réside dans la délicate traçabilité de toutes les transactions pour séparer les fraudes dissimulées dans le système de la finance légale. Le professeur **Jean-François Gayraud** le souligne dans sa contribution au forum sur la technologie contre le crime[636] en donnant 10 facteurs qui ne facilitent pas la répression des infractions de détournement des codes d'algorithmes.

Parmi ces 10 facteurs, retenons d'abord l'aléatoire découverte des manipulations frauduleuses liées à la structure même du marché du trading de haute fréquence. Sur la question, quelques éclaircissements sont utiles. Daniel GUINIER définit le trading de haute fréquence comme *des programmes qui scrutent les carnets d'ordre en permanence pour confronter l'offre à la demande et calculer le cours d'équilibre du titre*[637]. A la suite de cette définition, l'expert GUINIER dresse une liste des risques liés à la pratique des transactions financières de haute fréquence et parmi ces risques figurent les vulnérabilités liées à la vitesse c'est-à-dire les erreurs nées des fluctuations de signal, ou encore la perte des paquets. Les risques ne sont uniquement techniques dans la mesure où la main humaine représente un danger pour ces transactions. Sont ainsi visés, les traders, les développeurs et terroristes financiers.

---

[636]Cf. **GAYRAUD Jean-François**, Fraudes et manipulations financières : quel avenir pour l'action policière a l'ère du trading de haute fréquence, International Forum on Technologies for a safer World, p 36-44, 8&9 juillet 2013.

[637]Cf. **GUINIER D.**, Contribution du 07 mars 2014 au Forum International de la Cybersécurité publiée en ligne sur http://www.observatoire-fic.com/les-transactions-financieres-a-haute-frequence-thf-problematique-et-securite-par-daniel-guinier-expert-en-cybercriminalite-et-crimes publiée su-financiers-pres-la-cour-penale-internationale-de-la-haye/

Le réel problème du trading de haute fréquence est le manque de contrôle suffisant. Monsieur GUINIER le dit clairement dans son expertise effectuée pour l'observatoire du Forum International de la Cybersécurité (FIC) : il repose *sur des technologies complexes et interconnectées.* Le système de trading de haute fréquence comporte des imperfections (avec des erreurs notamment celles du système de paquets) et des subtilités (complexité des outils utilisés et leur interconnexion) que seuls des experts sont à même de comprendre. Tolérer certains actes à des salariés dans le but d'obtenir des chiffres d'affaires et des taux d'investissement important est source de difficulté de recadrage et de définition des responsabilités en cas de pertes par la suite.

Il faut ensuite mentionner la délicate définition juridique des pratiques illégales en termes d'opération de type trading. En effet, la frontière entre les pratiques dites illégales et les actions tolérées est mince. Jusqu'à quels montant un trader est-il libre d'engager la société pour laquelle il travaille ou celle qu'il représente. L'affaire Jérôme KERVIEL[638]en France avec la Société Générale en est un cas concret. Dans cette affaire très médiatisée[639], la fraude à l'origine des décisions judiciaires est l'introduction frauduleuse de données informatiques dans un système de traitement automatisé de données du marché financier.

Après, il faut considérer comme facteur l'identification matérielle des opérations et par conséquent l'identification des auteurs et l'administration des preuves contre ces dits auteurs.

Il convient de spécifier que les cybercriminels s'érigent en défenseur des libertés d'expression. Ils utilisent ce droit comme arme et exercent des représailles qui amplifient

---

[638] Cf. Cour d'Appel de Paris pôle 5, chambre 12, du 24 octobre 2012 ; Crim. 19 mars 2014, arrêt n° 1193, N/ R 12-87.416 FP-P+B+R+I, numéro de pourvoi 12.87-116, arrêt de cassation partielle avec renvoi.

[639] Plusieurs journaux télévisés et écrits ont présenté l'affaire Jérôme KERVIEL contre la Société Générale sous divers aspects, cf. : http://www.lexpress.fr/actualite/societe/justice/jerome-kerviel-condamne_1119764.html, http://www.lemonde.fr/societe/article/2014/05/18/le-defi-de-jerome-kerviel-a-la-justice-francaise_4420781_3224.html

davantage les difficultés à tous les sanctionner. A la suite des sanctions des Etats-Unis matérialisées par la fermeture de certains sites de streaming des tenants d'organisations de hackers notamment le groupe « ANONYMOUS » ont décidé d'attaquer ouvertement les sites de certains journaux (comme l'express) et de certaines hautes institutions à savoir le FBI.

Cette prétention à défendre leurs droits est une source de difficultés et entrave l'efficacité de la lutte contre la cybercriminalité. Le problème vient du fait qu'il est quasiment impossible de localiser physiquement ces pratiquants cybercriminels de la première heure.

Ces facilités de contournement constituent un des volets des échecs des multiples moyens mis en place pour lutter contre la cybercriminalité. Il faut dès lors mesurer cet aspect en mesurer l'ampleur pour parvenir à des solutions idoines.

Tous les moyens mis en place par l'ensemble des législations sont contournés de manière tout à fait aisée par les délinquants numériques du fait de leur adaptation rapide aux innovations technologiques.

En outre, il n'y a pas que le contournement des systèmes légaux et de sécurité mis en place qui intéressent les cybercriminels. Il faut préciser que dans une certaine mesure ces organismes détournent les lois. En effet, ces groupes qualifiés de cybercriminels par l'ensemble des pouvoirs étatiques revendiquent certaines lois pour servir de support à la commission de leurs actes. Comment appliquer les sanctions ?

Sous quelle qualification doivent- elles être poursuivies puisque ces organisations se servent des textes légaux et des principes fondamentaux comme cause de leurs actions pourtant infractionnelles.

Les contournements réalisés par les cybercriminels sont possibles du fait de leur adaptation constante aux technologies numériques. Aucune nouveauté ne leur échappe. Pire, ils travaillent à les développer et à parer aux éventuelles règles de sécurité mises en place.

D'ailleurs cette raison de l'adaptation aux innovations n'est pas l'unique source de prolifération du fléau.

La pratique constante de l'outil informatique et des autres technologies par les cybercriminels leur donnent la latitude de s'adapter facilement aux innovations en cours. Mieux, ils en font leur métier et deviennent des imbattables sur les questions concernées. Cet état des choses constitue un véritable frein à la lutte, principalement aux moyens mis en œuvre pour les appréhender et les punir.

Ils ont de la sorte une aisance particulière à ne pas se faire démasquer.

Dès lors, il leur est loisible d'envoyer des attaques directes à des institutions censées les combattre et détruire leurs activités. Certains groupes en arrivent à revendiquer leurs attaques comme s'il s'agissait d'une nouvelle forme de terrorisme et c'est le cas de se rendre compte de l'habileté et la provocation avec lesquelles sont exposés sur des sites les victoires de ces « hacktivistes ».

Hormis les activités des cybercriminels européens, ceux de l'Afrique de l'Ouest se jouent des lois répressives dans la mesure où elles sont à peine en cours d'élaboration. Partant de cet état du droit africain, les délinquants ne sont pas inquiétés et même s'ils devraient l'être, le faible nombre de sanctions effectives sur le terrain n'est pas un argument convaincant. Il en faudrait bien plus.

Par ailleurs, ces Etats dans lesquels les législations ne sont pas encore au point comme en Europe, pourraient servir de paradis d'hébergement aux cybercriminels.

En effet, puisque les structures sur place ne sont pas réellement adéquates pour les appréhender et les sanctionner, il serait non seulement difficile pour des pays européens de les atteindre mais en plus, ils pourraient par des techniques aisées contourner le peu de moyens existant sur place. Dans cette optique, les cybercriminels seraient susceptibles d'être localisés mais les règles étatiques concernées n'étant pas suffisamment claires, empêcheront de les punir.

La longueur d'avance des délinquants numériques par rapport aux organes régulateurs quant aux innovations sans cesse grandissantes des technologies de l'information a permis la prise de conscience des mutations de la cybercriminalité.

C'est pourquoi, il convient de répondre à cette criminalité particulière par une stratégie adéquate. C'est dans ce sens, qu'on peut valablement soutenir que la question de la répression est délicate.

La cybercriminalité est le nouveau visage de la délinquance organisée : derrière ces cybercriminels se cachent de véritables réseaux maffieux d'armes, d'escrocs qui profitent des risques limités d'identification qu'offre internet (surtout en Afrique). Les cybercriminels n'ont de la sorte aucun intérêt à laisser démolir leurs réseaux maffieux.

Le recours à ces infractions numériques, quelle que soit la forme qu'elles empruntent, sert à alimenter et à approvisionner les marchés de blanchiment d'argent, de drogues, de ventes de marchandises illicites et contrefaites.

En fait, la cybercriminalité a mué. On est ainsi passé d'une simple contamination des systèmes informatiques par des virus à de véritables industries avec des fournisseurs de services, de virus clés en main, d'entreprises innovantes, fournisseurs d'adresses mails, de fichiers de coordonnées bancaires, tendance particulièrement nette aux Bahamas et en Russie. L'ambivalence[640] des moyens de lutte contre la cybercriminalité constituent un autre facteur de contournement des législations mises en place.

En effet, un même logiciel peut à la fois servir à nuire et à protéger. Autre exemple dans le même ordre d'idée, une enquête diligentée contre une personne peut générer plusieurs autres informations qui ne sont pas nécessairement utiles à l'enquête concernée. Qu'est ce qui est fait du surplus d'informations ? C'est la question des contrôles par l'Etat de ses services et par conséquent des limites de l'enquête. A titre illustratif, la France est condamnée par la Cour Européenne des Droits de l'Homme dans une décision du 18 septembre 2014 pour avoir conservé au Système de Traitement des Infractions Constatées, des informations concernant monsieur François X[641]. Ces informations peuvent être consultées par sa compagne dans le cadre de leur séparation et la garde des

---

[640] Louise **FINES** traite clairement de cette ambivalence des outils technologiques dans son ouvrage sur les crimes invisibles paru chez Liber à Montréal en 2013, cf. Les crimes invisibles, délits contemporains, dénonciations et temps de réaction, p. 76.

[641] Cf. Cour Européenne des Droits de l'Homme, 5ème section arrêt du 18 septembre 2014, pour une version en ligne de la décision voir http://www.legalis.net/spip.php?page=breves-article&id_article=4281.

enfants. C'est ce qu'a souligné David BENICHOU un an auparavant, s'agissant des inquiétudes des structures et entreprises de sécurisation des systèmes[642].

On en arrive à un détournement des lois à des fins malsaines par les cybercriminels Avec les supposées problématiques ou droits que veulent défendre des hackers, comment faire la part des choses et être certain de poursuivre les vrais cybercriminels.

Encore une question difficile et sérieuse à laquelle les pouvoirs étatiques doivent répondre.

C'est dire que la définition d'actes cybercriminels reste encore à préciser par les législateurs.

A la date actuelle, la cybercriminalité demeure une boîte de Pandore dans laquelle est incorporé tout ce qui relève de fraude ou de falsification informatiques alors que certains comportements en eux-mêmes ne sont pas des actes cybercriminels au sens propre du terme.

Au titre de ces défenseurs des causes comme la liberté d'expression ou toute autre cause du même genre, s'inscrit l'organisme WIKILEAKS.

WIKILEAKS est une organisation qui s'est assignée pour rôle de dévoiler tous les secrets d'Etats dont elle aurait connaissance. Cette organisation a pour porte-parole Julian ASSANGE. Cette fondation a donc décidé de faire un combat dans la guerre de l'information tant les pouvoirs étatiques dans le monde entier restent secrets sur l'ensemble des pratiques et stratégies. La pratique de WIKILEAKS s'appuie sur l'importance ou la gravité du leaks (en anglais fuite[643]). Il ne faut mentionner que le porte-parole est un hacker de la première heure.

---

[642] Cf. David BENICHOU, Sécurité des Systèmes d'Information, rapport publié à la documentation française, 2005

[643] Définition tirée du Dictionnaire HARRAPS Anglais-Français Shorter, Chambers United Kingdom, 2009, p. 514.

L'ampleur des actions des Hackers comme WIKILEAKS se mesure aux conséquences des informations divulguées. En témoigne l'affaire ENRON, qui a été provoquée par les révélations du site WIKILEAKS[644].

Sous couvert de la liberté d'expression, certains internautes divulguent des informations sur des sites de restaurants, d'hôtels, loisirs, sur certains lieux sans de véritables enquêtes, à l'image des guides officiels comme le guide Michelin, ni avoir été mandatés par les enseignes visées. Ces informations causent pour ces lieux des préjudices (manque de visites, de clientèle) allant jusqu'à la baisse du chiffre d'affaires[645]. La conséquence est la création d'un nouveau métier « les faiseurs d'images» ou de « relationnistes », leur rôle consistant à embellir l'image du client qui peut être aussi bien une personne physique comme une entreprise ou encore un restaurant, une auberge…. Le travail du faiseur d'images consiste surtout à « nettoyer » l'image du client sur la toile c'est-à-dire qu'il vérifie sur internet ce qui peut être dit pour retirer toutes les mauvaises critiques, les commentaires désagréables, susceptibles de le mettre en difficulté.

L'autre hypothèse est celle de la diffusion des faux avis par des agences spécialisées mandatées pour tromper le consommateur[646]. Ce type d'action trompeuse est souligné par la DGCCRF[647] qui attire l'attention des consommateurs.

---

644 Voir *Le Monde diplomatique* du 8 mars 2002 avec l'article intitulé « *Enron, symbole d'un système* ». Voir aussi *Le Figaro* du 30 novembre 2010, partie Economie : le quotidien précise dans son titre « *Wikileaks cible les banques » ;* voir également E. FREYSSINET, la cybercriminalité en mouvement, éditions LAVOISIER, 2012.

645 Estelle ROSSET, *Les commentaires internet pèsent fortement sur la fréquentation des hôtels et restaurants à Limoges*, Journal le populaire du centre du 06 octobre 2014 et en ligne : http://www.lepopulaire.fr/limousin/actualite/departement/haute-vienne/2014/10/06/les-commentaires-internet-pesent-fortement-sur-la-frequentation-des-hotels-et-restaurants_11170530.html

646 Cf. Isabelle Rey-Lefebvre, Les faux avis sur Internet se multiplient, *Le Monde* du 02 Août 2014. Compléter avec l'article de l' Agence Française de Presse (AFP), TripAdvisor soupçonné de diffuser de faux avis en ligne, *Le Parisien* du 21 mai 2014, et pour http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=29&cad=rja&uact=8&ved=0CFUQFjAIOBQ&url=http%3A%2F%2Fwww.leparisien.fr%2Fflash-actualite-economie%2Ftripadvisor-soupconne-de-diffuser-de-faux-avis-en-ligne-21-05-20143859745.php&ei=Xs1MVJ7OKMSdPd6_gLAH&usg=AFQjCNEkxH0H0TncHWztErJQzMIVXKVtaw.

A la difficulté de choisir entre une harmonisation générale ou spéciale des lois incriminant la cybercriminalité, s'ajoute l'absence de coordination des politiques de lutte contre la cybercriminalité.

b- Le manque de coordination des politiques de lutte contre la cybercriminalité

La coordination des politiques de lutte contre la cybercriminalité s'entend de la définition des lignes à suivre et du temps de réalisation des objectifs fixés.

En effet, contrairement aux Etats de l'Union Européenne, ceux de l'Afrique de l'Ouest ne mènent pas la recherche de solution contre la cybercriminalité de manière coordonnée. Chaque Etat de l'espace ouest africain considéré avance à son rythme si bien que chacun privilégie les domaines qu'il estime être une priorité par rapport à ses populations, aux demandes et aux réalités.

Il en résulte une dispersion et un manque de coordination des politiques. C'est ainsi qu'au niveau des lois, on note un décalage temporel important entre les dates d'édiction : tandis que certaines lois sur la protection des données à caractère personnel datent de 2008 comme c'est le cas du Sénégal, d'autres sont de 2013 pour citer l'exemple du Niger ou de la Côte-d'Ivoire.

La même problématique se pose au niveau de la mise en place des structures en charge de lutte contre la cybercriminalité. Les polices et gendarmeries des Etats de l'Afrique de l'Ouest sont à peine dotées d'outils informatiques et de matériels de recherche et d'enquêtes indispensables à leur travail. Là encore, la part contributive des Etats africains directement concernés reste moins importante que ses Etats européens partenaires. Par exemple, il faut attendre des plaintes des ressortissants français, pour que les autorités françaises s'investissent dans des partenariats avec le Togo[648] notamment en favorisant la

---

[647] Cf. La lettre de la DGCCRF - Concurrence et consommation n°2 juillet/août 2014 disponible en ligne : http://www.economie.gouv.fr/files/files/directions_services/dgccrf/documentation/Lettre_CetC/lettre_CetC_2.pdf

[648] Cf. La lettre de l'Ambassade de France au Togo, *Janvier 2012 - n°2* ; voir également le Rapport du FORUM SUR LA GOUVERNANCE DE L'INTERNET (FGI/IGF 2013) Deuxième édition, année 2013.

formation des policiers et gendarmes par un gendarme de l'Office central français de lutte contre la criminalité liée aux technologies de l'information et de la communication. C'est grâce à une telle initiative que la Cellule de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (CLCTIC) a vu le jour.

Les lois réprimant les actes cybercriminels ne sont pas suffisamment coordonnées et les peines qu'elles prévoient le montrent. Il s'avère nécessaire de les ajuster. Or ces ajustements sont un autre aspect des difficultés de répression de la cybercriminalité.

B- Les ajustements des peines

La difficulté d'harmoniser les peines se ressent surtout au niveau des sanctions des infractions cybercriminelles édictées d'un Etat à l'autre. Et ce constat n'est pas propre aux Etats européens uniquement. Il en va de même des Etats de l'Afrique de l'Ouest.

a- La nécessité de coordination des peines prononcées

Il arrive qu'il y ait des vides juridiques dans certains Etats et cela pourrait justifier l'absence d'incidence des peines déjà prononcées par un juge.

Il convient de souligner dans ce cadre que Monsieur EL CHAER, dans sa thèse sur la criminalité informatique devant la justice pénale, soutient que la difficile définition des sanctions à la criminalité informatique est liée à une absence de définition de l'ordinateur. Il en déduit un manque de rigueur dans la classification des fraudes informatiques.

L'absence d'incidence des condamnations d'un criminel à l'étranger sur les peines prononcées dans le nouvel Etat de commission d'une infraction donnée est une limite à l'efficacité des sanctions contre la cybercriminalité. Cette question soulevée peut être résolue par les procédures d'exequatur qui favorisent la reconnaissance des décisions de justice généralement et des peines en particulier rendues par le juge d'un Etat. Le problème pourrait également être réglé avec les conventions multilatérales ou plus souvent bilatérales signées en matière de coopération de police judiciaire.

Il faut cependant de s'interroger de l'efficacité des procédures d'exequatur en la matière. Cette procédure pourrait-elle par ailleurs s'étendre et s'appliquer en cas de conventions existant entre Etats de l'Union européenne et Etats de l'Afrique de l'Ouest ?

Dès lors analysons l'impact des accords sur les flux de transferts internationaux dont la plupart des Etats de l'Afrique de l'Ouest sont signataires.

b- Le faible effet des sanctions dissuasives

La cybercriminalité ne cesse d'évoluer malgré les sanctions prononcées. Certaines de ces punitions sont dites dissuasives. Il faut cependant constater avec regret qu'elles n'ont pas l'effet escompté. Du moins, la portée de la dissuasion n'est pas suffisante pour freiner d'autres délinquants à réitérer des actes déjà réprimés. L'exemple des jeunes ouest-africains permet d'illustrer le propos. Il est possible de lire sur des sites d'information et dans l'actualité des journaux des arrestations, des interpellations de jeunes ivoiriens (voir site de la plateforme de lutte contre la cybercriminalité, ou encore sur abidjan.net) ou de jeunes sénégalais (osiris.net ou encore dans les quotidiens internationaux dédiés à l'Afrique tel jeune Afrique) pour des arnaques aux sentiments, ou des fraudes bancaires via des réseaux numériques.

Par ailleurs, l'extrême généralité des engagements des Etats[649] est un autre paramètre à considérer. En effet, les engagements des Etats relatifs à la prise des sanctions dans les systèmes de coopération sont rédigés en des termes très généraux et sans précisions des modalités d'établissement des sanctions concernées si bien que *l'effet dissuasif recherché est annihilé*[650].

A la suite des analyses qui précèdent se dégage un nombre limité de sanction que sont les amendes, les peines privatives de liberté selon les degrés de gravité des infractions cybercriminels. Il faut envisager les niveaux de responsabilité pour déterminer

---

[649] Cf. **A. BERNARDI**, Stratégies pour une harmonisation des systèmes pénaux européens, in Archives de politique criminelle 2002/1 n°24, p. 209.

[650] Cf. **BERNARDI A.**, Stratégies pour une harmonisation des systèmes pénaux européens, in Archives de politique criminelle 2002/1 n°24, p. 209, article dans lequel l'auteur cite la Convention EUROPOL de 1995

à bon escient les sanctions. En termes d'ajustement, trouver les responsables sur des infractions complexes comme la cybercriminalité relève de techniques juridiques précises. A titre d'illustration, en matière de falsification de données, qui est responsable, uniquement l'auteur direct de la falsification ou doit-on tenir compte également du responsable du traitement de données ayant servi de base à la commission de cette infraction ?

C'est la question de la complexité des degrés de responsabilité dans le traitement des sanctions contre la cybercriminalité.

§2- La complexité des degrés de responsabilité dans la cybercriminalité

Déterminer les niveaux de responsabilité est fonction de l'infraction considérée. Qu'il s'agisse de responsabilité civile ou pénale, des conditions doivent être remplies. En l'espèce, la cybercriminalité se rapporte à la commission d'infractions. Le fait générateur est donc un délit ou un crime. La responsabilité de principe à engager est la responsabilité pénale.

Ainsi, la responsabilité est engagée différemment selon qu'il s'agisse d'infractions liées aux supports informatiques ou en réseaux ou encore par des canaux plus directs et laissés en libre accès au public. Plusieurs cas de figure se présentent.

Premièrement, l'hypothèse d'un acte cybercriminel qui fait intervenir un numéro de carte vitale ayant été falsifiée ou utilisée par une personne non titulaire de ladite carte. Si le titulaire de la carte n'a jamais eu de lien avec le faussaire, il est possible de lier la fraude directement aux services de caisse d'assurance maladie qui ont en charge tous les traitements de dossiers relatifs aux cartes vitales sur l'ensemble du territoire.

Les services concernés devraient mettre en place une sécurité permettant de protéger le titulaire de la carte vitale dès l'instant où cette carte contient des données permettant d'identifier cette personne.

---

comme un exemple d'instrument conventionnel à caractère universel ou régional visant à développer des

Si à l'inverse, il existe un lien entre le faussaire et le titulaire de la carte, la Caisse d'assurance maladie pourrait aisément tenir pour responsable le titulaire de la carte.

Deuxièmement, l'hypothèse dans laquelle un message est envoyé par une enseigne de distribution, chez laquelle le client (destinataire du message) aurait conclu un précédent achat. Le client reçoit sur son téléphone un message écrit comportant la confirmation de la commande d'un nouveau téléphone qu'il n'aurait pas commandé en réalité.

Si ce client n'a effectivement rien commandé, deux interrogations : qui a passé commande à sa place et pourquoi cette commande virtuelle correspond-t-elle à certaines données qu'il aurait à un moment précis utilisées dans ses relations clients-vendeurs avec l'enseigne de distribution ? Il s'avère après vérification que le destinataire du message écrit n'a effectivement rien commandé, et que sa carte bancaire aurait été utilisée par une autre personne.

La responsabilité de l'enseigne pourrait être engagée car il n'existe en principe aucun lien direct entre le titulaire d'une carte bancaire et son numéro personnel de téléphone mobile.

Ce lien entre la carte bancaire et le numéro de téléphone n'étant créé qu'au moment de l'achat d'une marchandise via le site internet de l'enseigne.

Il arrive cependant que des règles de la responsabilité civile interfèrent vue la complexité de cette criminalité particulière.

Il convient d'analyser les actions des hébergeurs et des fournisseurs d'accès internet afin de délimiter leur niveau de responsabilité dans la répression de la cybercriminalité.

Dès lors quelle est la nature de la responsabilité des fournisseurs d'accès internet ou des hébergeurs ? (A) A quelles conditions leur responsabilité peut-elle être engagée ? (B)

Les règles sont-elles les mêmes dans l'Union européenne et en Afrique de l'ouest ?

---

formes de coopération pénale entre les Etats et favorisant une un rapprochement des systèmes punitifs.

A- La nature de la responsabilité des fournisseurs d'accès internet et des hébergeurs

La nature de la responsabilité dépend du fait générateur à l'origine de cette responsabilité. Il faut ensuite déterminer si elle est civile ou pénale compte tenu de l'existence d'un contrat entre le fournisseur d'accès ou l'hébergeur et son client ?

Les habitudes de commerce ont désormais évolué et les consommateurs développent plus de comportements d'achat sur internet. C'est la raison pour laquelle le dispositif législatif européen touche tous les niveaux de la consommation avec les différentes directives élaborées.

a- Au sein de l'Union européenne

Les fondements textuels sont la convention de Budapest, plusieurs directives européennes et enfin les lois nationales comme la Loi sur la Confiance dans l'Economie Numérique du 21 juin 2004 en France.

Dans la Convention de Budapest (Convention de lutte contre la cybercriminalité), il n'existe pas réellement des dispositions relatives à la responsabilité des fournisseurs d'accès internet ni des hébergeurs. Il faut donc regarder les dispositions des directives européennes qui prévoient clairement les obligations de ces prestataires et qui en déterminent les effets quant à la responsabilité qu'ils encourent.

Il s'agit d'abord de **la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000** relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur « *directive sur le commerce électronique*»[651]. Concernant ce dispositif, il faut préciser qu'il a vocation à réguler les prestations de services en ligne de matière contractuelle. Avec le changement des habitudes de consommation, c'est l'encadrement des relations contractuelles entre les prestataires de service qui proposent des biens ou des prestations à vendre et les internautes ou les e-consommateurs.

[651]Cf. J.O.C.E., n° L 178 du 17 juillet 2000, p. 1 et s

Légiférer sur le commerce électronique au sein de l'Union européenne apparaît incontournable pour la sécurité des opérations financières dans cet espace. En effet, cette directive prévoit les règlements certes des contrats mais également la gestion des contentieux qui pourraient survenir dans la vie de ces contrats numériques.

La directive 2000/ 31 définit donc l'hébergeur comme un prestataire dont le rôle est purement technique, automatique et passif, impliquant qu'il n'a ni le contrôle ni la connaissance des contenus. En appui de cette définition, il est possible d'affirmer que l'hébergeur ne saurait être responsable en cas de données ou d'informations volées. Sur ce point, l'article 6-1-3 de la loi (LCEN) dispose que « *les personnes physiques qui assurent même à titre gratuit pour la mise à disposition du public par des services de communication au public en ligne, ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande du destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* ».

C'est dire que la responsabilité pénale des hébergeurs n'est pas retenue ou du moins n'est pas facilement engagée en raison de leur manque de contrôle sur les contenus stockés par leurs services.

Sur le fondement de ces textes, les juges ont tranché plusieurs cas, par exemple l'arrêt Rose B rendu par la Cour d'Appel de Paris. Les faits sont les suivants :

A la suite de la réalisation en 2010 du film « la Rafle », madame Roselyne B dite « Rose B. G. » a fait l'objet d'un article « Rose B devrait fermer sa g…» publié sur un blog hébergé par la société JFG Networks. S'estimant outragée par les propos de cet article, Madame Rose B demande le retrait de l'article à la société JFG Networks. Sans réaction de la part de la société, madame B l'assigne en référé d'heure à heure le 7 mai 2012 devant le Tribunal de Grande Instance de Paris pour le refus du retrait de l'article outrageant. Le tribunal de Grande instance la déboute dans son ordonnance du 29 mai

2012[652], de ses demandes et elle saisit alors la Cour d'appel de Paris[653] afin de voir l'ordonnance reformée.

La Cour d'appel confirme l'ordonnance du tribunal dans sa décision du 4 avril 2013. Les juges d'appel estiment que les propos de la société JFG Networks entrent dans le champ de la liberté de critique et d'expression sans atteindre l'abus.

Au titre des directives relatives aux fournisseurs d'accès internet et hébergeurs, est ensuite concernée, **la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002** concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite « *directive vie privée et communications électroniques* »[654]. Le texte concerné soulève les questions de diffusions des informations personnelles des internautes notamment dans les échanges de documents, d'informations par le canal des courriels ou autres moyens de communications électroniques. Il met l'accent sur la protection de la vie privée et permet ainsi de faire la différence entre les communications électroniques qui sont sujettes à diffusion publique et celles qui relèvent de la vie privée et qui par conséquent sont protégées au même titre que le droit à la vie privée.

La directive 2002/58 a été modifiée en 2009 grâce à la directive 2009/140/ce du Parlement européen et du Conseil du 25 novembre 2009[655] modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques pour inclure une obligation de faille de la part des opérateurs de télécommunication : l'obligation de notification des failles de sécurité.

---

[652]Cf. Ordonnance du TGI de Paris du 28 mai 2012 commentée à la Revue Lamy Droit de l'Immatériel, juin 2012, n°2795.

[653]Cf. Cour d'Appel de Paris pôle 1, Chambre 2, arrêt du 4 avril 2013.

[654]Cf. J.O.C.E., n° L. 201 du 31 juillet 2002, p. 37

[655]Cf. J.O.U.E. n° L. 337/37 du 18 décembre 2009

La transposition de cette directive s'est faite selon la culture de protection des Etats de l'Union Européenne. En effet, en Espagne, c'est dès 2007 que la directive a été transposée. Ce pays fait partie des Etats ayant une importante culture de la sécurité informatique notamment avec sa loi sur les données personnelles qui est fortement axée sur la sécurité des données.

Il en va de même en Allemagne où la transposition a eu lieu dans la même année en 2007 grâce à un règlement et il a alors une force plus contraignante.

Cette directive n'a été transposée en France qu'en 2012 par un décret n° 2013-436 du 30 mars 2012. La difficulté de ce texte est la définition même de l'obligation de notification de failles de sécurité. Ce n'est pas la seule zone d'ombre dans la mesure où les débiteurs de cette information ne sont pas clairement déterminés. Certes, le texte de la directive dispose notamment en France que ce sont les opérateurs de télécommunication qui sont tenus de cette obligation mais il faut s'interroger sur l'obligation en ce qui concerne les hébergeurs et les fournisseurs d'accès internet. Ces deux catégories sont-ils des opérateurs de télécommunications compte tenu de la nature des prestations qu'ils proposent ?

Quelle différence existe-t-il entre un hébergeur et un fournisseur d'accès internet ?

L'hébergeur d'un site a pour mission de mettre à la disposition des internautes un site Internet géré par des tiers. Il s'agit d'un prestataire de service à qui la loi LCEN accorde une responsabilité pénale allégée par rapport aux éditeurs de communications numériques.

Les obligations mises à la charge des opérateurs de téléphonie et des hébergeurs ont pour finalité de les rendre responsables au regard des dispositions des différentes directives. Certes, elles visent à protéger le consommateur, mais elles sont surtout émises pour encadrer les actes de ces prestataires et hébergeurs. D'ailleurs, l'obligation de notification des failles de sécurité le montre clairement.

C'est dans ce cadre, il est possible de citer la responsabilité des hébergeurs de sites ou de blogs. A l'heure actuelle, tout individu a la latitude de construire un blog. C'est une pratique en vogue sur la toile. Tous les sujets sont permis à condition pour l'hébergeur du blog de remplir certaines conditions prévues par la loi.

D'autres directives protégeant les relations contractuelles en ligne des consommateurs doivent être mentionnées dans le cadre des sources de responsabilité des prestataires de service de communication et des fournisseurs d'accès internet. Il s'agit de la **directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002** concernant la commercialisation à distance de services financiers auprès des consommateurs et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE[656]. Elle traite des opérations bancaires effectuées à distance donc par l'intermédiaire des connexions électroniques. Ces opérations sont la plupart du temps des pistes d'exploitation pour les délinquants électroniques. Il est de ce fait important de prévoir des textes pour réguler ces échanges en vue de protéger le consommateur.

Comment est réglée la question de responsabilité en Afrique de l'Ouest ?

b- En Afrique de l'Ouest

Du côté ouest-africain, la complexité commence également avec la détermination du fondement légal. Comment agencer le droit OHADA et les dispositions légales créées par la CEDEAO ? L'interrogation est de mise puisqu'en matière de commerce électronique et des affaires liées, la CEDEAO traite des questions de responsabilité des fournisseurs d'accès de services électroniques. Il s'agit de savoir comment combiner ces deux structures de sortes à utiliser les textes juridiques adaptés au domaine de compétence concerné. L'OHADA est l'organisation en charge de l'Harmonisation en Afrique du droit des Affaires. La CEDEAO est l'organisme économique des Etats ouest-africain. L'OHADA a donc une compétence territoriale plus large mais un domaine d'intervention limité en ce qu'il ne traite uniquement du droit des affaires. Quant à la CEDEAO, elle a une compétence territoriale limitée aux Etats Ouest- Africains qui en sont membres mais à un champ d'action large compte tenue de la dimension économique qui inclut à la fois les affaires publiques, privées, les investissements et toutes les couches qui se rapportent à l'économie d'une façon générale.

[656] Cf. la directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs publiée au J.O.C.E. n° L. 271 du 9 octobre 2002, p. 17 et s

En matière de responsabilité des fournisseurs d'accès de service, l'article 6 de l'acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO dispose que : « *toute personne physique ou morale exerçant une activité entrant dans le champ d'application du présent Acte additionnel est responsable de plein droit à l'égard de son cocontractant de la bonne exécution des obligations résultant du contrat, que des obligations soient à exécuter par elle-même ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci*».

A l'analyse, cette disposition est classique à tout contrat et on peut en déduire que le fournisseur d'accès internet est tenu aux obligations classiques liées à son contrat. Mais, elle est tout de même spécifique puisqu'il importe peu que le fournisseur d'accès ait délégué sa mission à un autre prestataire. Sa responsabilité n'est pas pour autant écartée.

A quelles conditions la responsabilité des prestataires internet est-elle engagée ?

B- Les conditions de la responsabilité des prestataires d'internet

Une fois la nature civile ou pénale de ces prestataires déterminées en s'appuyant sur les différentes obligations dont ils sont tenus, quelles sont les conditions d'engagement ou non de cette responsabilité ?

Dans sa thèse sur la responsabilité des fournisseurs de moyens de communication électronique, Madame ALBRIEUX démontre que ces prestataires ne sont pas directement auteurs des faits notamment cybercriminels qui pourraient se produire à la suite des prestations de fourniture d'accès internet qu'ils opèrent.

La responsabilité relative aux contenus n'est pas qu'occasionnelle dans la mesure où les fournisseurs d'accès ou les intermédiaires ou encore les opérateurs de réseaux n'ont pas toujours les moyens de les contrôler ; sauf par exemple lorsqu'ils disposent de système de contrôle éditorial grâce à des logiciels de filtrage de contenus comme c'était le cas dans l'affaire Statton Oakmont Inc v Prodigy[657].

[657]Cf. Décision de la Cour Suprême de New-York de 1995, citée par C. GUERRIER & M-C. MOUGET dans Droit et Sécurité des Télécommunications, p. 347.

En Allemagne, le producteur est responsable. A l'opposé, l'offreur d'accès ne l'est pas dans la mesure où il n'a de rôle que d'acheminer le contenu. Il sert de transit. Il est un intermédiaire.

En Belgique, c'est la proportion du rôle joué par le prestataire qui détermine sa responsabilité ou non. Il s'agit de la capacité du prestataire, en tant qu'administrateur à contrôler les contenus injectés sur la toile.

Il ressort de ces différents cas que le prestataire de service, fournisseur d'accès ne sera responsable qu'à la condition d'avoir été ou non en mesure de bloquer le contenu des sites incriminés.

En droit sénégalais par exemple, le 1) de l'article 3 de la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques définit les fournisseurs d'accès internet 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*. Et en se fondant sur cette définition, c'est un principe d'irresponsabilité pénale des fournisseurs d'accès qui est posée à condition que le fournisseur d'accès internet limite son rôle technique au transport d'informations sur le réseau.

Toujours selon le droit sénégalais, le 2) de l'article 3 de la loi précitée définit les hébergeurs comme *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*. Les hébergeurs ne sont responsables que dans deux cas mentionnés au 3) du même article 3 :

- s'ils avaient effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou

- si, dès le moment où ils en ont eu cette connaissance, ils n'ont pas agi promptement pour retirer ces données ou en rendre l'accès impossible.

La responsabilité pénale des hébergeurs n'est pas directement déterminée par les contenus stockés par les personnes à qui ils délivrent leurs services. Cette responsabilité est limitée aux deux conditions alternatives précédemment citées.

Conclusion du chapitre1

La mise en œuvre du dispositif répressif de la cybercriminalité permet d'aborder non seulement l'aspect préventif de la question mais également l'aspect coercitif. Il en ressort que la répression de la cybercriminalité obéit à différentes étapes qu'il est permis de qualifier de capitales aussi bien les unes que les autres. S'agissant des contours préventifs c'est-à-dire les actes posés par les acteurs de la lutte contre la cybercriminalité pour éviter que ces actes soient commis, plusieurs obstacles apparaissent. Pour ces problématiques, en ce qui concerne le continent africain et principalement la partie ouest-africaine, la prévention contre la cybercriminalité est en construction. Les opérations d'adressage (téléphoniques, numériques ou de noms de domaine) sont en évolution et cela constitue un point positif pour la lutte contre le fléau cybercriminel.

Quant à la rédaction des lois et à leur harmonisation, la procédure de réflexion commune engagée par les Etats membres de la CEDEAO et de l'UEMOA emprunte certes la technique européenne mais semble prudente même si dans certains dispositifs, les Etats parties gagneraient à être plus précis. En effet, s'agissant des sanctions édictées, elles sont laissées à la charge de chaque Etat. Concernant l'Europe, il y a beaucoup d'imperfections malgré une mise en place préventive en avance en comparaison du continent africain. C'est surtout dans la mise en œuvre des harmonisations législatives et des peines que l'Union européenne pèche par ses hésitations et l'excès de considération des différences culturelles.

Le problème de l'Union européenne dans la répression de la cybercriminalité n'est pas l'absence de textes incriminant les actes cybercriminels. Il n'est pas non plus remis en question la mise en place des instruments et des structures favorisant la répression du fléau. Le dilemme est celui de la coordination des compétences de ces instruments et organes créés pour réprimer la cybercriminalité et punir ses adeptes. C'est une question de hiérarchisation des compétences punitives qui revient. Cette interrogation que l'Union européenne a du mal à résoudre depuis ses différents organes qu'il s'agisse de l'Office de Lutte Anti-Fraude, d'EUROJUST, d'EUROPOL ou encore de ces organes

communautaires par rapport aux entités étatiques. Comment articuler les différentes structures mises en place dans l'objectif de sanctionner efficacement la cybercriminalité ? Comment agencer les différentes compétences, tout en respectant les autonomies et indépendances requises pour les différentes entités créées. La question de la coordination politique au niveau de l'Union européenne est la réelle difficulté. Il s'agit plus d'une organisation structurelle des organes en charge de la répression de la cybercriminalité que d'une absence totale d'harmonisation.

L'importance des politiques de sanctions établies sera mesurée à la lumière de la pratique qui découle des applications des textes de lois élaborés.

Le problème se situe ailleurs quant à l'espace ouest-Africain :

Les structures sont-elles suffisantes et équipées pour mener à bien la lutte et la répression efficiente ? La qualité et le nombre traduiront la mise en œuvre effective de la répression.

CHAPITRE 2 : LA MISE EN ŒUVRE DE LA REPRESSION

Les politiques mises en place en vue de la répression de la cybercriminalité sont mises en œuvre par des organismes avec un statut d'autorité administrative indépendante à l'instar de la CNIL au plan national, du Groupe 29 au plan européen mais également par des structures beaucoup plus internationale comme INTERPOL. Cette mise en œuvre en dehors des instances judiciaires est quotidiennes et nécessite d'aborder la question du rôle de ces structures dans la coercition de la cybercriminalité. L'efficacité de la politique mise en place est effectivement mesurée à travers l'efficacité des textes règlementaires d'application. De ce fait, le recours à un organe consultatif et coercitif avec des compétences fondamentales comme la Commission Nationale de l'Informatique et des Libertés (CNIL) est d'un intérêt majeur. Cet organe a inspiré la création d'une autre entité de dimension régionale au niveau européen (le Groupe 29)[658]. Le CNIL a stimulé d'autres entités similaires partout en Europe. D'autres organismes de terrain viennent, en outre, en appui à ces deux structures nationale et régionale dans cette lutte pour endiguer le fléau cybercriminel. Leurs rôles, actions et compétences seront envisagées en même temps que ceux de la CNIL. En dépit du retard accusé par le continent africain, il est également en train de mettre en place de telles structures. Il en découle une coopération continuelle entre l'Union Européenne et l'Afrique de l'Ouest. C'est pourquoi l'action est au cœur des activités de la CNIL et des autres organismes d'une part (section 1) mais également du fait des structures ouest-africaines d'autres part (section 2).

---

[658] Ce comité de réflexion porte le nom de l'article 29 de la loi Informatique et Libertés du 6 janvier 1978 : c'est cette disposition légale qui institue le groupe.

Section 1 : L'importance de la Commission Nationale Informatique et Libertés dans la lutte et les autres organismes

L'action française pour combattre la cybercriminalité passe par l'encadrement des aspects clés comme les données à caractère personnel et leur traitement confiés à la Commission Nationale Informatique et Libertés connue (CNIL).

Cette autorité administrative indépendante a des institutions correspondantes dans l'ensemble des pays de l'Union européenne. Si l'appellation de ces organismes diffère d'un pays à l'autre, leurs missions semblent être harmonisées.

En ce qui concerne la France, la création de la CNIL remonte à l'année 1978 avec la Loi Informatique et Libertés[659].Ce texte législatif n'est pas l'unique texte important pour cette commission. En effet, plusieurs autres textes de diverses natures sont fondamentaux en ce qui concerne la CNIL, ses activités et ses actions. Il s'agit de :

- la Convention 108, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[660]et de son protocole additionnel[661].

- la Charte des droits fondamentaux de l'Union européenne[662], particulièrement en son article 8 du titre 2 qui fait référence à la protection des données à caractère personnel.

En effet, elle prévoit que : « *Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux*

---

[659] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[660]Cf. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981, STCE n° 108.

[661] Cf. Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, du 08 novembre 2001, ratifié le 1er avril 2004, Série des Traités des Communautés Européennes n° 181.

[662] Cf. JOCE C 364/1 du 18 décembre 2000.

données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

- la Directive européenne n° 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[663].

Au niveau européen, le texte de référence est la directive européenne 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[664]. Cette directive contient en effet des dispositions relatives à la protection des données personnelles des individus et encadre juridiquement les transmissions de ces données. C'est ainsi qu'à l'heure actuelle, tous les Etats de l'Union Européenne ne l'ont pas encore transposée dans leur législation. La directive a pour conséquence la modification de certaines législations notamment au moment de la transposition dans les droits internes concernés.

Certains Etats comme l'Espagne, n'ont pas eu besoin de modifier considérablement leur législation. En effet, en ce qui concerne l'Espagne, sa loi d'origine[665] sur la protection des données à caractère personnel a été élaborée sur la base du projet de la directive 95/46/CE[666]. C'est pour cette raison que c'est par la simple loi du 13 décembre 1999 qu'a été modifié le texte d'origine du 29 octobre 1992. De plus la constitution espagnole

---

[663] La directive qui figure à ces références JO L 281 du 23.11.1995, p. 31, a été modifiée par le règlement de 2003, Règlement (CE) no 1882/2003 du Parlement européen et du Conseil du 29 septembre 2003 portant adaptation à la décision 1999/468/CE du Conseil des dispositions relatives aux comités assistant la Commission dans l'exercice de ses compétences d'exécution prévues dans des actes soumis à la procédure visée à l'article 251 du traité CE au Journal Officiel des Communautés Européennes L 281 du 31. 10. 2003.

[664] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050. Elle est en phase d'être modifiée et remplacée par un règlement : cf. Proposition de règlement du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), Communication de la Commission Européenne du 25 janvier 2012 , n° 2012/0011 (COD).

[665] Loi du 29 octobre 1992 sur la protection des données personnelles, cf. la loi organique 5/1992 sur la règlementation du traitement automatique des données personnelles : Ley Orgánica 5/1992, de Tratamiento Automatizado de datos de carácter personal.

[666] Cf. Note de synthèse réalisée par le Sénat sur la transposition de la directive relative à la protection des données à caractère personnel dans l'Union européenne, étude publiée sur le site du sénat.

en son article 18-4 précise « *la loi limitera l'usage de l'informatique pour garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits* »

En ce qui concerne la France, elle a transposé la directive grâce à la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[667]. Pourquoi une transposition si tardive ?

En analysant les faits, il faut mentionner que la proposition de la directive 95/46 dite vie privée est l'œuvre de la CNIL, qui a fait un important lobbying auprès des instances européennes afin de transposer l'exemple français de protection des données à caractère personnel. Il apparaît donc étonnant que la France fasse par la suite l'objet de pressions de la part de la Cour européenne de Justice avant de procéder à la transposition de la directive dans le droit français.

La transposition est au départ prévue pour le 24 octobre 1998 mais est par la suite reportée. Le retard dans la transposition de la directive européenne dite « vie privée » est due selon certaines analyses du Conseil d'Etat[668] à l'insuffisance de formation des magistrats.

Il faut dire qu'en matière de protection des données, la France a l'un des systèmes les plus complets, à la fin des années 70. La première loi française sur la protection des données à caractère personnel du 6 janvier 1978 jugée extrêmement sévère, a plusieurs fois été modifiée et ce notamment en 2011 par une ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques[669].

---

[667] Elle est parue au JORF n°182 du 7 août 2004 page 14063 texte n° 2.

[668] Etudes du Conseil d'Etat de décembre 1989 sur les problèmes posés par la transcription en droit interne des directives communautaires.

[669] Ordonnance parue au Journal Officiel de la République Française n°0197 du 26 août 2011 page 14473 texte n° 49.

Cette directive est à l'heure actuelle le texte de base en matière de protection des données au plan européen. Mais la législation européenne fait l'objet de réflexions accrues notamment avec l'examen de la proposition de règlement européen des données à caractère personnel.

En effet, les députés européens examinent la proposition de faire de la directive un instrument plus contraignant. C'est l'occasion de réviser certaines dispositions jugées peu protectrice des droits des citoyens européens.

L'organisme en charge de l'information et la protection des données à caractère personnel est la CNIL. Pour mener à bien sa mission, la CNIL a un pouvoir de contrôle et de sanction[670].

Cette autorité incontournable n'est heureusement pas le seul organe en charge de telles questions. D'autres organismes tant au niveau national qu'européen interviennent.

C'est pourquoi, il peut être permis de parler de la CNIL, de ses pairs et des autres organismes venant en appui.

§1- La CNIL et les institutions européennes équivalentes

La Commission Nationale pour l'Informatique et les Libertés (CNIL) est l'appellation française de l'organisme en charge du contrôle des données personnelles des individus.

Cette autorité administrative indépendante a des institutions équivalentes dans tous les Etats de l'Union Européenne. C'est d'ailleurs sous son inspiration qu'a été créé un organisme européen représentant l'ensemble des Etats dénommé « Groupe article 29 ». Cette dénomination particulière est liée au fait que ce groupe de travail a été constitué par la Commission européenne sur la base de l'article 29 de la directive européenne de 1995. L'article 29 institue le groupe à vocation de la protection des traitements des données à caractère personnel au niveau de l'union européenne au point 1 de l'article en

[670] www.cnil.fr

ces termes : « il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel ». Il convient pour des raisons de clarté de s'intéresser d'abord à l'organisation de la CNIL ou des autorités correspondantes dans chacun des Etats avant de déterminer les rôles et compétence du Groupe 29 dans la lutte contre la criminalité informatique.

A- Organisation et fonctionnement de la Commission Nationale pour l'Informatique et les Libertés

L'optique d'harmonisation qui régit les Etats de l'Union européenne explique qu'ils se soient tous mis à une politique de protection des données personnelles. Cette politique s'est élaborée au fur et à mesure de l'expérience acquise et en tenant compte des particularités de chacun des Etats[671].

Chronologiquement, les pays comme la Suède sont très en avance en la matière dans la mesure où dès les années 1973 la loi sur la protection des données[672] appelée *Datalagen,* est élaborée.

A sa suite, l'Allemagne a légiféré sur la question grâce à la loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données[673]. Il faut souligner que cette loi a été modifiée par la loi fédérale de protection des données du 20 décembre 1990 amendée par la loi du 14 septembre 1994. Ce n'est qu'en 1978 que la France a finalement adopté la loi informatique et libertés alors qu'elle fait partie du fait de ses travaux précurseurs depuis les années 1974.

---

[671] L'étude comparative a été réalisée à partir des documents figurant sur cette page de la CNIL : http://www.cnil.fr/fileadmin/documents/.../panorama-legislation.pdf.

[672] Cf. **G. LANGROD**, Vie administrative à l'étranger: essai de conciliation en Suède du libre accès aux dossiers administratifs et de l'existence de banque de données, in *la Revue administrative*, 27e année, n°157 (Janvier –Février 1974),pp.69-71, Presses Universitaires de France ; **J. FRAYSSINET**, l'informatique et le secret des fichiers, in *La Revue administrative* 30e année, n° 176, mars-avril 1977, p.175-185, PUF ; Bernitz Ulf, La protection des consommateurs en Suède et dans les pays nordiques in *Revue internationale de droit comparé*, Vol. 26 n°3, Juillet-septembre 1974. pp. 543-576.

[673] Disponible sur : http://www.datenschutz.de : des Bundesbeauftragte für den Datenschutz

Dans cette même année, l'Autriche, le Danemark, et certains pays de l'Espace Economique Européen comme la Norvège ont fait de même.

Si la mise en place de législations sur la protection des données personnelles s'est faite aussi tôt, c'est-à-dire dès les premières heures du développement des réseaux numériques pour les entreprises et les particuliers, il convient de remarquer que cette action des législateurs est visionnaire.

Puisque la protection des données personnelles implique de mesurer les activités numériques comment ces organes gèrent-ils par exemple les flux d'échanges ?

a- L'organisation générale de la protection des données personnelles par la CNIL

La Commission Nationale de l'Informatique et des Libertés en France est une autorité administrative indépendante dont la vocation est à la fois d'anticiper les possibles dérives liées à l'usage des outils communicationnels et de répondre aux préoccupation des usagers en les en informant et en recevant leurs plaintes.

Elle a également pour mission de recevoir les plaintes en cas d'infractions réalisées et de sanctionner les contrevenants à certaines dispositions législatives.

Comment est organisée la CNIL ? Quel est son mode de fonctionnement ?

1- Composition et Organisation

La CNIL est composée de 17 membres dont 12 sont élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent. La CNIL a à sa tête un président élu par les autres membres de la Commission et il s'agit à l'heure où nous écrivons de Madame Isabelle FALQUE- PIERROTIN. Son équipe se compose de la manière suivante :

- 4 parlementaires soit 2 députés et 2 sénateurs désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste[674] ;

---

[674] cf. 1° de l'article 13 de la loi Informatique et Libertés modifié par la loi n°2011-525 du 17/05/2011 art.54.

- 2 membres du Conseil économique, social et environnemental[675]élus par cette assemblée ;
- 6 représentants des hautes juridictions répartis comme suit : deux membres ou anciens membres du Conseil d'État, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'État[676], deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation[677], et deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes[678].

- 5 personnalités dont deux qualifiées pour leur connaissance de l'informatique sont désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat[679].

Les trois autres de ces personnalités sont qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles et nommées par décret[680]. La durée du mandat des commissaires est de 5 ans. En ce qui concerne les parlementaires, la durée du mandat dépend de celle de leur mandat électif.

Dans son rapport d'activité 2011, la CNIL a ainsi exposé les chiffres clés en termes d'actions et une analyse de ces données permettra de faire la lumière sur son activité en matière de lutte contre la cybercriminalité[681].

Pour une meilleure appréciation des évolutions ou des échecs de cet organisme, il sera intéressant de comparer les actions dans chaque Etat membre.

---

[675] cf. 2° de l'article 13 de la loi Informatique et Libertés, modifié par la loi organique n°2010-704 du 28/06/2010 art.21

[676] cf. 3° de l'article 13 de la loi Informatique et Libertés.

[677] cf. 4° de l'article 13 de la loi informatique et Libertés

[678] Cf. 5° de l'article 13 de la loi Informatique et Libertés.

[679] cf. article 13, 7° de la loi informatique et Libertés modifié par la loi n° 2011-334 du 29/03/2011 art. 1

[680] cf. article 13, 6° de la loi informatique et libertés

[681] CNIL, 31ème rapport annuel, la documentation française ; consulté en ligne le 28 novembre 2011 et http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf

Il apparaît important d'effectuer une comparaison à partir de la date de création de chacun de ces organes dans l'Union Européenne.

Sur un plan régional, la CNIL ne possède pas encore d'antennes. Ces antennes régionales permettraient un travail de qualité au sein des régions et faciliteraient la coordination avec les services centraux de Paris. Cette répartition décentralisée non encore établie de la CNIL a fait l'objet en 1998 d'une question sénatoriale. En effet, le Sénateur Serge MATHIEU avait posé une question écrite[682] n° 07 281, relative à la déconcentration de la CNIL. Il interrogeait le ministère de la justice sur la création d'antennes régionales de la CNIL. Au cours de son mandat, de 2004 à 2011, le Président de la CNIL, Monsieur Alex TÜRK, a présenté un projet de déconcentration de la CNIL afin de faciliter le travail de l'autorité et assurer la qualité de ses services. Sa proposition n'a eu qu'une réponse partielle dans la mesure où à l'heure actuelle, la CNIL ne possède pas d'antennes décentralisées au niveau régional mais il est possible de désigner un représentant au niveau des entreprises privées et des administrations publiques. Ces représentants de la CNIL sont appelés des Correspondants Informatique et Libertés[683] (CIL) ou encore Correspondant à la Protection des données personnelles (CPDP). La Commission recommande de désigner des Correspondants Informatique et Libertés pour qu'ils assurent les missions de protection des données et de suivi des activités de sécurité informatique. Ils sont munis d'équipements nécessaires (comme par exemple des lignes extranet) pour les missions dont ils ont la charge.

Cette organisation particulière fait appel à une comparaison de la Commission Informatique et Libertés en France et l'organisme correspondant en Allemagne, pays organisé en Etats fédérés et fédération.

2- Fonctionnement

---

[682] Question écrite n° 07-281 publiée au JO Sénat du 02/04/1998, p. 1012.

[683] L'institution du Correspondant Informatique et Libertés date de la loi n °2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés publiée au JORF n°182 du 7 août 2004 page 14063.

En France, la CNIL accorde des autorisations aux requérants pour effectuer des traitements de données. Il en va de même lorsqu'il s'agit pour ces requérants d'utiliser des adresses des personnes physiques ou morales à des fins professionnelles. C'est ainsi que l'article 51 de la loi du 6 août 2004 renvoie aux dispositions du code pénal et plus particulièrement à l'article 226-16. Cet article dispose que : « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »

Il ressort de cette disposition que le législateur français est particulièrement attaché au respect des formalités requises par la loi et il veut surtout respecter les principes fondamentaux, la liberté de communiquer ou la liberté de refuser de faire connaître les données personnelles par exemple.

Si les démarches administratives prescrites ne sont pas respectées, soit les autorisations aux fins de traitement de données ne sont pas accordées, soit, dans l'hypothèse où elles auraient déjà été accordées, les responsables de traitement peuvent faire l'objet de sanction allant du simple avertissement au retrait de l'autorisation.

Il faut souligner que dans le cadre de la répression de la cybercriminalité, la CNIL intervient en amont[684]. En effet, c'est dans le cadre de contrôle des obligations relatives au traitement des données des entreprises que la CNIL applique la loi informatique et Libertés. La CNIL sera essentiellement sollicitée pour des prospections commerciales abusives ou encore de personnes indûment fichées par la Banque pour des incidents de paiement. Dans d'autres cas la CNIL prononce des sanctions. C'est ainsi qu'

[684] L'interview téléphonique de Monsieur Didier GASSE, responsable des communications électroniques à la CNIL, a été l'occasion pour ce membre de la formation restreinte de l'institution de nous mentionner cette intervention en amont.

ACADOMIA, structure de cours à domicile destinés aux particuliers, a été condamnée pour avoir publiés dans les fiches clients, des mentions injustes et fausses à l'endroit de certains de ses employés, professeurs à domicile[685].

En ce qui concerne la cybercriminalité, les infractions graves ne sont pas réellement du ressort de la CNIL mais des instances pénales judiciaires. Et pourtant certains secteurs comme la liberté d'expression ou la protection des données par l'Etat, devraient être gérés par la CNIL ou du moins les limites de ces libertés pourraient être du ressort de cette autorité administrative indépendante. En effet, les questions de la surveillance des individus par les Etats s'appuient sur des objectifs de protection et au nom de la protection des citoyens, les Etats surveillent toutes les communications. A rebours, et au nom de la liberté d'expression, les individus s'expriment, via les réseaux sociaux, les réseaux numériques et internet. Dans ce cadre, la CNIL et les institutions équivalentes doivent avoir un pouvoir de contrôle et de sanction suffisant pour mettre les limites.

Par contre, il existe des domaines dans lesquels la CNIL va apporter une réelle expertise technique. Il s'agit des domaines comme celui des données sensibles c'est-à-dire les données médicales, ou encore les questions de sécurité informatique. Le maximum de garanties est mises en place par la CNIL via la loi informatique et Libertés afin d'éviter les fraudes.

D'ailleurs, dans le cadre des interventions en amont, la CNIL vient de voir sa collaboration avec l'Etat renforcée avec la signature de la convention avec l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) en date du vendredi 11 janvier 2013 à la suite de la visite du

---

[685] Délibération n° 2010-113 du 22 avril 2010 de la formation restreinte portant avertissement à l'encontre de la société AIS 2 exerçant sous l'enseigne ACADOMIA (cette décision a fait l'objet d'un recours devant le Conseil d'Etat) et voir également sur le site de la CNIL sous le lien http://www.cnil.fr/la-cnil/actualite/article/article/la-cnil-adresse-un-avertissement-a-acadomia-pour-des-commentaires-excessifs-dans-ses-fichiers/. Complément avec l'article d'**Alexandra GONZALEZ** paru dans le journal France Soir du 28 mai 2010 intitulé : « *le PDG d'ACADOMIA défend le fichage* » et l'article de **Luc CEDELLE** et **Franck JOHANNES** dans Le journal Le monde du 29 mai 2010 : « LA CNIL adresse un sévère avertissement à l'entreprise de soutien scolaire Acadomia ».

Ministre de l'intérieur Manuel VALLS à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (O.C.L.C.T.I.C)[686].

Des domaines d'interventions précis de la CNIL sur des questions pointues méritent d'être explicités dans le cadre de la cybercriminalité.

α. Les cookies dans la protection des données personnelles des individus.

Les cookies sont des fichiers placés sur le disque dur de l'ordinateur de l'internaute lorsqu'il visite un site Internet permettant au fournisseur de contenu ou à la régie publicitaire de stocker un certain nombre d'informations relatives à ses habitudes de navigation[687].

Les cookies offrent ainsi la possibilité de proposer à l'internaute des publicités portant sur des produits susceptibles de l'intéresser et plus globalement permettent une navigation fluide sur Internet. A titre d'illustration, si vous avez l'habitude de consulter des sites de voyage à destination des pays d'Afrique, à chaque fois que vous vous mettrez sur un navigateur de recherches internet, des publicités relatives aux billets d'avion à destination des pays pour lesquels vous consultez occasionnellement des informations s'affichent dans la bannière publicitaire des pages internet. Vous n'avez nul besoin de les avoir sollicités au préalable. Grâce aux cookies, ces informations sont stockées et montrent par la même occasion que votre adresse IP est localisée et répertoriée dans la base de ces régies publicitaires.

La question ici se pose de savoir à quelle hauteur les cookies pourraient favoriser des actes cybercriminels ?

Dans l'option affirmative, en quoi la CNIL contrôle ou encadre ces cookies dans la protection des données personnelles des individus ?

---

[686] Cf. La cybercriminalité au centre de la visite des ministres de l'Intérieur et de l'Innovation et de l'Économie numérique voir sur le site du ministère de l'intérieur : http://www.interieur.gouv.fr/fr/Actualites/L-actu-du-Ministere/Lutte-contre-la-cybercriminalite; voir également http://pro.clubic.com/it-business/securite-et-donnees/actualite-535480-cnil-cyberpolice-europe.html

[687] Anne-Laure Falkman Counsel, August & Debouzy, Cookies : l'« opt-in » va-t-il changer les choses ? Contrats Concurrence Consommation n° 10, Octobre 2011, alerte 73.

Sur la question de savoir si les cookies sont une source de la commission d'actes cybercriminels, il convient pour répondre de se référer à la nature des infractions visées. Par exemple, plusieurs actes de nature cybercriminelle ont pour commencement d'exécution les intrusions dans les systèmes informatiques. Or, l'acceptation sans réserve, et régulière des cookies pourrait constituer une porte ouverte aux cybercriminels. Il s'agit pour ces derniers d'utiliser ces fichiers pour y glisser des fichiers espions de nature à infecter le système informatique de l'internaute acceptant. C'est pour éviter les intrusions frauduleuses que la loi régule l'acceptation des cookies.

Le texte régulateur est la directive n° 2002/58/CE du 12 juillet 2002 dite Directive « vie privée et communications électroniques »[688] au terme de laquelle le régime applicable aux cookies est passé d'un régime d'« opt-out » à un régime d'« opt-in ». Qu'est-ce que le régime opt-out ?

Tandis que l'opt-in renvoie au système de consentement préalable, l'opt-out revient au mécanisme fondé sur le droit d'opposition. Ainsi, dans l'opt-in, il est exigé une *demande pour marquer le consentement, il faut un acte positif d'inscription à savoir par exemple le fait de « cocher la case pour recevoir la newsletter »*[689]. Depuis 2002, la règle de mise en matière de prospection commerciale est l'opt-in. S'agissant de l'opt-out, il induit le consentement de l'utilisateur par défaut mais il est possible de se désinscrire et c'est le message « cochez la case pour ne plus recevoir la newsletter ».

La CNIL en France intervient quant aux incriminations des actes relatifs aux données personnelles dès lors qu'il s'agit d'expliquer, d'informer les populations. Elle le fait généralement via son site internet aux moyens de documents sous forme de question. C'est notamment le cas récemment avec la loi relative au délit d'usurpation d'identité. Elle opère un double point juridique et technique dans un article publié le 17 mars 2011 -

---

[688] Directive du Parlement européen et du Conseil du 12 juillet 2002 n° 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) publiée au JOCE du 31 juillet 2002 L 201 p. 0037-0047

[689] Cf. **MATTATIA F.**, Traitement des données personnelles, parue aux éditions Eyrolles, à Paris, en 2013, p. 25.

donc après promulgation de la loi - intitulé « L'usurpation d'identité en questions ». A ce propos, la CNIL n'hésite pas à qualifier de vol d'identité, ce nouveau délit surtout sur Internet, pour le grand public.[690]Avec le décret n° 2011-2023 du 29 décembre 2011 relatif aux pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés[691], la CNIL voit ses pouvoirs de sanctions s'accroitre.

D'ailleurs à ce titre, il convient de noter que les sanctions prononcées par la CNIL sont graduelles et obéissent à un ordre chronologique précis. Cette chronologie traduit le suivi des dossiers notamment de plaintes qui lui sont adressées. En témoigne les sanctions prises par la CNIL depuis le 28 juin 2006[692]. Il n'est pourtant pas sous-entendu qu'aucune sanction n'ait été prononcée avant cette date. Que peut-on tirer de l'analyse des sanctions prononcées par la CNIL en comparaison des tribunaux judiciaires ?

Dans le cadre du traitement des données par des organismes, la CNIL est appelée à effectuer des contrôles. Partant, elle a la possibilité de prononcer un avertissement contre le responsable qui ne respecte pas les obligations de déclaration prévues par la loi Informatique et Libertés. Il s'agit là du premier échelon des coercitions. Si le responsable reste inactif face à cet avertissement de l'autorité indépendante, la CNIL le met en demeure de faire cesser le manquement et ce, dans un délai qu'elle lui fixe. L'échelon suivant est celui de la sanction pécuniaire prévue à l'article 47 de la loi précitée. Il peut arriver que la sanction pécuniaire fasse effet et que le responsable du traitement se mette en règle. Dans le cas où il ne le fait pas, la quatrième étape est franchie et il se voit adresser une injonction de faire cesser le traitement (si ce dernier relève de l'article 22 de la loi) ou alors l'injonction contient le retrait de l'autorisation accordée dans l'hypothèse où le traitement est relatif à l'article 25. Il s'agit donc d'une réelle gradation de la punition puisqu'on passe de l'avertissement au retrait de l'autorisation.

---

[690] Cf. : http://www.cnil.fr/vos-libertes/vos-droits/details/article/lusurpation-didentite-en-questions

[691] Revue de science criminelle 2009 p. 317.

[692] Article L 121-1 du code de la consommation

Une illustration d'avertissement public est la condamnation de la société Pages jaunes par la décision de la CNIL[693] en date du 21 septembre 2011 l'avertissant pour avoir aspiré des contacts sur des réseaux sociaux. Cette sanction a été validée par le Conseil d'Etat dans un arrêt[694] du 12 mars 2014. Des faits, il ressort que sans recueillir le consentement des personnes concernées, le site PagesBlanches s'est servi d'informations aspirées automatiquement sur les réseaux sociaux tels que Facebook, Copains d'avant, Viadeo, Linkedin, Twitter et Trombi, pour enrichir ses pages d'annuaire téléphonique. Ces informations collectées se composent des noms, prénom, photographies, établissements scolaires, employeurs, profession et localisation géographique des internautes avaient ainsi été collectés et agrégés sur les Pages blanches, aux côtés du numéro de téléphone de la personne recherchée.

Il n'est cependant pas exclu pour les parties plaignantes de poursuivre le responsable du traitement à la fois devant la CNIL et les juges judiciaires.

La CNIL traite d'une manière générale les données à caractère personnel parmi lesquelles les données médicales, dites sensibles. Quelle protection leur est réservée ?

b- La protection des données médicales

En matière de santé, les nouvelles technologies de l'information jouent également un rôle dans la mesure où les données médicales sont désormais exportables. Se pose alors la question de savoir en quoi la CNIL en France et les organes correspondant au sein de l'Union Européenne parviennent à exercer leur mission de contrôle. Par ailleurs, en cas de dérives quelle politique est mise en place en terme de prévention ou de sanction ?

---

[693] Cf. Délibération de la formation restreinte n°2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes, disponible sur légifrance: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000024583206

[694] Cf. Conseil d'État, 10ème et 9ème sous-sections réunies du 12 mars 2014, numéro de pourvoi 353193, disponible sur légifrance : http://legifrance.gouv.fr/affichJuriAdmin.do;jsessionid=B37532A10ACBDA5163CD84BCAE7060FE.tpdjo07v2?oldAction=rechJuriAdmin&idTexte=CETATEXT000028717840&fastReqId=813207794&fastPos=44

Dans ce cadre, il conviendra d'analyser les problèmes juridiques qui naissent et auxquels seront confrontés les autorités, une fois les problèmes éthiques envisagés[695].

Dans cette optique, se posent des problématiques, de sécurité des données communiquées et des difficultés liées à la confidentialité de ces données.

L'Organisation Mondiale de la santé (l'OMS) a constamment recours aux systèmes d'information et de la communication. C'est pourquoi, elle s'est dotée d'une politique de prévention des risques, d'atteinte, de fraude et surtout de protection. Cette politique règlemente tous les secteurs usagers de ces systèmes d'information et de communication s'agissant aussi bien de l'utilisation personnelle des employés que de toute autre. Il existe tout de même un domaine non règlementé par l'Organisation Mondiale de la santé : la protection des données médicales. Leur protection est laissée à l'appréciation nationale des Etats[696]. L'OMS n'a donc pas de politique prévue en ce sens.

S'agissant de l'utilisation des données médicales (relatives à la santé, aux données génétiques), considérées comme des données sensibles, il existe au Luxembourg un règlement. Il s'agit du règlement Grand-ducal du 2 octobre 1992 portant spécialement sur les conditions et les modalités de l'utilisation des données nominatives dans les banques de données médicales, sur l'utilisation à des fins thérapeutiques, à des fins de recherche et leur communication à des tiers[697]

La prise en compte des enjeux de la protection des données médicales passe par la compréhension qu'en font les professionnels du domaine de la sécurité informatique. Ce sont eux qui en parlent le mieux dans la mesure où ils sont au fait de la question compte tenu des risques qu'ils côtoient au quotidien. C'est dans ce cadre que Monsieur Philippe

---

[695] Les aspects juridiques et éthiques de la protection des données issues du dossier médical informatisé et utilisées en épidémiologie, Santé Publique 2006, volume 18, n° 1, pp.107-117

[696] Information recueillie auprès de fonctionnaires de l'OMS, Genève à la suite d'interviews avec la collaboration de Monsieur Sergio YACTAYO du Programme des maladies épidémiques « Control of Epidemic Diseases (CED) Pandemic and Epidemic Diseases (HSE/PED) et madame Chantal STREIJFFERT GARON du département légal de l'OMS.

[697] Cf. http://www.cndp.public.lu/fr/index.html

Corneloup, Responsable Ventes Secteur Public, chez Fortinet[698] en France intervient quant à la protection des données médicales dans une interview de parue dans le CIO MAG.com[699]. Selon cet expert de sécurité de systèmes, il existe divers risques liés au piratage des données de santé ou des données médicales. Il s'agit de :

- un risque vital pour les patients

- un risque juridique pour les professionnels et établissements de santé (parce que leur responsabilité peut être engagée)

- un risque financier pour les établissements de santé.

Il découle de ce qui précède l'exigence législative d'une protection des données par une politique de sécurité. Le non-respect de ces exigences est sanctionné de 2 ans de prison et 300 000€ d'amende.

En France, le cadre légal de la télémédecine et de la télésanté est défini par la loi **n°** 2009-879 du 21 juillet 2009 dite loi Hôpital, Patients, Santé et territoires portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires[700] et le décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine[701]**.**

L'étude européenne réalisée par l'organisme DECISION[702] pour la Fédération des Industries Electriques, Electroniques et de Communication (FIEEC) et pour l'Agence des Systèmes d'Information partagés de Santé (ASIP) permet de mettre en lumière les responsables de la protection de la circulation des données médicales.

---

[698] FORTINET est une entreprise de sécurisation des systèmes et réseaux informatiques créé en 2000.

[699] Philip Corneloup, L'urgence d'une véritable sécurisation des systèmes de santé, CIO Mag.com, Février/ Mars 2013, n°25, p.13-15.

[700] Loi n° 2009-879 du 21 juillet 2009 dite loi Hôpital, Patients, Santé et territoires portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, publiée au JORF n°0167 du 22 juillet 2009 page 12184 texte n° 1.

[701] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, publié au JORF n°0245 du 21 octobre 2010 page texte n° 13.

[702] Cf. Etude sur la Télésanté et Télémédecine en Europe réalisée par DECISION pour la Fédération des Industries Electriques, Electroniques et de Communication (FIEEC) et pour l'Agence des Systèmes d'Information Partagés de Santé, Mars 2011.

En effet, il ne s'agit pas des compétences de la CNIL ou des institutions équivalentes qui organisent simplement le cadre des applications légales établies. Cette protection relève de la volonté politique des institutions de l'Etat ainsi que d'une coordination des organismes de santé et autres structures en relation avec la médecine.
De la sorte, ce sont des entités du type MEDCOM, au Danemark notamment, qui prennent en charge et assurent la protection des données médicales. Le MEDCOM regroupe des autorités publiques, des organisations et des établissements privés du secteur de la santé au Danemark. Il en est de même du NICTIZ aux Pays-Bas, qui comprend en son sein les assurances publiques et privées, professionnels de la santé et patients, administrations publiques et industriels.

La protection[703] des données à caractère personnel par la CNIL ne suffit pas. Ces données sont inter-changées au niveau de l'Etat français certes (entre les administrations et les entreprises) mais aussi au niveau de l'Europe et de l'international. Les règles établies au sein de la France n'ont pas spécialement vocation à régir l'ensemble des relations intervenant en dehors du territoire. C'est pourquoi, l'intervention des autres commissions en charge de la protection des données à caractère personnel mérite d'être étudiée.

Il est important de mentionner les questions relatives au dossier médical personnalisé surtout dans les cas dans lesquels les patients d'un Etat de l'Union (par exemple un français) vont se faire soigner dans un autre pays (Italie ou Espagne). C'est l'hypothèse des opérations chirurgicales lourdes pratiquées à l'extérieur de la France notamment pour des raisons financières. Comment les données des patients transférées ou échangées entre les différents centres hospitaliers sont-elles protégées ?

1- La sécurité des données médicales

[703] Il est question essentiellement de protection par des textes uniquement et des avis émis par la CNIL.

La sécurité des données médicales se rapporte à la gestion des instruments comme le dossier médical personnalisé[704] ou encore la protection des données échangées entre hôpitaux et organismes de santé. Ces données échangées servent de base aux prescriptions médicales numériques. *D'ailleurs, une donnée médicale non fiable peut conduire à la mort du patient*[705]. C'est pourquoi l'ensemble des informations contenues dans le dossier médical personnel du patient ou encore les données recueillies sont importantes et leur intégrité doit être constamment garantie.

Le dossier médical personnalisé[706] est défini comme un dossier informatisé et accessible par internet créé pour chaque bénéficiaire de l'assurance- maladie[707].

Le dossier médical personnalisé soulève des questions relatives à la protection des données qu'il contient. Le traitement de ces données est encadré mais cet encadrement juridique est-il toujours respecté par les professionnels lors des échanges de ces informations des patients ?

Il faut savoir que le dossier médical est un mécanisme en phase de tests au niveau des hôpitaux publics et des professionnels de santé. Les dispositifs techniques ne sont pas encore tout à fait établis et les normes juridiques se créent au fur et à mesure de la pratique de cet arsenal dans le milieu des professionnels de santé.

A côté du dossier médical personnalisé, les données médicales sont également concernées lorsqu'elles sont collectées par des appareils médicaux notamment dans le cadre de traitement de maladies cardiaques par exemple. Pour des interventions chirurgicales de patients portant des appareils ou devant être implantés de Pacemaker, ou encore en attente de recevoir des changements d'appareils vitaux comme des valves

---

[704] Dans son article « *Informatisation et confidentialité des données médicales* », parue dans la revue *Laennec*, 2007/1 Tome 55, p. 12-22, **BRODIN Marc** soulève les inquiétudes liées au dossier médical personnalisé comme par exemple le manque suffisant de confidentialité des données médicales qui transitent par la voie informatique.

[705] Cf. **CARTAU Cédric**, La sécurité du système d'information des établissements de santé, Presses de l'Ecole des Hautes Etudes en Santé Publique, 2012, p. 31.

[706]Cf. **MORVAN** Odile, « L'e-dossier médical personnel » Est-ce que j'ai le choix ?, *VST - Vie sociale et traitements*, 2004/4 n° 84, p. 38-45.

cardiaques, les appareils de collecte de données (ici le rythme cardiaque et la fréquence des battements du cœur du patient) comme des KOLTER contiennent des informations importantes retraçant la vie des patients. Ces données collectées doivent être protégées en tant données sensibles et leur intégrité doit être conservée.

Les applications mises en place pour garantir les transferts de patients avec un même dossier médical d'un médecin à l'autre sont au stade de l'expérimentation au niveau de l'Europe[708].

2-Les médicaments contrefaits

Il s'agit d'un autre type de cybercriminalité qu'on peut qualifier de cybercriminalité médicale. Ce sont des fraudes et des contournements légaux qui surviennent dans l'utilisation de ces instruments numériques au service de la santé comme par exemple la vente illégale en ligne de médicaments. Comment est sanctionnée cette vente illégale en ligne ?

L'ordonnance n° 2012-1427 du 19 décembre 2012 relative au renforcement de la sécurité de la chaîne d'approvisionnement des médicaments, à l'encadrement des médicaments sur Internet et à la lutte contre la falsification des médicaments est introduite dans le code de la santé pour réglementer ce domaine de vente en ligne des médicaments[709].

La protection des données médicales est particulière dans la mesure où ces données sont catégorisées comme des données sensibles par la loi informatique et libertés comme des données sensibles. C'est dans le respect de ce concept que la CNIL s'est prononcée quant à l'exploitation des feuilles de soins électroniques à des fins

---

[707]Cf. G.**DESGENS-PASANAU**, la protection des données à caractère personnel, la loi « Infomatique et libertés » Lexisnexis., Paris 2012, p. 131-132.

[708] Cf. Revue au cœur de l'e-santé n° 2 juillet 2012 et n° 3 février 2013.

[709] Cf. Ordonnance n° 2012-1427 du 19 décembre 2012 relative au renforcement de la sécurité de la chaîne d'approvisionnement des médicaments, à l'encadrement des médicaments sur Internet et à la lutte contre la falsification des médicaments publiée au JORF n°0297 du 21 décembre 2012 page 20182 texte n° 11. Voir également Focus, *Les Tribunes de la santé*, 2013/1 n° 38, p. 11-20.

d'études statistiques retraçant l'usage des médicaments. Les données utilisées, du fait de leur statut de données sensibles, sont anonymisées afin d'en assurer la sécurité.

Dans la délibération du 8 septembre 2011, la CNIL a autorisé une société, la société Celtipharm, qui avait collecté des données de santé contenues dans les feuilles de soin de plusieurs usagers, à utiliser ces données dans une étude épidémiologique. Par un arrêt du 26 mai 2014, le Conseil d'Etat[710] vient valider cette autorisation qui avait fait l'objet d'un recours en excès de pouvoir, formé par la société *IMS Health*.

Les questions relatives aux médicaments contrefaits vendus via les réseaux numériques sont abordées sous l'angle des risques et du déplacement de la responsabilité médicale. Dans l'article, Viagra 2.0 et contrefaçon[711], les auteurs, PRZYSWA Éric et GUARNIERI Franck soulignent les principaux risques liés à la vente en ligne de médicaments : il s'agit d'abord de risques informationnels car les patients deviennent des consommateurs d'informations qu'ils hiérarchisent : et c'est alors traduit par le fait pour un consommateur de lire plusieurs sites pour se documenter sur un produit sans pour autant passer par un médecin ou un pharmacien.

Il est ensuite question de risques sanitaires (dans la mesure où très peu de contrôles et d'analyse sont effectués quant à la fabrication de ces médicaments et à leur transport puisqu'ils passent par des circuits physiques. Les conditions de conservation ne sont pas les mêmes que celles des médicaments vendus par des pharmacies, qui, eux suivent des processus de contrôle prévus par les lois médicales. Et enfin, il s'agit de risques de faire de certains consommateurs habitués des distributeurs et dans ce cas, plusieurs cybercriminels russes ont filtré des réseaux créant ainsi une maffia. Ce dernier risque, qui est criminel conduit à la création de réseaux de médicaments contrefaits.

---

[710] Cf. Conseil d'état Section du contentieux – 10ème et 9ème sous-sections Décision du 26 mai 2014

[711] Cf. **PRZYSWA E**. et **GUARNIERI F**., Viagra 2.0 et contrefaçon, *HERMES*, n°69, 2014, p. 183-185.

Ces différents problèmes traduisent selon les auteurs la crise normative. Internet est difficile à réguler et les médicaments qui transitent par les réseaux numériques sans respecter les normes établies traduisent cette difficulté.

Ces crises sont aussi liées au déplacement des responsabilités médicales.

Les questions de données personnelles sont relatives à divers domaines et révèlent la pluridisciplinarité des autorités comme la CNIL. Elles sont également complexes et exigent pour leur traitement des compétences et une assiduité dans les moyens mis en place. Comment ces différentes problématiques sont-elles abordées par les institutions équivalentes de la CNIL ?

B- La protection des données par les institutions équivalentes de la CNIL

La CNIL a des institutions équivalentes dans les autres pays de l'Union Européenne. Quelles sont les méthodes de travail bien que les règles de base soient les mêmes, compte tenu de l'appartenance à l'Union Européenne. Comment l'autorité de protection des données travaille-t-elle en Espagne? Existent-ils des ajouts ou des subtilités en Allemagne ?

a- L'Agence Espagnole de la Protection des Données

L'Agence Espagnole de la Protection des données est l'autorité en charge de la protection des données en Espagne. C'est une autorité administrative indépendante qui obéit à une organisation et un fonctionnement spécifique du fait des compétences réparties entre l'administration centrale de l'Etat, des dix-sept communautés autonomes, des provinces et des communes.

1. Organisation de l'agence espagnole de la protection des données

L'Agence est un organisme indépendant à part entière dans la mesure où son organe de direction est unique. Bien qu'il soit désigné par le gouvernement sur proposition du

Ministre dont la compétence est requise dans le secteur concerné, il ne reçoit de consignes ni d'instructions d'aucune autorité[712].

D'ailleurs, le pouvoir exécutif n'a aucun contrôle sur son activité. Elle dispose des pleins pouvoirs disciplinaires ainsi que de pouvoir de contrôle et de surveillance quant à la législation relative à la protection des données. Elle mène ses missions et ses activités grâce à ces différents pouvoirs qui lui sont conférés.

2. L'activité et les missions de l'Agence espagnole des données

L'Agence espagnole est l'une plus active parmi les autorités européennes en charge de la protection des données. Pour preuve, de cette assertion, elle a organisé du 4 au 6 novembre 2009, la réunion des Autorités en charge de la protection des données. Ce type de réunion des différentes autorités en charge de la protection des données est, pour elles, l'occasion d'échanger leurs expériences respectives.

En outre, l'Agence espagnole de la Protection des Données est au cœur des faits à l'origine de la condamnation de Google Spain dans l'arrêt de la Cour de Justice de l'Union Européenne du 13 mai 2014, affaire C-131/12 relatif au droit à l'oubli numérique[713].

Cette autorité espagnole axe essentiellement sa mission de contrôle dans l'éducation des entreprises au respect des dispositions de la loi informatique et des libertés grâce aux sanctions prises. C'est d'ailleurs par le biais des amendes infligées aux contrevenants qu'elle se finance[714]. La particularité de l'Espagne est son organisation en provinces et communes autonomes avec une administration centrale de l'Etat. Cette singularité influence la hiérarchisation des institutions et l'Agence de la protection des données n'échappe pas à cette règle.

---

[712] Cf. Etude de **Juan de la CRUZ FERRER,** Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié (Tome 2 : Annexes), Rapports d'office parlementaire,

[713] Arrêt de la Grande Chambre de la CJUE du 13 mai 2014, aff. C-131/12, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González.*

[714] Cf. Martin BAVIERE, La protection des données à caractère personnel, de la sensibilisation à l'éducation, Mémoire de Mastère Spécialisé en « Management et Protection des Données à Caractère Personnel » Sous la direction de M. Bernard FORAY ISEP promotion 2012/2013.

Qu'en est-il de l'Allemagne ?

b- Le Commissaire fédéral de la Protection des données en Allemagne

En Allemagne, c'est le Commissaire fédéral de la Protection des données qui est l'autorité en charge de la protection des données personnelles. Il est appelé le *Datenschutzbeauftragter* et sa désignation est obligatoire dans la mesure où il est le maillon-clé du système de protection en Allemagne[715]. L'Allemagne étant une République fédérale, il existe une autorité par Land et une autre commune à tous les Länder. Cette nomenclature est propre à la structure de l'Etat allemand et représente un gage de succès dans un domaine aussi sensible que la protection des données.

L'Allemagne organise la protection des données par Land. Chacune de ses provinces étatiques désigne un commissaire à la protection des données en charge des contrôles liés aux traitements informatiques de sa province. C'est une organisation par secteur qui tient compte des activités concernées mais également de leur envergure nationale (et dans ce cas c'est au Commissaire de la protection des données au niveau étatique qui a en charge les contrôle et les sanctions en cas d'entrave aux lois) ou régional.

Au niveau de l'Union européenne, il existe le Groupe dit « article 29 » qui réunit l'ensemble des commissions ou organismes en charge de la protection des données en caractère personnel. Quels sont les apports de ce groupe en matière de répression de la cybercriminalité ?

C- Au niveau européen : le groupe article 29

Les différentes autorités de contrôle en charge de la protection des données des individus dans l'Union européenne (27 autorités en tout) se réunissent et échangent régulièrement en vue de coordonner leurs actions.

---

[715] Cf. **A.V. KOSSI**, la protection des données à caractère personnel à l'ère de l'Internet, impact sur l'évolution du cadre normatif et nouveaux enjeux. Etat des lieux en France et en Allemagne, Peter Lang, Frankfurt am Main, 2011, p. 151.

En témoigne la régularité des conférences « Informatique et Libertés ».

Celle de 2009 a eu lieu à Madrid et avait été organisée par l'Agence espagnole de protection des données du 4 au 6 novembre. Cette rencontre est la plus importante consacrée à la vie privée au niveau mondial. Elle réunissait près de 80 autorités de protection des données, des représentants de la société civile, de l'industrie mondiale, de cabinets d'avocats internationaux, et d'autres autorités publiques. Au cours de ce forum, une résolution visant à établir des standards internationaux pour la protection de la vie privée et des données à caractère personnel.

Dans cette optique, le G29 essaie de lutter contre les cas d'incompétence des juridictions de l'Union européenne. En effet, il arrive que certains sites hébergés hors de l'union européenne constituent l'origine de commissions d'infractions en direction des ressortissants de l'union. Dans de telles hypothèses, les personnes se retrouvent devant une incompétence du juge de leur Eta et parfois même du juge communautaire. En guise d'exemple, l'ordonnance du TGI de Paris du 19 octobre 2006. A la suite de cette affaire qui n'est pas un cas isolé, le G29 a tenté d'exercer des pressions sur les prestataires de service[716].

Il s'est d'ailleurs prononcé sur les codes de conduites encore appelés les Binding Corporate Rules.

a- Les Binding Corporate Rules (BCR) : Codes de bonne conduite des entreprises.

A l'origine, les Binding Corporate Rules sont des règles instituées en vue de favoriser une bonne utilisation de l'internet au sein des entreprises. En ce qui concerne les entreprises, ces règles sont importantes dans la mesure où elles encadrent et désignent un code de conduite qui définit la politique interne d'un groupe en matière de transferts de données personnelles hors de l'Union européenne[717].

---

[716] Cf. Revue de science criminelle 2009, p. 317

[717] Pour la définition des Binding Corporate Rules en ligne http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/les-bcr/; Voir également la délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à

Toutes les entreprises ne sont pas concernées. Il s'agit essentiellement des multinationales exportant des données depuis leurs filiales situées au sein de l'Union européenne vers des pays tiers[718] n'assurant pas un niveau de protection équivalent à celui de l'Union européenne.

Elles sont également des règles prises en relai du Safe Harbor pour les données en direction des États-Unis. Le Safe Harbor est un ensemble de règles auxquelles adhèrent les entreprises américaines qui souhaitent recevoir des données en provenance de l'Union Européenne. Les principes du Safe Harbor ont été élaborés par le Département du commerce américain surtout pour les entreprises exportatrices de biens ou de services. En collaboration avec l'Union Européenne et la Suisse notamment, ce programme a été élaboré et est entré en vigueur en octobre 1998. Un site est dans le même temps mis en place pour informer et faciliter l'adhésion des entreprises intéressées. Il s'agit du http://export.gov/safeharbor/. C'est au groupe 29 qu'est confiée la charge des documents relatifs à l'accord Safe Harbor[719].

b- D'autres domaines propres à la cybercriminalité

Le Groupe de l'article 29 se charge de divers domaines dédiés essentiellement à la cybercriminalité. Il s'agit de la protection des données médicales, dites données sensibles et des objets « connectés ».

1- Dans le domaine des données médicales

La protection des données médicales est particulièrement délicate. Et c'est essentiellement sur les questions relatives aux puces d'identification par radiofréquence (RFID) que le groupe des autorités de protection s'est prononcé quant au domaine des données de santé dans son avis 9/2011 sur la proposition révisée des entreprises relative

---

caractère personnel relatifs à la gestion de clients et de prospects (norme si mplifiée n° 48) cf. JORF n°0162 du 13 juillet 2012 page texte n° 72

[718] Ces pays sont notamment les Etats non membres de l'Union européenne, ou encore les pays d'Afrique

[719] En témoigne l'élaboration de projet de documents de travail relatif à la sphère de sécurité, traduction en français de *Safe Harbor* cf. Projet de document de travail sur le fonctionnement de l'accord "Safe Harbor" Adopté le 2 juillet 2002

au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) adopté le 11 février 2011[720].

2- Pour les objets connectés

Les objets connectés hormis le corps humain appellent des réflexions sur la santé mobile. En effet, des applications sont aujourd'hui développées sur des Smartphones et autres appareils de communication. Quel encadrement pour ces données stockées dans ces mémoires mobiles ? Les interventions du groupe article 29 sur les questions prennent surtout la forme d'avis ou de recommandations. C'est dire que le cadre légal n'est pas encore complètement fixé. Ces questions nouvelles sont au stade de réflexion de la mise en place de leur encadrement. Il s'agit de travaux de réflexion et d'élaboration de politiques.

Sur les questions de mobiles, le groupe article 29 a, en 2013 émis un avis *Opinion 02/2013 on apps on smart devices*[721]. Cet avis concerne les applications sur les appareils mobiles d'une manière générale.

Pour poursuivre leur action sur les nouvelles préoccupations nées des *objets intelligents*, les autorités de protection des données réunies ont émis un avis du 16 septembre 2014 intitulé « *l'Internet des objets »*[722] afin de proposer des recommandations sur les objets connectés. Ces recommandations s'adressent pour l'essentiel aux opérateurs afin qu'ils facilitent la mise en conformité des objets avec les règlementations européennes déjà établies.

S'agissant des questions de santé en ligne ou de santé mobile, le Groupe article 29 a effectué des travaux en appui avec le Conseil National de l'ordre des médecins

---

[720] Cf. Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) adopté le 11 février 2011, 00327/11/FR WP 180.

[721] Cf. Opinion 02/2013 on apps on smart devices, 00461/13/EN WP 202, adopté le 27 février 2013.

[722] Cf. Opinion 8/2014 on the on Recent Developments on the Internet of Thing, Adopted on 16 September 2014.

(CNOM). En 2014, en collaboration avec la Commission européenne, le CNOM a travaillé sur les questions de santé mobile et le groupe article 29 a pris part à ces séances de réflexion sur ces questions importantes.

D'autres secteurs enfin comme l'intervention des services répressifs ont fait l'objet de travaux du groupe article 29.

3- L'intervention des technologies de détection dans le travail des services répressifs et d'autres services de sécurité

Le groupe article 29 a émis un avis 1/2007 sur le Livre vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité[723].

Selon les observations du groupe de travail, certaines définitions trop larges comme les technologies de détection posent problème. Le groupe a dès lors recommandé une distinction précise pour un domaine où il est techniquement possible de tout faire. C'est dans ce cadre que le groupe « article 29 » estime *qu'il est essentiel pour toute évaluation future d'opérer une distinction claire entre les différents types de technologies de détection (la télévision en circuit fermé, les étiquettes d'identification par radiofréquences, la biométrique, etc.) afin de leur adapter spécifiquement les solutions de protection des données.*

La précision est donc un gage de sécurité et permet ainsi de garantir l'efficacité des mesures mises en place.

Outre les organismes étatiques et européens en charge des données, d'autres organismes avec différentes attributions interviennent dans la mise en œuvre de la stratégie coercitive de la cybercriminalité.

§2- La contribution d'autres organismes complémentaires

[723] Cf. Avis 1/2007 sur le Livre vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité adopté le 09 janvier 2007,

Créer des structures complémentaires pour assure une sécurité et surtout une répression efficace est l'originalité trouvée par les pouvoirs publics des Etats de l'Union européenne. La complémentarité s'apprécie par rapport au rôle d'appui assigné à ces entités d'étendue nationale, régionale ou même internationale. Le cas particulier de la France permet de se rendre compte de cette pléthore d'organismes créés pour renforcer les moyens de lutte existant déjà.

D'autres exemples d'Etats voisins facilitent la comparaison pour desceller les similitudes et les apports des uns par rapport aux autres. En ce sens, le cas du Royaume Uni pourra être présenté.

L'approche européenne mérite d'être abordée compte tenu de l'aspect transversal et sans frontière de la plupart des actes cybercriminels.

A- Le cas particulier de la France

Dans la lutte quotidienne contre la cybercriminalité, plusieurs institutions ont été mises en place. Elles sont affectées à des services ou rattachées à des administrations déjà existantes.

La police, la gendarmerie et les différents services du Ministère de l'intérieur se voient ainsi affectes des effectifs au niveau des agents afin d'assurer une action coordonnée et efficace sur tous les plans. Ces institutions sont régies par des décrets portant leur création et sont, par la suite, insérés dans le code pénal et le code de procédure pénale.

Au plan national français, l'agence nationale de la sécurité des systèmes d'information (ANSSI), le centre d'expertise gouvernemental de réponse et de traitements des attaques informatiques (CERTA), l'office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC), la direction centrale du renseignement intérieur (DCRI) et la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI) sont des entités nouvelles agissant en application des textes de lois édictés.

a- Le Secrétariat Général de la Sécurité et de la Défense Nationale

Le Secrétariat Général de la Sécurité et de la Défense Nationale (SGDSDN) assiste le Premier ministre dans ses missions de défense et de sécurité nationale. Il a sous sa coupole l'Agence nationale de la sécurité des systèmes d'information.

b- **L'Agence Nationale de la Sécurité des Systèmes d'Information**

L'agence nationale de la sécurité des systèmes d'information (ANSSI) est rattachée au SGSDN. Elle a été mise en place à la suite de l'élaboration du livre blanc de 2008[724] sur la sécurité informatique. Ce livre écrit grâce à la collaboration des opérateurs et des structures en charge de la défense nationale a considéré les attaques informatiques comme une menace pour la sécurité nationale. L'ANSSI est créée grâce au decret n° 2009-834 du 7 juillet 2009[725] portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

La compétence de l'ANSSI est nationale et porte sur les attaques informatiques, qu'elle doit détecter au plus tôt et réagir rapidement. Elle est un conseil pour les administrations et les opérateurs privés. Elle est surtout chargée de la protection des services interministériels de l'Etat. L'ANSSI émet des alertes régulièrement et informe les différents acteurs de la sécurité nationale. Cette structure est technique et émet régulièrement des alertes non seulement pour les entreprises mais aussi pour les pouvoir publiques quant aux attaques informatiques. Dans ce cadre, elle a élaboré un référentiel permettant la sécurité des entités administratives et étatiques depuis 2009 et cette norme technique appelée Référentiel Général de Sécurité entre en vigueur le 1er juillet 2014. Elle vise à sécuriser les échanges électroniques entre organes administratifs surtout les données des citoyens confiées aux autorités administratives[726].

Elle est aidée par ailleurs dans cette tâche par le CERTA.

---

[724] Le livre blanc de 2008 est consultable sur http://www.livreblancdefenseetsecurite.gouv.fr/

[725] cf. Journal officiel de la République Française n°0156 du 8 juillet 2009.

[726] cf. http://www.ssi.gouv.fr/fr/menu/actualites/le-rgs-version-2-0-en-vigueur-au-1er-juillet-2014.html

.

c- Le Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA)

La création du centre d'expertise Gouvernemental de Réponse et de traitement des Attaques informatiques (CERTA) a été annoncée par le Ministre Lionel JOSPIN, le 19 janvier 1999 lors du Comité Interministériel pour la société de l'information[727].

Le Centre d'Expertise gouvernemental de Réponses et de Traitement des Attaques informatiques (CERTA) est une structure d'alerte et d'assistance sur Internet inaugurée en 2001 par l'Etat français en vue de lutter contre les intrusions informatiques. Il s'inscrit dans le réseau mondial Computer Emergency Response Team (CERT). Il est rattaché aux services de la défense et de la sécurité nationale et a pour objet d'assurer la détection des vulnérabilités et la résolution des incidents concernant la sécurité des systèmes informatiques[728.]

Son rôle est essentiel en matière de cybercriminalité dans la mesure où cet organisme traite des intrusions informatiques, l'une des pratiques cybercriminelles répandues. Il émet des alertes pour prévenir des dangers immédiats. En fait, le CERTA détecte les intrusions informatiques d'un point de vue général et émet des avis. Exemple d'avis du CERTA en date du 21 septembre 2012, sous le numéro CERTA-2012-ALE-006-003[729.]

Hormis les avis, les alertes, des bulletins d'actualités sont régulièrement édités par le Centre d'expertise de réponse de traitement des attaques informatiques. Ces documents permettent de voir le travail effectué et facilitent la coordination des services de l'Etat en charge de la lutte contre la cybercriminalité. Ce sont des moyens de communication. Ces documents sont de supports de travail qui font intervenir notamment l'Agence Nationale

---

[727] Cf. Revue Sécurité Informatique, CNRS, avril 2001, n°34, p1 et suivantes.

Le discours du ministre est repris pour la partie concernant le CERTA sur le site officiel du CERTA : http://www.certa.ssi.gouv.fr/certa/certa.html.

[728]Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, http://www.certa.ssi.gouv.fr

[729] La version papier est consultable dans les annexes liées à la thèse page et disponible sous le lien suivant http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-006.pdf

de la Sécurité des Systèmes d'Information. A côté du CERTA intervient un office tout aussi important.

d- L'Office Central de Lutte contre la Cybercriminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)

Créé depuis 2000 par le décret n°2000-405 du 15 mai 2000, l'OCLCTIC est régi par les dispositions du code pénal. Il s'agit des articles 226-16 à 226-24 les articles 323-1 à 323-7. Quant au code de procédure pénale, ce sont les articles D2 à D8-2 qui y sont relatifs.

Les codes de répression ne sont pas les seuls dans la mesure où d'autres textes comme le code de propriété intellectuelle, la loi du 9 juillet 1966[730] portant organisation de la police nationale, la loi du 6 janvier 1978 relative à l'informatique[731], aux fichiers et aux libertés, la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité[732].

e- La Direction Centrale du Renseignement Intérieur (DCRI)

La Direction Centrale Renseignement Intérieur a été créée en 2008 par le décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur[733] . Elle est issue du rapprochement de la direction centrale des généraux et de la direction de la surveillance du territoire[734]. La Direction Centrale du Renseignement a pour rôle de prévenir et de réprimer sur le territoire français les activités inspirées engagées ou soutenues par des puissances ou des organisations étrangères et de nature à menacer la sécurité du pays[735].

---

[730] Loi n°66-492, JORF du 10 juillet 1966 p. 5899

[731] Loi n° 78-17, J.O.R.F. du 7 janvier 1978 p. 227.

[732] Loi n° 95-73, J. O. R. F. n° 0020 du 24 janvier 1995, p. 1263.

[733] Décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur est paru au JORF n°0150 du 28 juin 2008, texte n° 4.

[734] http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcri

[735] Cf. article 1 du décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur.

A ce titre, elle est investie de la lutte contre la cybercriminalité puisque la société actuelle est dépendante du développement des techniques de l'information et de la communication. C'est surtout sa mission de renseignement qui oblige cette structure à être au cœur des activités liées à l'information et à la communication.

f- La Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI)

Elle a pour mission de riposter rapidement à toute nouvelle infraction mettant en jeu les nouvelles technologies par enquête, assistance ou formation.

En pratique, les organes en charge de la lutte contre la cybercriminalité distinguent les infractions spécifiques des classiques. C'est dans cette optique que s'inscrit la BEFTI qui estime d'une part que les actes relevant de la cyber délinquance sont les délits classiques commis par le biais des nouvelles technologies et d'autre part la criminalité informatique regroupe les infractions réellement spécifiques[736].

La France est investie dans la lutte contre la haute criminalité technologique et le Royaume Uni également. Comment s'articule l'activité dans cet Etat ?

B- L'exemple d'un Etat voisin : le Royaume Uni

Plusieurs structures existent dans le domaine de la lutte contre la cybercriminalité.

Il s'agit notamment du Crime Survey for England and Walls anciennement British Crime Survey, du National Hi Tech Crime Unit (NHTCU), de l'Unified Incident Reporting and Alert Scheme (UNIRAS) et de l'Audit Commission for Local Authorities and National Health Service in England and Wales (ACLANHS). Pour une clarté des institutions établies et dont l'activité est effective, il faut s'intéresser aux organismes qui, pour la répression de la cybercriminalité sont actifs. Il s'agit du Crime Survey for

[736] Cf. **CRESPIN Y**., Colloque AFDIT, Revue Lamy Droit de l'Immatériel, 2006.

England and Walls, de la National Crime Agency[737] d'une manière générale, la National Cyber Crime Unit (NCCU) et la Police Central e-Crime Unit (PCeU).

a- The Crime Survey for England and Walls

Cette enseigne est traduite comme étant une enquête de criminalité britannique et portait auparavant le nom de British Crime Survey. Elle a pour objectif principal de répertorier des cas de crimes décrits par les victimes elles-mêmes. C'est depuis le mois d'avril 2012 que l'appellation a changé et ce dans le but de respecter la couverture médiatique associée. Elle travaille en collaboration avec l'organisme général de la lutte contre le crime au Royaume Uni c'est-à-dire la National Hi-Tech Crime Unit.

Cette manière de procéder est pragmatique en ce qu'elle repose sur des faits concrets et non sur des hypothèses abstraites.

b- The National Hi Tech Crime Unit

Instaurée par le Ministre de l'intérieur Jack STRAW en 2001, avec pour mission de « chasser » les groupes de criminels organisés en bande et agissant dans le cyberespace[738], la National Hi Tech Unit mène des actions coordonnées avec le ministère de la justice britannique mais également avec d'autres Etats comme les Etats-Unis, l'Australie. Fort de cette coordination, des opérations en vue de l'arrestation de membres de groupes actifs ne respectant pas les lois protégeant les droits d'auteurs ou le Copyright Act sont effectuées. Dans ce cadre, il est possible de citer les partisans du groupe « DrinkOrDie », qui, après avoir usé de la procédure du plaider coupable, se sont engagés à coopérer avec le bureau du procureur en l'aidant par la dénonciation d'autres membres du même groupe en cas d'infractions contre le Copyright Act[739]. Cette opération est dénommée Opération Buccaneer, du nom d'un texte de loi contre DrinkOrDie[740], un

[737] Cf. National Crime Agency établie par The Crime and Courts Act 2013, part 1.

[738] Cf. http://www.esds.ac.uk/government/bcs/

[739] Cf. D. S. WALL, Crime and deviance in cyberspace, op; cit. p. 237.

[740] Cf. idem ; US department of Justice, "Federal Law Enforcement Targets International Internet Piracy Syndicates" (December 11, 2001): http://www.usdoj.gov/opa/pr/2001/December/01_crm_643.htm

immense groupe de pirate de bases de données en ligne. Grâce à cette pratique plusieurs réseaux de cybercriminels sont démantelés. Il semble que ce soit une piste à explorer. La difficulté c'est de ne pas pouvoir avec certitude mesurer les exigences des cybercriminels en matière de négociation. C'est un peu la limite de ce mécanisme de négociation en amont avec des délinquants. Ils deviennent par ce truchement, indispensables. Rien non plus ne garantit leur fiabilité en termes de confidentialité. Il n'est pas certain avec ce genre de pratique, bien qu'efficace dans certaines circonstances que les délinquants n'utilisent pas les informations dont ils ont eu connaissance, dans d'autres crimes ou délits dans d'autres domaines.

S'agissant de la cybercriminalité, la NCA collabore avec la NCCU dans l'optique de réponses plus spécifiques.

c- La National Cyber Crime Unit (NCCU)

Son rôle est essentiellement de déterminer, d'identifier et comprendre les facteurs qui participent à la croissance des activités cybercriminelles sur le territoire du Royaume Uni. Ses identifications et analyses permettent de cibler et définir le type de réponses pénales ou techniques à apporter en guise de solutions. La NCCU se composent de spécialistes issus des rangs de la Police centrale en charge de la criminalité informatique. Il s'agit de la Police Central e-Crime Unit. Celle-ci comporte des spécialistes dans les services de la Police de la Métropole (Metropolitan Police Service) et dans la division de la criminalité organisée propre à la cybercriminalité (Cyber division of the Serious Organised Crime Agency appelé SOCA).

Les subdivisions de cette structure sont révélatrices du rôle d'investigation important conféré à la police au Royaume-Uni. Ces larges pouvoirs d'investigation montrent une activité de terrain quotidienne et spécifique. C'est la constitution même de l'appareil judiciaire britannique qui déteint sur la mise en place des services répressifs de la cybercriminalité.

Il en ressort également qu'elle est rangée dans la criminalité organisée et traitée comme elle.

Si la pratique se mêle à la compréhension théorique de la cybercriminalité dans les rangs des agences de lutte contre la cybercriminalité au Royaume Uni, la stratégie est étudiée par des agences d'audit comme le « National Audit Office ».

En plus de ces études, les unités spécialisées de détectives privés, organisées en association pour lutter contre la criminalité commise sur les réseaux en ligne FALCON interviennent directement auprès des personnes privées et des hommes d'affaires.

D'autres organismes importants en matière de répression de la criminalité numérique sont le « Scotland Yard Computer Crime Unit » et le « Independent Authority Of Posts And Telecommunications in Netherlands » interviennent. Ces structures travaillent avec le SPAMHAUS qui est une organisation à but non lucratif ayant son siège à Genève en Suisse et installée également à Londres.

Il faut en parallèle citer d'autres organismes comme le « Unified Incident Reporting and Alert Scheme ou encore le Audit Commission for Local Authorities and National Health Service in England and Wales en charge de toutes les questions d'analyse des données de santé.

Les structures s'organisent dans chacun des Etats membres mais il existe également des organismes au plan européen en charge de la coercition de la cybercriminalité.

C- Les organismes au niveau européen

Plusieurs organismes européens sont en charge de l'application des normes européennes en vue de la lutte contre la cybercriminalité. L'ENISA, le contrôleur européen et surtout la coordination des Etats membres à travers la création d'un point de contact unique PHAROS contribuent activement à ce combat.

a- L'Agence Européenne de la Sécurité des réseaux et de l'Information (ou the European Network and Information Security Agency : ENISA)

Dans l'optique de favoriser la coopération policière et judiciaire, a été mise en place l'Agence européenne de la Sécurité des réseaux et de l'Information. Elle est entrée en

vigueur par l'adoption de la Régulation n° 460/2004 du Parlement Européen et de Conseil du 10 mars 2004[741]. L'actuel directeur est le professeur Udo Helmbrecht.

Les opérations de l'Agence ont commencé en Crète en septembre 2005 après une période d'essai à Bruxelles[742]. Ces opérations consistent essentiellement dans la protection des systèmes d'information. Et grâce la Communication de la Commission au Parlement européen relative à la protection des infrastructures d'informations critiques, de 2009[743], est exprimée la volonté de protéger les infrastructures numériques et de favoriser une réelle coordination entre les Etats. La simple protection des systèmes d'information se complexifie ou s'améliore avec la mise en place d'exercice pratique de détection, de compréhension et de préparation d'attaques cybercriminelles. La protection prend dès lors une forme préventive et active avec ces exercices adressés aux professionnels des différents Etats membres de l'Union Européenne ainsi que des institutions européennes.

Pour permettre aux participants de préparer les exercices de simulation de cybersécurité, l'ENISA publie en 2009 un guide appelé *Good Practice Guide on National Exercises, Enhancing the Resilience of Public Communications Networks*[744].

Dès 2010, et en appui avec les Etats membres de l'Union Européenne et le Centre de Recherches de l'Union Européenne (Joint Research Center : JCR), l'Agence européenne de la sécurité des réseaux et de l'information, organise le premier exercice paneuropéen

---

[741] La régulation n° 460/2004 est publiée au Journal officiel de l'Union européenne L 77/1, du 13 mars 2004.

[742] http://www.enisa.europa.eu/about-enisa

[743] Cf. « Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience », communication from the commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions on critical information infrastructure protection, Brussels 30.03.09, COM(2009) 149 final.

[744] Cf. Evangelos OUZOUNIS, Panagiotis TRIMINTZIOS, Panagiotis SARAGIOTIS, Good Practice Guide on National Exercises, Enhancing the Resilience of Public Communications Networks, ENISA,décembre 2009.

appelé CyberEurope 2010[745]. Elle en facilite la mise en place. Cet exercice biennal concerne tous les moyens de communication et des technologies dans leur globalité : le téléphone, les bases internet, les plateformes des services de banque et toutes les voies empruntées par les logiciels. L'exercice s'est répété en 2012 et 2014.

Ce CyberEurope consiste en des simulations d'attaques numériques et intéresse les professionnels de plusieurs Etats de l'Union Européenne et à chaque exercice, des objectifs précis sont prévus.

Pour l'édition de 2014, quatre-cents professionnels originaires de vingt-six (26) Etats membres de l'Union Européenne, trois (3) pays de l'AELE ainsi que des institutions de l'UE ont participé[746]. L'objectif de ces exercices est de permettre aux candidats de *tester leur capacité à gérer des cyberattaques.* L'exercice se déroule *en trois phases[747] au cours d'une année :*

- *La première phase est une phase technique de détection des incidents, d'enquêtes, de mesures d'atténuation et des échanges d'informations*. Elle intervient
- *La seconde phase est dite opérationnelle ou tactique : elle sert à émettre des alertes, évaluer les crises, d'analyser des conseils, des tactiques.*
- *La troisième phase est une phase stratégique, durant laquelle le processus de prise de décision, l'impact politique et les cas publics sont examinés.*

Depuis le 18 juin 2013, l'agence bénéficie d'une nouvelle règlementation[748] 526/2013 sur la sécurité des systèmes et travaille en collaboration avec les Computer Emergency

---

[745] Cf. Cyber Europe 2010, Evaluation Report, European Network and Information Security Agency, 2011 disponible en ligne: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010

[746] Cf. : http://www.europaforum.public.lu/fr/actualites/2014/10/comm-cybereurope/index.html

[747]Cf. Communiqué de presse du 28 avril 2014 de l'ENISA, disponible en ligne sous : https://www.enisa.europa.eu/media/press-releases/cyber-europe-2014-se-tient-aujourd-hui

[748] Cf. Règlement (UE) n o 526/2013 du parlement européen et du conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004, JOUE du 18 juin 2013, L 165/41.

Response Teams (CERTs), le centre de cybercriminalité européen et d'autres institutions de l'Union européenne.

A côté de l'ENISA, le contrôleur européen de la protection des données travaille dans le sens de la libre circulation de ces informations.

b- Le contrôleur européen de la protection des données personnelles

Le poste du contrôleur européen de la protection des données personnelles a été créé en 2001 par le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[749].

Dans la mesure où les institutions et les organes de l'Union Européenne sont amenés à traiter des données personnelles, il a fallu mettre un place un organe chargé de leur contrôle. C'est ce rôle que s'est vu assigné le contrôleur européen[750].

Il veille donc à ce que les institutions et les organismes communautaires respectent la vie privée de la personne identifiable dont ils ont à traiter les données personnelles. Il les conseille de ce point de vue. Tous les organes et les institutions sont concernés à savoir le Conseil de l'Europe, l'Union européenne, le comité économique et social européen, la cour des comptes européenne, la banque d'investissement européenne, le fonds européen d'investissement, le médiateur européen, le comité des régions. C'est dire que le contrôleur européen a un champ de compétence large et varié. Cette mission qui lui est confiée est étendue : il travaille en coordination avec les institutions et les organes de chaque Etat en charge de la gestion des traitements des données à caractère personnel.

Le traitement des données à caractère personnel est un aspect de la coercition de la cybercriminalité. Les Analyses de recoupement en sont un autre. D'où l'importance du point de contact unique créé au sein de l'espace de l'Union européenne.

---

[749] Le règlement (CE) n°45/2001 est publié au JOCE L 8/1du 12 janvier 2001

[750] http://europa.eu/about-eu/institutions-bodies/edps/index_fr.htm

L'Union européenne met en place une nouvelle force anti-cybercriminalité appelée la *Joint Cybercrime Action Task Force (*J-CAT) avec à sa tête Andrew ARCHIBALD. Les Etats membres de cette force sont la France, les Etats-Unis, la Grande-Bretagne, l'Autriche, la Hollande, l'Allemagne et l'Italie. Et la force est opérationnelle depuis septembre 2014 avec une période de tests de six mois pour lutter contre les *botnets*, les chevaux de troie et l'ensemble des activités menées dans l'internet noir c'est-à-dire en marge des usages traditionnels et conventionnels.

c- La Plateforme d'Harmonisation d'Analyse de Recoupement et d'Orientation des Signalements : point de contact unique

La Plateforme d'Harmonisation d'Analyse de Recoupement et d'Orientation des Signalements été pensée en 2007 par l'Union Européenne[751]. Cette plateforme a été mise en place sur le site www.internet-signalement.gouv.fr en vue de permettre aux particuliers de signaler des contenus illicites. Cette mesure est le prolongement de l'action de coopération judiciaire et pénale mise en œuvre au sein de l'Union Européenne entre les Etats.

La plateforme a certes une fonction de signalements mais elle exerce surtout auprès des particuliers un rôle de conseil et partant un rôle préventif. Du point de vue des utilisateurs, il n'est pas simple de se rendre compte de la portée immédiate des signalements de contenus illicites effectués. Par contre sur le plan judiciaire, cet outil est très efficace. Compte tenu des techniques dont les gendarmeries, les agents et les services de police judiciaire ainsi que les ministères ont été dotés ces dernières années, un travail de terrain considérable d'appréhension des individus s'adonnant à des pratiques malsaines via internet, est fait. Une fois les adresses IP des ordinateurs repérées, les propriétaires sont inévitablement arrêtés et sanctionnés par les autorités compétentes.

Qu'en est-il de l'office européen de police ?

---

[751]Cf. :http://europa.eu/legislation-summaries/justice-freedom-security/fight-against-organised-crime/14560-fr.html

d- L'office Européen de Police : EUROPOL [752]

Pour garantir la lutte contre la criminalité organisée tout en mettant fin aux contrôles transfrontières des personnes dans un espace de liberté, de sécurité et de justice, l'Union Européenne arrive à la création d'Europol[753]. Ainsi, EUROPOL est régi par la Convention Europol établie sur la base de l'article K. 3 du Traité de l'Union européenne portant création d'un Office européen de police en date du 26 juillet 1995.

Parce qu'EUROPOL constitue un prolongement de l'Unité de Drogue Europol, l'Office Européen de Police a un champ de compétence limité à l'origine. Il est compétent pour connaître de trafic illicite de stupéfiants, de traite des êtres humains, de filières d'immigration clandestine, de trafic de matières nucléaires et radioactives, de trafic de véhicules volés ainsi que de blanchiment d'argent lié à ces formes de criminalité[754]. L'office de police Européen est à l'origine de la création du centre européen de lutte contre la cybercriminalité, inauguré en 2013 et dont le siège est à La Haye.

1. Le centre européen de lutte contre la cybercriminalité

Le centre européen de lutte contre la cybercriminalité dans les locaux d'Europol (à La Haye) se place au cœur de la coopération dans la défense d'un internet à la fois libre ouvert et sûr[755]. Le texte récemment en débat a pour objectif est de mettre en confiance les consommateurs des services en ligne notamment[756]. A la lecture de cet objectif, des

---

[752] Loi n° 2005-496 du 19 mai 2005 autorisant l'approbation du protocole modifiant la convention portant création d'un Office européen de police (convention Europol) et le protocole sur les privilèges et immunités d'Europol, des membres de ses organes, de ses directeurs adjoints et de ses agents (1) publiée au JORF n°116 du 20 mai 2005 page 8730 texte n° 5.

[753] Cf. Actes du colloque sur la convention Europol : l'émergence d'une police européenne, p. 17.

[754] Convention Europol, article 2 §2, Convention sur la base de l'article K. 3 du Traité de l'Union européenne portant création d'un Office européen de police, JO n° C316 du 27/11/1995, p 0002- 0032. Voir également Mme **Constance CHEVALLIER-GOVERS**, De la coopération à l'intégration policière dans l'Union Européenne, thèse de droit public, Université de Panthéon-Assas, Paris II, sous la direction de Mario BETTATI, 20 mai 1998.

[755] Commission européenne - Communiqué de presse « Un Centre européen de lutte contre la cybercriminalité pour combattre la criminalité sur l'internet et protéger les consommateurs en ligne » Bruxelles, le 28 mars 2012.

[756]Cf. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=FR&guiLanguage=fr

interrogations quant à l'efficacité des dispositifs similaires à savoir la directive sur la règlementation du commerce en ligne, se posent.

Depuis le début de l'année 2013, c'est-à-dire depuis son inauguration le 11 janvier 2013, le centre est actif et a même signé un accord avec des collaborateurs américains afin de renforcer les échanges d'informations entre l'Union Européenne et les Etats-Unis[757].

Il ressort de cette coopération, que plusieurs types d'infractions entrent dans le champ de compétence du centre: il s'agit aussi bien des fraudes à la carte bancaire effectuées en ligne[758] que les contrefaçons de marque en ligne ou encore de l'usage frauduleux des noms de domaine.

Le rôle de ce centre est de lutter contre la cybercriminalité grâce notamment à des échanges d'informations. Concrètement, quelle est la procédure mise en place s'agissant de la répression ? Les démantèlements des réseaux de cybercriminels aboutissent-ils à des sanctions réelles ou sont-elles des débuts de correctifs aux actes cybercriminels ?

La portée des agissements du centre de lutte contre la cybercriminalité est cruciale d'un point de vue sanction. Quelle est-elle ?

Les actions du Centre européen de lutte contre la cybercriminalité se sont précisées surtout en 2013 et 2014.

En effet, le centre s'appuie sur une stratégie particulière en ce qu'il cible les actions menées par les cybercriminels grâce à plusieurs entités étatiques et internationales. C'est le cas de l'European Union Cybercrime Taskforce qui est à l'origine d'une opération test nommée *Joint Cybercrime Action Task Force*.

---

[757] Cf. http://europe-liberte-securite-justice.org/2013/01/15/lutte-contre-la-cybercriminalite-europol-signe-un-accord-avec-les-etats-unis/

[758] Cf. le rapport public d'EUROPOL sur la question des fraudes à la carte bancaire via internet et les réseaux numériques: https://www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf. Et pour d'autres actions de l'EC3 comme le *Police Ransome*, cf. http://europa.eu/rapid/press-release_IP-14-129_fr.htm.

Son rôle est de mener les enquêtes en matière de cybercriminalité et de faciliter une action coordonnée des services interétatiques. Le test a débuté le 1er septembre 2014 pour une durée de six mois[759].

Les tests opérés par cette nouvelle force européenne viennent s'ajouter aux résultats des actions menées par le centre européen de lutte contre la cybercriminalité. Plusieurs opérations du centre ont en effet permis de soutenir les enquêtes menées par les polices nationales notamment dans des cas d'infractions empruntant les logiciels malveillants pour attaquer des ordinateurs de civils, à pirater leurs données et à exiger des sommes en contrepartie du nettoyage des ordinateurs infectés. Ces premiers succès de démantèlement de réseaux de cybercriminels montrent que les Etats de l'Union européenne pourraient réussir pour une part importante l'éradication de la cybercriminalité.

L'action du centre européen de Lutte contre la cybercriminalité porte ses fruits dans la mesure où le 16 juillet 2014, un vaste réseau de cybercriminels roumains a été démantelé par le centre[760]. Ces stratégies coordonnées de joindre plusieurs organismes travaillant ensemble sur l'intégralité des infractions intervenant dans les réseaux de cybercriminels sont efficaces.

Pour l'année 2014, le centre a mené des opérations du type *Police Ransom, dans le cadre d'attaque informatique qui bloque l'ordinateur de la victime et l'accuse d'avoir accéder à des sites illégaux*[761].

Dans d'autres actions comme l'affaire du réseau zombie ZeroAccess, le centre travaille en collaboration avec des structures comme Microsoft et les unités de police criminelle allemande, néerlandaise, suisse, de Lettonie et du Luxembourg en charge de la lutte contre la cybercriminalité[762].

---

[759] Cf. Journal Les Echos du 28 juillet 2014: « Europol renforce son arsenal contre la cybercriminalité », à consulter en ligne sur : http://www.lesechos.fr/monde/europe/0203670979414-europol-renforce-son-arsenal-contre-la-cybercriminalite-1028392.php

[760] Cf. https://www.europol.europa.eu/content/international-network-romanian-cybercriminals-dismantled.

[761] Cf. communiqué de presse de la Commission européenne, Centre européen de lutte contre la cybercriminalité – un an après, 10 février 2014.

[762] Idem.

ZeroAcess, est un botnet qui dont l'activité principale était de détourner les annonces publicitaires en ligne pour s'enrichir. Ces détournements des clics de connexions prennent fin grâce à l'action coordonnée des compétences des acteurs suscités. Ce vaste réseau de cybercriminels est démantelé en décembre 2013[763].

C'est grâce à la procédure employée dans les domaines traditionnels d'enquêtes sur les crimes organisés (la drogue ou les trafics de médicaments contrefaits) [764] qu'Europol contribue régulièrement à l'arrestation des criminels en matière de cybercriminalité.

En parallèle de l'EUROPOL, il convient de mentionner l'Organisation Internationale de Police Criminelle. Elle a un objectif beaucoup plus large, c'est-à-dire un champ d'action international. D'ailleurs, elle est souvent sollicitée par les Etats africains notamment.

2. L'organisation internationale de police criminelle (OIPC)

L'organisation internationale de police criminelle est un réseau d'experts au sein d'INTERPOL et constitue une réponse aux exigences de coopération internationale suscitée par la nature transfrontalière de la criminalité contre la technologie.

Elle comprend pour ce faire une sous-direction spécialisée sur la cybercriminalité financière.

Elle dispose également d'un système de codification des infractions informatiques au sein de son secrétariat général.

En ce qui concerne la cybercriminalité, l'OIPC est régulièrement sollicitée par les Etats Africains pour la formation de ses spécialistes en vue de lutter contre la cybercriminalité.

---

[763] Cf. Cybercrime: Europol et Microsoft font plier l'énorme botnet ZeroAccess, voir http://lexpansion.lexpress.fr/high-tech/cybercrime-europol-et-microsoft-font-plier-l-enorme-botnet-zeroaccess_1425114.html#qJYsa8FywVYJvueY.99

[764] Cf. https://www.europol.europa.eu/sites/default/files/publications/fr_europolreviewfrench.pdf , à la page 59 et suivantes du document.

Le rapport de la vingt-deuxième (22ème) conférence régionale de l'Interpol en Afrique[765] a été l'occasion pour sa présidente Madame BALLESTRAZZI, de le souligner : l'Algérie est désormais dotée d'instruments pour lutter contre la cybercriminalité notamment la formation de spécialistes dans le domaine. Ces moyens sont mis à la disposition de tous les Etats africains qui en manifestent le besoin.

Sous un angle plus général, il faut considérer le rôle d'INTERPOL dans la lutte contre la cybercriminalité avec les interventions spécifiques en matière de propriété intellectuelle. En effet, divers actes concrets sont le fait de l'OIPC dans le domaine des contrefaçons, des piratages.

Il s'agit de son rôle de coordination : INTERPOL est un point de contact entre les Etats membres et les secteurs d'activités victimes des atteintes à la propriété intellectuelle. C'est dans cet objectif qu'il aide à démanteler les réseaux de criminels responsables de ce type d'atteintes[766].

L'OIPC dispose de services de formation en ligne interactifs comme l'International Intellectual Property Crime Investigators College, de séminaires de formations des spécialistes et de la Conférence internationale annuelle sur la répression des atteintes à la propriété intellectuelle, essentiellement basée sur des actions opérationnelles.

Toutes ces initiatives et actions font d'INTERPOL ou de l'OIPC une arme particulière contre la cybercriminalité. Elle attaque un point spécifique du fléau qui est l'ensemble des atteintes à la propriété intellectuelle et permet ainsi une meilleure diffusion de l'information et du renseignement.

Il ressort de cette section que la répression de la cybercriminalité est un exercice qui exige de la part de tous les organismes créés dans ce but, un travail collaboratif. Ces

---

[765] La 22 ème édition de la Conférence régionale d'Interpol en Afrique s'est tenue du 10 au 12 septembre 2013, à Oran en Algérie, Pour cela voir http://www.interpol.int/fr/News-and-media/Events/2013/22nd-African-Regional-Conference2/22nd-African-Regional-Conference,

opérations de recherches, de compréhension de cette criminalité particulière et technique nécessite une action sans cesse coordonnées et mûrement élaborée.

L'élaboration de la stratégie coercitive, se construit chaque fois un peu plus. Au fur et à mesure des attaques informatiques, numériques ou électroniques, les Etats de l'Union européenne à travers les structures étatiques et multinationales trouvent des stratagèmes pour sanctionner les cybercriminels et pour prévenir leurs exactions.

Les organes mis à contribution de la sanction contre la criminalité contre la haute technologie sont mis à rude épreuve aussi bien au niveau européen qu'au plan international.

Dans ce cadre, le continent africain n'a pas d'autres alternatives que d'intégrer les cases de cette lutte internationale. C'est pourquoi, des structures de lutte contre la cybercriminalité mais surtout de sanction y sont également instaurées.

Section 2 : L'instauration d'organismes de mise en œuvre en Afrique de l'Ouest

Au niveau de l'Afrique de l'Ouest, le foisonnement des organismes de lutte contre la cybercriminalité est récent.

Il faut d'ailleurs noter la collaboration renouvelée avec les structures européennes dans ce domaine et dans divers Etats notamment l'Espagne et même en dehors de l'Union Européenne.

Le caractère récent des législations laisse une impression d'impuissance de l'administration pénale d'une manière générale. En réalité, il n'en est rien. En l'absence de textes conçus à la perfection pour encadrer des situations conflictuelles nées des fraudes cybercriminelles, des organismes prennent le relai de cette lutte. Il faut croire que

---

[766] Cf. Fiche pratique d'INTERPOL n° COM/FS/2012-01-FHT-01 de février 2012 disponible en version pdf sur le site d'INTERPOL.

l'élaboration des textes réprimant la cybercriminalité se fait à la lumière des résultats observés par ces structures.

D'un point de vue constructif, la démarche n'est pas mauvaise : c'est grâce aux applications concrètes et des situations de fait que seront rédigés les textes de loi. De la sorte, ils ont la prétention de ne pas être abstraits puisqu'ils règlementeront des hypothèses déjà connues et expérimentées.

Dans cet esprit, il faut mentionner les organismes régionaux d'envergure économique qui luttent déjà contre les actes cybercriminels. Il s'agit de l'UEMOA et de la CEDEAO qui comportent des divisions en charge des sanctions contre les fraudes informatiques et leurs dérivés. Il ne s'agit pas de la cybercriminalité dans son acception large mais la prise en compte du phénomène par ces structures régionales est un bon début de sensibilisation des autres organismes étatiques à la question. Dès lors, comment envisager l'instauration d'entités de mise en œuvre de coercition et de sanction de la cybercriminalité en Afrique de l'Ouest ? (§1).

Sous l'influence des Etats du Conseil de l'Europe et avec la participation de l'Union européenne, l'Union Internationale des Télécommunications a institué un organisme appelé IMPACT pour la gestion des problèmes numériques au niveau du continent africain. Cet organe n'est-il pas une prémisse de la collaboration euro-africaine pour venir à bout de la cybercriminalité ? L'analyse des structures coercitives en Afrique de l'Ouest impose de faire la lumière sur cette interrogation importante (§2).

§1- Les structures coercitives de la cybercriminalité

Pour matérialiser les sanctions légales édictées, plusieurs structures sont mises en place afin d'assurer des missions d'appui à la loi et donner des conseils aux usagers de manière générale. Dans divers Etats notamment au Nigéria, Etat particulièrement prisé par les cybercriminels, il existe des commissions ou des structures en charge de cet appui. Depuis 2006, les réalités du terrain ont bien évolué dans la mesure où plusieurs colloques ont eu lieu et des solutions pratiques ont été mises en place.

Au titre de ces réunions de réflexion, la réunion régionale des procureurs au Nigéria a favorisé des échanges entre les différents procureurs quant à la mise en place

des procédures pénales. Ces interrogations concernent principalement l'adaptation des procédures afin de les rendre plus appropriées. Il s'agit de les rendre effectives dans la mesure où en dépit des lois prises pour appréhender les cybercriminels notamment l'article 419 du code pénal, les procédures restent jusque-là très peu spécifiques à un domaine aussi précis que les cybermenaces. Certains organismes ont une vocation régionale et ont des agences ou des représentations dans chaque Etat de l'Afrique de l'ouest. D'autres sont propres et particuliers d'un Etat à l'autre. C'est dire qu'il y a des structures nationales (A) et d'autres régionales (B).

A- Les structures nationales

Plusieurs organismes nationaux en Afrique de l'Ouest ont en charge la lutte contre la cybercriminalité. C'est le cas de l'Autorité de Régulation des Télécommunications en Côte-d'Ivoire. Elle exerce ses missions en collaboration avec plusieurs autres entités (a).

Parmi ces dernières, la plateforme de lutte contre la cybercriminalité, est nationale mais a vocation dans un avenir proche à devenir régionale (b).

Outre ces organismes, il existe d'autres structures plus techniques comme le CERT qui ont des représentations nationales dans certains Etats de l'Afrique de l'ouest (c).

a- L'Autorité de Régulation des Télécommunications en Côte-d'Ivoire

La lutte contre la cybercriminalité est accentuée avec d'importants changements comme l'attribution de pouvoirs quasi-juridictionnels à l'Agence des Télécommunications de Côte- d'Ivoire (ATCI). Elle est devenue depuis l'ordonnance n° 2012-293 du 21 mars 2012 sur les Télécommunications et les Technologies de l'Information et de la Communication[767], l'Autorité de Régulation des Télécommunications de Côte d'Ivoire.

L'ARTCI est une autorité administrative indépendante dotée de la personnalité juridique et d'une autonomie financière.

---

[767] cf. Ordonnance n° 2012-293 du 21 mars 2012 publiée au Journal Officiel de la République de Côte-d'Ivoire du 14 août 2012, n°8, 54ème année.

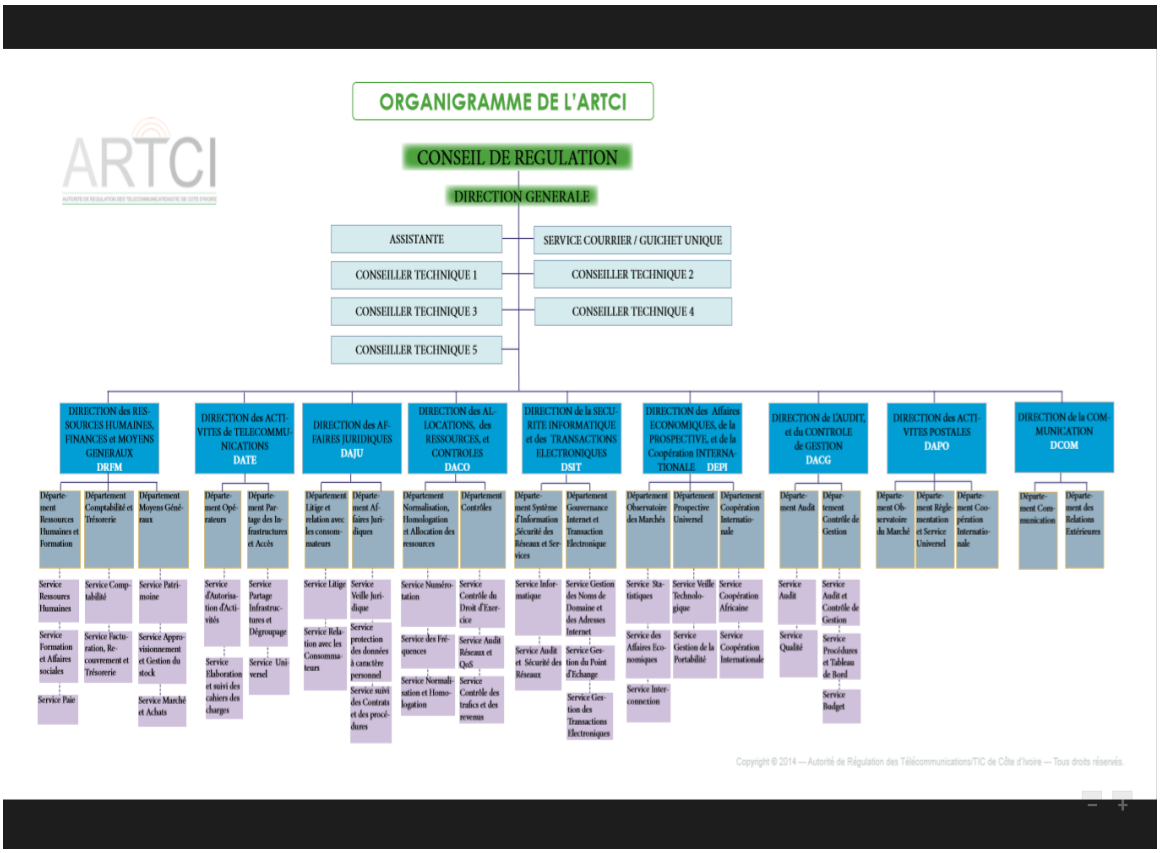
En réalité, ce sont les membres du Conseil de Régulation qui ont des pouvoirs quasi-juridictionnels. Comment est hiérarchisée l'ARTCI ? Avec quelles entités travaille-t-elle dans la lutte contre la cybercriminalité ?

1. L'organisation de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire.

Créée par le décret n° 2012-293 du 21 mars 2012, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) est née de la fusion du Conseil des Télécommunications de Côte d'Ivoire (CTCI) et de l'Agence des Télécommunications de Côte d'Ivoire (ATCI). Elle a une structure pyramidale avec en tête le Conseil de régulation.

Le Conseil de Régulation est un collège de sept (7) membres dont le Président. Il a en charge les missions de gestion juridiques, techniques, administratives et financières de l'ARTCI. Ce conseil de régulation a sous sa responsabilité la Direction générale qui elle-même coiffe plusieurs autres directions.

Il s'agit de la Direction des Affaires Juridiques et litiges (DAJU), la Direction Activités Télécommunications (DATE), la Direction des Affaires ressources et Contrôles (DACO), la Direction Ressources humaines, Finances Moyens généraux (DRFM), la Direction Economique, Prospective et Coopération internationale (DEPI), Direction Audit, Contrôle de Gestion (DACG) et la Direction Sécurité Informatique et Transactions Electroniques (DSIT).



Organigramme de l'ARTCI disponible sur :
http://www.artci.ci/index.php/organigramme/Organigramme/organigramme.html

2. Les collaborations de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire.

Dans le cadre de ses collaborations, l'ARTCI développe des partenariats avec l'ensemble des structures en charge du problème de la cybercriminalité. Dès le 24 janvier 2012, la présentation de la Plateforme de Lutte Contre la Cybercriminalité[768] met un point d'honneur sur la collaboration de l'Agence de Régulation des Télécommunications avec les services de police et de gendarmerie. Cette nouvelle structure donne surtout une leçon quant à l'état d'avancement de la lutte contre la cybercriminalité. Pour renforcer ses à initiatives, l'ARTCI échange avec la Direction Informatique des Traces Technologiques (DITT), service de la police nationale qui travaille sur les problématiques numériques.

[768] Le site officiel de la plateforme est http://www.cybercrime.interieur.gouv.ci/

A l'instar de la CNIL, il existe en Afrique des structures comme le CENTIF, qui a en charge le traitement d'informations financières (CENTIF) et le CI-CERT qui traite les incidents informatiques (CI-CERT).

A ces entités s'ajoutent la Plateforme de Lutte Contre la Cybercriminalité (PLCC), qui travaille régulièrement avec l'ARTCI et son équivalente au Sénégal : la Brigade Spéciale de lutte contre la Cybercriminalité.

b- Deux structures spéciales en charge de la lutte contre la cybercriminalité

Ces deux structures sont équivalentes de par leurs missions. Elles interviennent en Côte-d'Ivoire : la plateforme de Lutte contre la Cybercriminalité et au Sénégal : la Brigade Spéciale de Lutte contre la cybercriminalité.

1. La Plateforme de Lutte Contre la Cybercriminalité (PLCC)

En Côte-d'Ivoire, le ministère de l'intérieur et l'Agence de Télécommunications ont collaboré pour créer un espace permanent destiné à répondre rapidement à la lutte contre la cybercriminalité. Cet espace prend la forme d'une plateforme appelée plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire.

La plateforme ainsi créée est régie par le décret 2011-476 du 21 décembre 2011 permettant à la Police Scientifique d'opérer avec beaucoup de célérité dans la lutte contre les cybercriminels. Les missions de la plateforme consistent essentiellement dans la conduite d'enquêtes judiciaires portant sur les infractions visant ou utilisant des systèmes informatiques. Elle a aussi en charge la régulation et le suivi des modes de traitement, de stockage et de transmission de l'information par les canaux numériques.

Il s'agit également pour elle d'apporter une assistance technique aux services de Police et aux services connexes chargés de l'application de la loi lors des enquêtes judiciaires.

En outre, la plateforme devra contribuer à la mise en place de moyens techniques et au développement de l'expertise pour l'examen et le traçage des systèmes d'information, et notamment l'audit et l'autopsie des disques durs d'ordinateurs, des téléphones et des autres médias.

Par ailleurs, la plateforme mène également des actions de sensibilisation et d'information sur la cybercriminalité auprès des populations et des autres services de

l'administration publique et du secteur privé. Elle devra enfin, participer à la définition et à la mise en œuvre de mesures techniques, organisationnelles et règlementaires dans le cadre de la lutte contre la cybercriminalité.

D'un point de vue pratique, la plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire est un véritable outil de démantèlement des réseaux de cybercriminels. Les activités des membres actifs sont révélatrices dans la mesure où plusieurs personnes s'adonnant à ces pratiques illicites sont mises aux arrêts et jugés pour les faits qu'elles ont commis. Il est possible d'en trouver trace sur le site officiel de l'entité : régulièrement les personnes accusées d'actes de détournements de fonds via les réseaux numériques, de vols d'identité ou encore de vols de cartes bancaires et surtout de craquage de codes d'accès voient leur identité révélée sur les pages publiques de ce site officiel.

Il est certain que sous certains aspects, de telles révélations paraissent dissuasives et ont une visée à la fois de sensibilisation mais également de dissuasion. L'objectif de sensibilisation concerne les victimes de tels actes, en les incitant à porter plainte et surtout à faire confiance aux autorités en charge de lutter contre les infractions cybercriminelles. L'optique de dissuasion est en direction des autres cybercriminels ou autres membres des réseaux dont les activités ne seraient pas encore découvertes par les autorités de police en charge de la lutte contre la cybercriminalité.

La plateforme de lutte contre la cybercriminalité fait partie intégrante du Tribunal de première instance d'Abidjan. Dès qu'elle reçoit des plaintes, la PLCC engage les poursuites, procède à l'enquête pour appréhender les cybercriminels et une fois, les individus appréhendés, elle les déferre au Parquet.

A cet effet, le Substitut du Procureur, Monsieur KONE Souleymane (en 2014) en charge de la cybercriminalité est un magistrat du Parquet détaché au Tribunal de Première d'Abidjan. Il a été nommé par le décret n ° 2011-299 du 17 octobre 2011 portant nomination de magistrats aux sièges des tribunaux de Première instance, de leurs sections

détachées et aux parquets près lesdits tribunaux et sections détachées[769]. Il est en charge des poursuites de l'enquête et travaille en lien direct avec la PLCC.

Les difficultés rencontrées par la plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire sont d'ordre pratique. En effet, la remise en cause des données divulguées sur le site officiel de la plateforme mérite d'être soulignée : les personnes interpellées par les agents de la plateforme ne sont pas encore déclarées coupables par les autorités judiciaires et cependant, leur identité, profession, et même photos sont publiées. Il est vrai que cette pratique a un caractère dissuasif mais elle soulève la question de la présomption d'innocence d'une part et celle de la protection des données d'autre part[770].

La plateforme gagnerait plutôt à publier des décisions de justice rendues dans le cadre de procédure déjà achevées. Cette publication des décisions sur la plateforme témoignera non seulement de l'efficacité des interpellations des policiers et des gendarmes mais en plus, elle sera la preuve que l'institution mise en place fonctionne effectivement. Dans une société au sein de laquelle les résultats sont attendus de la part des contribuables civils notamment, cette procédure de publication des décisions rendues par la justice à la suite de personnes interpellées est nécessaire.

Si la plateforme de lutte contre la cybercriminalité est un exemple de structure coercitive contre la cybercriminalité, elle doit être étendue à d'autres Etats de la sous-région dans la mesure où la cybercriminalité mine toute la région. A ce jour, il n'existe pas encore de structure de ce type dans tous les autres Etats. Il pourrait être envisageable soit d'étendre le champ de compétence de la PLCC soit d'en créer dans les autres pays de l'Afrique de l'ouest. Cette proposition vise à assurer une coercition non limitée à un seul Etat mais étendue à plusieurs Etats de la même région. D'ailleurs, la région gagnerait en termes de lutte coordonnée. Dans ce cadre, il pourrait être intéressant d'instaurer des

[769] Cf. Décret n°2011-299 du 17 octobre 2011 portant nomination de magistrats aux sièges des tribunaux de Première instance, de leurs sections détachées et aux parquets près lesdits tribunaux et sections détachées, publié au Journal Officiel n° 51 du jeudi 22 décembre 2011.

[770] La critique est vive sur la question de protection des données de la part des populations ivoiriennes : cf. commentaires sur la plateforme de lutte contre la cybercriminalité et journal Abidjan.net

échanges de bons procédés permettant à la PLCC ivoirienne d'être un centre de pilotage pour les nouvelles entités à mettre en place dans les autre pays.

La question de l'extension de la PLCC ou de son instauration en dehors des frontières ivoiriennes mérite une attention particulière. Elle a une équivalente au Sénégal. Il s'agit de la Brigade Spéciale de lutte contre la Cybercriminalité.

2. La Brigade Spéciale de Lutte contre la Cybercriminalité

La Brigade Spéciale de Lutte contre la Cybercriminalité du Sénégal est l'équivalente de la plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire. Cette unité spécialisée fait partie de la direction de la police judiciaire du Sénégal.

La Brigade Spéciale de lutte contre la cybercriminalité a démantelé un réseau de cybercriminels sur les appels internationaux[771]. En effet, ces individus utilisaient les canaux de réseaux téléphoniques et des logiciels installés sur un téléphone pour passer des appels internationaux à des prix locaux. Les personnes interpellées ont été déférées à la police nationale[772].

En plus des organismes établis au niveau de la police et en charge des enquêtes, d'autres entités aussi spécialisées dans le traitement de l'informatique doivent être implantées dans le cadre de la recherche de sanctions contre le fléau cybercriminel. Dans cet objectif, le déploiement de structures d'étendue régionale est une garantie d'une lutte efficace contre la criminalité transfrontalière.

C'est d'ailleurs le moyen utilisé pour la mise en place des CERT dans les Etats. Cette manière de procéder fait du CERT une structure à la fois nationale (parce que présente dans chaque Etat, pour l'instant pas tous les pays de l'Afrique de l'ouest) et régionale (puisqu'il existe un AFRICA CERT qui coiffe tous les CERT présents en Afrique).

---

[771] Cf. Communiqué de Presse de Osiris du 1er novembre 2014 : La Brigade Nationale de Lutte contre la Cybercriminalité de la Police Nationale démantèle le réseau des fraudeurs sur les appels internationaux, disponible en ligne : http://www.osiris.sn/Communique-de-presse-La-Brigade.html.

[772] Cf. Bureau des Relations Publiques de la Police Nationale, 31 octobre 2014.

c- Les représentations nationales du CERT

Le Centre de Traitement des Incidents informatiques (CERT) se décline en plusieurs appellations comme par exemple le Computer Security Information Response Team (CSIRT) comme c'est le cas au Bénin ou encore de NITA-CERT pour le Ghana) et enfin le CI-CERT pour la représentation en Côte-d'Ivoire.

1. Le Centre de Traitement des incidents informatiques en Côte-d'Ivoire (CI-CERT)

Le Centre de Traitement des incidents informatiques en Côte-d'Ivoire a été mis en place en ce qui concerne la Côte-d'Ivoire par l'ARTCI, en 2010. Il a en charge les veilles technologiques. Il reçoit également des plaintes de la part aussi bien des entreprises que des particuliers. Le CI-CERT est une structure chargée de lutter contre les failles informatiques à savoir les intrusions frauduleuses, les falsifications et autres menaces informatiques dirigées contre les entreprises et les particuliers.

Le CI-CERT[773] est engagé dans la lutte contre la cybercriminalité. Il prend une part active dans le projet de sensibilisation de lutte contre la cybercriminalité dénommé SECURITIC de concert avec certains acteurs impliqués dans cette problématique, à savoir : Google, la Plateforme de Lutte Contre la Cybercriminalité et l'Association des Usagers d'Internet en Côte-d'Ivoire (AUI-CI).

L'année 2013 est marquée par de multiples actions de sensibilisation, à travers les interventions dans les médias traditionnels et nouveaux[774].

Le bémol à relever est l'insuffisance de collaboration et de coordination sur un plan régional bien qu'il existe le souci de remédier à cette carence. En effet, les dispositions relatives à la mise en place de CERTs se mettent progressivement en place au niveau sous régional. Par exemple le Burkina Faso qui s'est doté d'un Centre National de cyber

[773] La précieuse contribution des membres de cette structure notamment Mlle KOUADIO Cynthia en charge de la communication au sein du CI-CERT a favorisé la communication des informations techniques et précises.

[774] Les interventions du CI-CERT dans les médias traditionnels c'est-à-dire la télévision, dans les forums notamment le forum régional sur les TIC mais également dans les médias nouveaux comme internet.

sécurité dénommé Centre de traitement des Infractions du Réseau et des Télécommunications (CIRT)[775].

Le CI-CERT entretient d'étroits liens de travail avec les CERTs (CERT Espagnol dénommé Instituto Nacional de Tecnologias de la Comunicacion en abrégé INTECO[776].

D'autres entités travaillent avec le CERT ivoirien. Il s'agit du CERT Américain dénommé US-CERT, le CERT de la banque Société générale et des organismes de lutte contre la cybercriminalité Africains existants comme IMPACT (Partenariat Multilatéral International contre les Cyber-menaces). L'IMPACT est lié à l'Union Internationale des Télécommunications (UIT).

L'efficacité des moyens mis en place pour combattre la cybercriminalité se mesure avec le recul des attaques informatiques. Un état des lieux de la question favorise la comparaison et permet de voir comment les Etats ouest-africains avec l'exemple de la Côte-d'Ivoire à travers le Ci-CERT travaillent à l'éradication de la cybercriminalité.

La part contributive des systèmes d'information géographique est importante bien que la géolocalisation des zones affectées ne soit pas facile[777] en matière d'Internet. Les adresses IP changent régulièrement d'une connexion à une autre. Mais le travail du CI-CERT cumulé avec les plaintes déposées dans ce domaine est un début qu'il convient de saluer. On assiste avec la surveillance des sites à un recul des attaques au fur et à mesure de l'augmentation des plaintes déposées et des incidents signalés. Cela montre l'utilité de structures comme le CI-CERT.

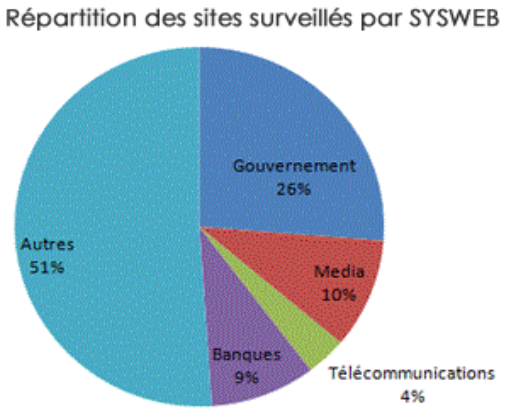
Les illustrations des tableaux et diagrammes permettent d'avoir une visibilité sur ces questions.

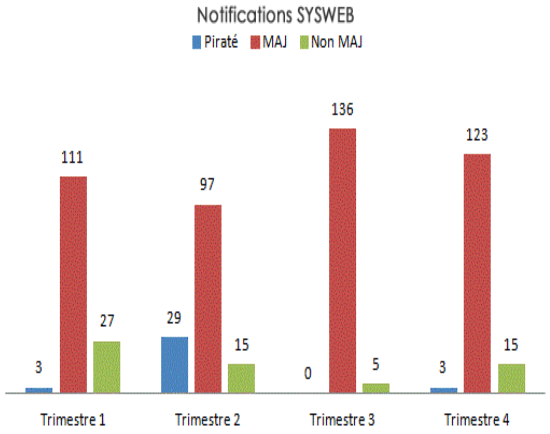
---

[775] Le CIRT du Burkina Faso correspond au centre de traitement des infractions du réseau et des télécommunications au Burkina Faso.

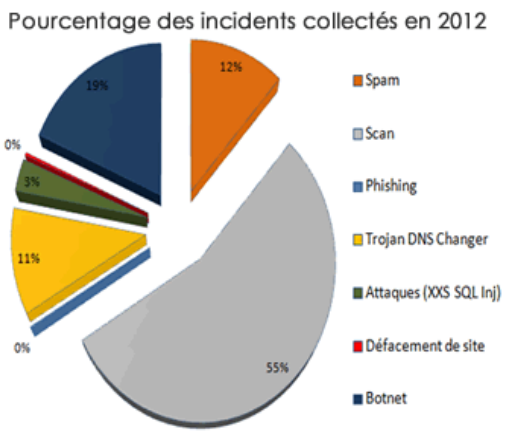
[776] INTECO- CERT dont le site officiel est http://cert.inteco.es

[777] La géolocalisation n'est pas évidente dans ces zones parce que les pistes satellitaires et les données liées ne sont pas totalement exploitées et développées pour en faciliter l'accès et l'usage.



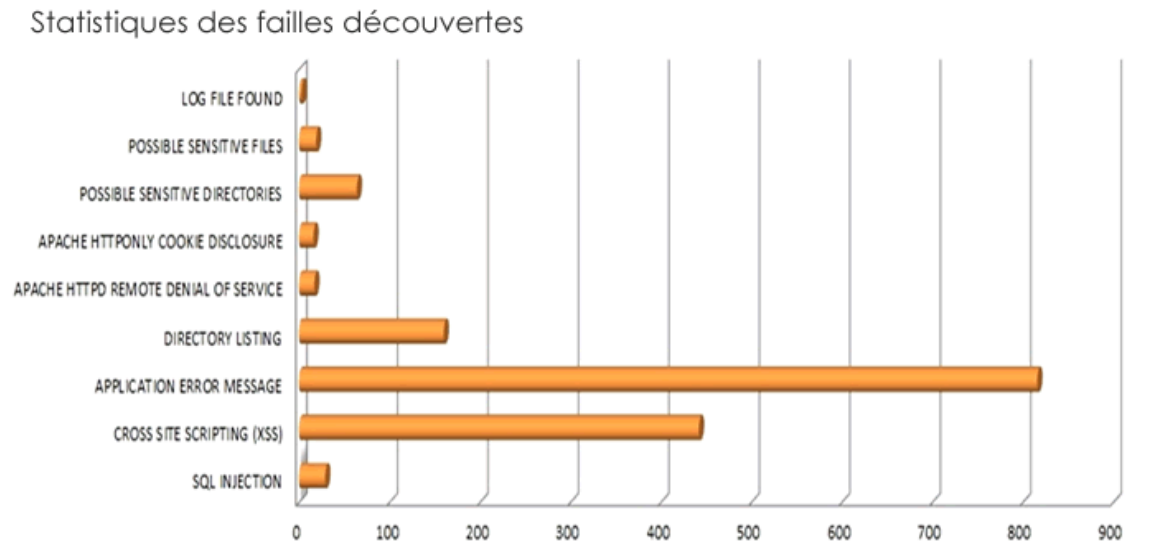


■ Incidents collectés en 2012



■ Failles web découvertes en 2012

Statistiques réalisées par le ci-cert en 2012, cf. Rapport d'activité 2012 de la structure.



	SQL INJECTION	CROSS SITE SCRIPTING (XSS)	APPLICATION ERROR MESSAGE	DIRECTORY LISTING	APACHE HTTPD REMOTE DENIAL OF SERVICE	APACHE HTTPONLY COOKIE DISCLOSURE	POSSIBLE SENSITIVE DIRECTORIES	POSSIBLE SENSITIVE FILES	LOG FILE FOUND
Series1	29	442	816	160	17	16	64	19	3

Diverses infractions interviennent sur le terrain ivoirien de la lutte contre la cybercriminalité. Il s'agit d'intrusion dans des systèmes informatiques par l'intermédiaire de virus par exemple SQL[778] injection ou encore de Cross site Scripting, l'une des infractions les plus en vogue (442 pour l'année en 2012) ou encore d'*application error message* (816). Les termes techniques employés soulignent le travail de déchiffrement opéré par les informaticiens du Ci-Cert notamment pour identifier le type d'acte concerné.

[778] SQL est un langage informatique, un ensemble de procédés, de requêtes pour communiquer avec des bases de données. C'est un mécanisme qui permet d'effectuer des extractions de données à partir d'une base de données.

S'agissant des chiffres, le tableau ci-dessous permet de comparer les plaintes, les interpellations, les dénonciations et retrace les actes concerts menés par le CI-CERT dans le cadre de ses actions de terrain.

Lutte contre la cybercriminalité par les actions du CI-CERT en 2012 et 2013[779]			
Années	**Plaintes et dénonciations**	**Préjudice financier**	**Répression**
2012	1846 e-mails reçus et traités	3.384.972.093 FCFA	71 interpellations
	692 plaintes enregistrées		51 condamnations
2013	9497 signalements dont 9179 e-mails et 318 appels téléphoniques	3.601.993.735 F CFA	66 interpellations
	552 plaintes enregistrées		

A la lecture de ce tableau, il apparaît que les chiffres correspondants aux signalements ont été multipliés par 5. En effet, il passe de 1846 à 9497. Deux raisons pourraient justifier cette explosion :

- la première raison est la mise en place de la Plateforme de lutte contre la Cybercriminalité. Cette structure travaille en collaboration avec le Ci-CERT qui effectue régulièrement des audits de sécurité. L'activité de la PLCC est aussi un moyen efficace de sensibilisation des populations.
- La seconde raison est la sensibilisation grâce aux arrestations dissuasives des cybercriminels par les agents de police en charge de lutte contre la

[779] L'ensemble des chiffres contenus dans le tableau provient des rapports annuels d'activité du Ci-CERT des deux années 2012 et 2013.

cybercriminalité. La prise de conscience par les internautes ivoiriens des risques liés à l'usage de l'internet et des réseaux numériques pousse les victimes à déclarer les attaques dont elles sont les cibles notamment par le biais des sites comme celui de la plateforme de lutte contre la cybercriminalité.

S'agissant des plaintes enregistrées, elles sont en baisse.

Quelles sont les infractions les plus marquantes du point de vue de la cybercriminalité ? Plusieurs infractions ressortent de l'audit des agents du CI-CERT. Le tableau ci-dessous permet de s'en rendre compte. Les valeurs sont exprimées en pourcentage :

Années	Spam	Phishing	Malware ZEUS	Attaques (XSS, SQL injection	Défacement de site web	Botnet
2012	83	76	242	108	38	309
2013	10	7	28	13	4	38

A la lecture de ce tableau, les actes de spam sont en régression entre 2012 et 2013. Il en va de même des autres infractions et on observe des progrès qui se chiffrent à pratiquement 90% de succès.

Par ailleurs et d'un point de vue répressif, la police numérique qui travaille en étroite collaboration avec les services de la Direction Générale des Renseignements et de la primature s'implante et a de plus en plus de poigne dans la lutte contre la cybercriminalité.

Dans d'autres pays comme le Ghana, l'entité est en phase d'installation.

2. Le NITA CERT au Ghana

Dans d'autres Etats comme par exemple au Ghana, le NITA CERT a été mis en place pour assister la coordination et le management de prévention, de détection et de

résolution des incidents de sécurité dans les ministères, départements et agences et autres institutions gouvernementales. Il s'agit de gérer tout incident auquel ils seraient confrontés dans le domaine de la sécurité informatique et des réseaux afférents. Il est opérationnel depuis juin 2012 et possède un site officiel est http://www.nitacert.gov.gh/.

Dans son discours du 03 octobre 2011, le ministre de la Communication ghanéen a présenté les différents travaux mis en place pour moderniser les infrastructures communicationnelles dans tous les secteurs d'activités y compris la justice, le gouvernement, les institutions et ainsi que le secteur de la sécurité informatique des institutions étatiques[780]. Les premiers pas de l'organisation sont soutenus par des initiatives entrepreneuriales et privées.

Si la répression de la cybercriminalité passe par des mesures techniques de surveillance, de contrôle et d'audit instaurées par les CERT au plan national, il reste à superviser ces activités au plan régional pour une meilleure coordination, vu l'aspect transfrontalier des actes de cybercriminalité. De ce fait, qu'en est-il des structures régionales ?

B- Les Structures régionales

Les structures régionales ont la particularité d'être représentées dans des Etats différents de l'Afrique de l'Ouest. Il s'agit notamment du CERT avec l'AFRICA CERT qui existe depuis juin 2010. Il est composé de plusieurs Etats non seulement ouest-africains mais d'autres régions de l'Afrique (a).

Outre les infractions informatiques (vol de données personnelles ou intrusions frauduleuses dans les systèmes informatiques par exemple), les atteintes financières qui empruntent les voies électroniques sont encadrées et gérées par la Cellule de Traitement des Informations Financières et d'autres structures comme la commission criminelle économique et financière du Nigéria « Economic and Financial Crimes Commission (EFCC) (b).

---

[780] Cf. http://www.nca.org.gh/downloads/MEET-THE-PRESS%202011%20FINAL.pdf

a- La version régionale des CERT : AFRICA CERT

AFRICA CERT comprend en son sein les pays suivants : le Burkina Faso, le Cameroun, la Côte-d'Ivoire, l'Egypte, le Ghana, le Kenya le Maroc, la Mauritanie, l'Afrique du Sud, le Soudan et la Tunisie. AFRICA CERT est un forum de règlement des incidents informatiques et travaille en collaboration avec plusieurs structures comme les différents CERT des Etats membres, mais également avec ITU- IMPACT (la collaboration entre l'Union Internationale des Télécommunications et le Partenariat multilatéral international de lutte contre les cybermenaces, l'ICANN, AFRINIC, le CERT du Japon (JPCERT), l'Organisation Internationale de la Francophonie, l'Organisation de la Coopération Islamique - Computer Emergency Response Teams (OIC-CERT).

Il s'agit pour cette structure d'émettre au plan régional des alertes avertissant des différents incidents informatiques et des mises à jour. C'est notamment le cas des virus ou des vers qui infectent des versions passées de logiciels. Par exemple les attaques virales de logiciels via des procédés Structured Query Language (SLQ).

AFRICA CERT est un cadre idéal pour observer les avancées des organismes en charge de la lutte contre la cybercriminalité au niveau de l'Afrique d'une manière générale. Les partenariats en ce domaine sont également le lieu de préciser les actions précises de l'Union Internationale des Télécommunications qui travaille avec l'IMPACT.

Les activités ne se limitent pas au domaine technique. Les aspects financiers sont également à encadrer.

b- Les cellules en charge du traitement des Informations financières

1- La Cellule Nationale de Traitements des Informations Financières (CENTIF)

La Cellule Nationale de Traitement des Informations Financières est une structure régionale avec une représentation dans chacun des Etats de l'Union Ouest-africaine. Partant de cette composition les différentes agences ou représentations se réunissent régulièrement en vue d'échange et de comparaison des applications pratiques des textes édictés par la cellule sur le plan régional.

La CENTIF a récemment intégré l'EGMONT GROUP of Financial Unit. Cette intégration de la cellule ivoirienne de lutte contre les infractions financières est l'expression de la coopération internationale.

Le but de cet accord est d'abord d'intégrer le CI-CERT au réseau de l'EGMONT Group of Financial Unit qui lutte contre le blanchiment d'argent[781] au plan international.

Il s'agit ensuite de mettre en pratique des stratégies de lutte contre les crimes organisés et mettre fin aux transferts de fonds illégaux dans l'espace sous régional puis international.

A cette structure, s'ajoute dans le domaine financier (puisque c'est essentiellement le but des fraudes en Afrique de l'Ouest), la commission criminelle économique et financière.

2- La Commission Criminelle Economique et Financière

Elle est connue au Nigéria sous l'appellation originelle « Economic and Financial Crimes Commission (EFCC). Elle a été créée en 2002 grâce à l'EFCC Act et adopté le 4 juin 2004.

Au Nigéria, il n'y a pas un seul et unique texte contre la cybercriminalité.

Il en existe plusieurs et ils sont associés pour que la Commission des Crimes financiers (EFCC) puisse remplir comme il se doit ses fonctions d'enquêtes et de juridiction en charge de réprimer la cybercriminalité[782]. Il s'agit du Computer Security and Critical Information Infrastructure Protection Bill 2005, du Advance Fee Fraud and other Fraud Related Offences Act 2006.

---

[781] Cf. **BENISSAD**, Blanchiment de capitaux: aspects économiques et juridiques, Économica, Paris, 2014. Le Groupe Egmont est un forum d'échange opérationnel pour les cellules de renseignement financier.

[782]Cf. **Maitanmi Olusola** , Ogunlere Samson, Ayinde Semiu et Adekunle Yinka, Cyber Crimes and Cyber Laws in Nigeria in *The International Journal Of Engineering And Science* (IJES) Mai 2013, Volume 2, Issues 4, pages 19-25.

Les différentes missions d'investigation et de juridiction de la Commission font d'elle la cible des cybercriminels. La Cour Suprême a traité des cas spécifiques de phising et de vols d'identité. En voici trois exemples.

Le premier cas est celui de l'arrêt de la Cour Suprême du Nigéria en date du 19 décembre 2008 et dont les faits opposaient Monsieur Mike AMADI à la République fédérale du Nigéria[783]. L'arrêt a été rendu sur le fondement du Code criminel (les articles 467 et 468) et des dispositions de l'Advance Fee Fraud Related Offences Act.

Dans les faits, Monsieur Amadi avait dupliqué le site officiel de la Commission des crimes économiques et financiers, copie du site officiel qu'il a par la suite utilisé pour opérer des transactions d'affaires frauduleuses faisant ainsi plusieurs victimes. Amadi est arrêté à la suite de ces fraudes s'élevant à 125 millions de dollars, inculpé par la Cour et condamné à 16 ans de prison.

Le second cas est également un phishing. Il s'agit de l'affaire *Chima Larry Ikonji and Blessing Onochie*, un couple dont chacun est condamné à une peine de 45 ans de prison pour avoir volé d'identité du Responsable exécutif de la EFCC dans le but tromper Monsieur William ELLISON un américain afin de lui dérober la somme de 750, 000 dollars[784].

Le troisième cas enfin celui de l'affaire *Muitala Abbas Ubandawaki*[785]. Les fraudeurs ont eu une peine de prison de 10 ans.

Les identités volées dans les trois cas de figure sont audacieuses puisque ce sont des hauts responsables de structures en charge de la lutte contre les fraudes en ligne, qui sont les cibles et dont les identités sont usurpées. La manœuvre réussie parce que les personnes

---

[783] Cf. Mike Amadi v. Federal Republic of Nigeria Suit No: SC.331/2007 commenté dans un article de Yusuf Ibrahim Arowosaiye, the new phenomenon of phishing, credit card fraud, identity theft, internet piracy and nigeria criminal law, intervention au cours de la 3rd Conference on Law and Technology, Faculty of Law, University Kebangsaan Malaysia and Faculty of Law, University of Tasmania, Australia, les 11 et 12 novembre 2008.

[784] Idem.

[785] Cf. Alert of the Economic and Financial Crimes Commission, vol. 2, n° .1 January 8, 2007 at 1 and 5.

visées comme victimes par les fraudeurs sont des personnes étrangères (des américains peu informées ou pas intéressées directement par ces hautes personnalités nigérianes).

Plusieurs autres structures interviennent dans le domaine de la sanction de la cybercriminalité et travaillent avec la commission criminelle économique et financière. Ce sont:

- La police nigériane « Nigeria Police Force » (NPF),

- Le Conseil National de Sécurité « the National Security Adviser » (NSA),

- le département des services de d'état : « Department of State Services » (DSS),

- l'Agence nationale de l'Intelligence : National Intelligence Agency (NIA),

- la société nigériane d'informatique : Nigeria Computer Society (NCS),

- le Group Internet du Nigéria : Nigeria Internet Group (NIG),

- l'Association des Fournisseurs d'accès Internet : Internet Services Providers' Association of Nigeria (ISPAN);

- l'Agence Nationale du Développement de l'information et de la Technologie : National Information Technology Development Agency (NITDA).

Malgré la création de cette multitude d'organismes, aucune action concrète n'est menée[786]. C'est le problème des structures africaines. Et pourtant avec les objectifs de lutte clairement affichés, ces entités gagneraient à progresser et à faire cesser les différentes fraudes et autres corruptions organisées sur l'ensemble de l'espace africain et en dehors des frontières.

Cette inaction conduit à s'interroger sur la stimulation qui pourrait être mise en place avec l'aide des autres Etats notamment de l'Union européenne.

---

[786] Cf. Oluwaseun Ayantokun, *Info Systems*, Lagos, 8th Juin, 2006.

En effet, beaucoup de ressortissants européens sont victimes des fraudes liées à la cybercriminalité. D'ailleurs, les infractions ont généralement pour origine des arnaques des Etats ouest-africains en particuliers et étranger à l'Union européenne en général. Sur ce point, on pense aux attaques informatiques des sites institutionnels des ministères des finances, en provenance des pays de l'Est ou de la Russie.

A côté des structures en lien direct avec la cybercriminalité, d'autres organes de lutte dans différents domaines faisant intervenir la criminalité contre la haute technologie sont à signaler. Il s'agit de l'institution spécialisée de la CEDEAO, le Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent (GIABA) au niveau de l'Afrique de l'Ouest. Le GIABA est créé depuis 2000 par la Conférence des Chefs d'Etats de la CEDEAO[787].

Le GIABA a en charge la lutte contre la criminalité financière et se trouve de facto lié à la lutte contre la cybercriminalité ; les trafics de fonds illicites et autres actions illégales comme le blanchiment d'argent, se servant de la cybercriminalité comme vecteur pour amasser des capitaux par des moyens et des canaux peu recommandés.

C'est dans ce cadre que le GIABA travaille avec l'EFCC du Nigéria : ces deux structures ont signé le 06 mars 2013 un *Memorandum of Understanding*, un accord pour apporter son assistance technique à la commission afin de lutter contre le crime au Nigéria[788].

La collaboration créée avec des Etats européen pourrait être un stimulant à cette inaction (à certains niveaux) des structures africaines.

---

[787] Cf. Décision AlDEC.9;/12/99 portant création du Groupement Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest (GIABA) et la Décision AlDEC.6/1 2/00 adoptant les statuts du GIABA.

[788] Cf. http://www.modernghana.com/news/451588/1/giaba-nigerias-efcc-sign-grant-agreement-on-techni.html

§2- L'importance de la collaboration européenne dans la sanction africaine de la cybercriminalité

L'importance c'est-à-dire l'étendue de la collaboration des continents européen et africain se ressent dans la lutte contre la cybercriminalité. En matière de technologie, et surtout s'agissant de la vulgarisation de ses emplois, l'Europe est pionnière. De ce fait, elle précède l'Afrique et cette dernière est en phase de diffusion des avancées technologiques et à petite échelle du numérique. C'est pourquoi, des leçons doivent être tirées pour une meilleure utilisation et des adaptations adéquates. D'une manière globale, l'Afrique n'a pas hérité des technologies uniquement de l'Europe. D'autres parties du monde comme le continent américain et plus récemment le continent asiatique (avec la Chine et l'installation massive des indiens) contribuent à propager la technologie en Afrique.

La collaboration doit se faire de plus en plus pour éviter les écueils comme la propagation incontrôlée (dans la pratique) et l'usage intempestif des technologies de l'information et de la communication. Les usages de ces infrastructures ne sont pas tant un manque de législations ou d'encadrement de la part des autorités des Etats de l'Union européenne, mais bien des erreurs de gestion dans le sens donné aux encadrements. Dans certains cas, ces fautes sont dues à l'absence d'éducation personnalisée des populations aux méfaits et le manque d'explication claire (et en amont) des interdictions. Dans d'autres cas, c'est le laisser faire qui n'est pas la solution adéquate. Il faut trouver un juste milieu dans la mise en place et surtout dans la mise en œuvre des politiques de lutte contre la cybercriminalité. L'équilibre de l'encadrement législatif et jurisprudentiel en Afrique peut être une des premières leçons à tirer puisque les corpus sont encore à l'état de construction (A).

Dans la suite des leçons à tirer, il convient d'analyser l'entraide judiciaire et douanière entre ces deux espaces. Comment appréhender concrètement des individus établis sur le continent africain s'il existe des preuves contre ces individus quant à la commission d'actes cybercriminels ? C'est la question de l'entraide judiciaire qui se pose dans des infractions transfrontières comme la cybercriminalité (B).

A- Les supports de la collaboration Europe- Afrique

Par supports de la collaboration, on entend les bases nécessaires à la manifestation des actes coordonnés entre l'Union Européenne et l'Afrique de l'ouest en matière de répression de la cybercriminalité. Ces socles sont en réalité des adaptations textuelles nécessaires (a) d'une part et la formation des acteurs en charge de la coercition des actes cybercriminels sur le terrain d'autre part(b).

a- Les équilibrages textuels

Il est actuellement question du droit de propriété des données à caractère personnel des individus. C'est l'une des préoccupations cruciales au cœur des règlementations européennes et qui va dans un temps très court arriver en Afrique de l'ouest. C'est ce qu'il est convenu d'appeler les encadrements textuels. Il faudrait ajuster les textes en essayant de prendre le contre-pied des lettres mis en place. En effet, la mise en place des normes au niveau européen et africain et par extension au niveau mondial, ne suffisent pas.

Finalement, n'est- il pas plus intéressant de procéder autrement ?

Parler d'équilibrage des textes est un moyen d'élargir la coopération des Etats de l'Union Européenne avec les Pays d'Afrique de l'ouest. En effet, la collaboration doit être étendue au travail de fond effectué par le Conseil de l'Europe. Plusieurs exemples récents éclairent ce propos.

Des assistances techniques et juridiques sont proposées aux Etats de l'Afrique (en général, et de l'Afrique de l'Ouest en particulier) pour aligner leurs lois contre la cybercriminalité sur les dispositions de la Convention de Budapest, seul texte contraignant à l'heure actuelle en matière de lutte contre la cybercriminalité.

Des ajustements sont encore possibles dans des terrains « vierges » comme le continent africain qui est en phase d'élaboration de ses textes et normes. Il est vrai que les lois relatives aux données personnelles sont créées mais il existe la possibilité d'éduquer les populations dans le sens de les responsabiliser.

Il faut se rendre compte que les règles de responsabilité ont considérablement changé : la norme de départ est celle selon laquelle il appartient à l'Etat de garantir la protection des

données (avec la loi de 1978). Ensuite, l'idée de base se métamorphose pour estimer que l'individu a le droit à la protection des données en précisant que c'est à lui de s'en assurer. Cette modification a pour conséquence de le rendre complètement responsable. Sauf que cette adaptation n'est pas bonne, elle n'est pas claire ni suffisamment encadrée pour prendre le soin d'expliquer à l'individu qu'il devient responsable de la protection de ses données du fait de leur diffusion consciente ou non. En d'autres termes, il est responsable de la sauvegarde de ses données. Il n'a pas d'office l'assurance d'être protégé s'il les diffuse via des réseaux notamment. Ce manque étant dû au fait que l'Etat n'assure désormais la protection que dans les hypothèses où l'individu aura veillé à une publication tenant compte des règles prévues par les lois. Ce que ne maîtrise pas l'individu c'est l'usage ultérieur de ses données personnelles à des structures. En l'état actuel des sociétés européennes comme africaines, les individus dans leur globalité n'ont pas vraiment conscience des effets de la diffusion de leurs données sur les réseaux numériques. Que faire si le responsable n'est pas si conscient qu'il aurait dû l'être ? C'est toute la problématique de la protection des données à caractère personnel par rapport à la cybercriminalité.

Si l'encadrement est fondamental, la mise en œuvre pratique l'est également. La formation des agents de terrain à tous les niveaux aussi bien dans la police, la gendarmerie que dans les entreprises est tout aussi importante pour donner du sens à la lutte contre cybercriminalité.

b- La formation des acteurs publics

Une des sources de difficulté de la répression des fraudes via internet est l'incapacité technique et professionnelle des agents africains en charge de la sanction ou de l'application des textes répressifs. Il s'agit des agents de police notamment, qui n'ont pas suffisamment de formation ou de qualification ou encore de compétences matérielles techniques pour appréhender les cybercriminelles. Ce constat a été fait dans plusieurs Etats en 2009 notamment au Nigéria, Etat de l'Afrique de l'Ouest

considéré comme un paradis cybercriminel[789]. Outre cette incompétence technique des policiers, il arrive que, même pour les cas dans lesquels ils ont les qualifications requises, ces agents censés assurer la sécurité des citoyens à tous les niveaux, ne sont pas dotés, pour remplir leur mission, d'équipements adéquats.

Par applications concrètes des accords, il faut comprendre les pratiques mises en place effectivement pour traduire la coopération des Etats en matière de lutte contre la cybercriminalité. C'est le lieu de préciser l'organisation de séminaires de formation des entités africaines en charge de la lutte contre la cybercriminalité par des organismes européens. A ce titre, l'OCLTIC a mené une action lors du séminaire sur le thème de la lutte contre la cybercriminalité du 21 au 25 novembre 2011 à l'attention de huit pays : le Bénin, le Burkina-Faso, la Côte-d'Ivoire, le Ghana, le Mali, le Niger, le Sénégal et le Togo[790]. Elle s'est achevée avec la formation d'étudiants aux problématiques de la cybercriminalité notamment en ce qui concerne l'Afrique de l'Ouest.

Grâce à ces formations pratiques, les étudiants mesurent mieux l'impact et l'ampleur de la cybercriminalité. Ils ne sont pas les seuls acteurs intéressés puisque des agents de police judiciaire ont également été formés par les agents de l'OCLCTIC. Il serait intéressant de mener de telles actions au niveau des magistrats, qui eux, sont au fait de la cybercriminalité en termes de rendre la justice. Les textes de loi en cours d'élaboration notamment avec l'apport des différents accords régionaux sont des débuts louables quant à la législation.

Ensuite, il faut souligner la prise en compte des accords signés en partenariat avec les Etats outre atlantique. En vertu des accords existants entre certains Etats comme le Bénin et la France des plans de lutte sont organisés au moyen de la tenue de séminaire de formation. Il en a récemment été ainsi avec le séminaire régional qui a eu lieu à Cotonou les 21 au 25 novembre 2011[791]. Cette opération a été renouvelée, au Bénin par exemple

---

[789] Cf. **EHIMEN O, BOLA A.** *Cybercrime in Nigeria*, article paru dans le Business Intelligent Journal, Janvier 2010, vol 3 n°1.

[791] cf. **GBETO Emmanuel**, « Séminaire régional contre la cybercriminalité au Bénin: La France parfait la formation technique des forces de sécurité africaines », cf. Journal L'EVENEMENT PRECIS du 22

en 2012 avec l'appui de *Francopol*[792]. Cet exemple pratique de coopération est la preuve de l'impact de conventions existantes entre les deux Etats.

Au titre des actions concrètes menées dans le cadre de la formation des acteurs publics de la lutte contre la cybercriminalité, le Groupement Interbancaire Monétique de l'UEMOA a formé en 2014, quatre cents (400) gendarmes en vue de lutter efficacement contre les fraudes aux cartes bancaires sur le continent africain. Cette action consiste en une prévention de ces actes qui rentrent dans la catégorie des actes cybercriminels les plus répandus au niveau du continent africain[793].

Les Etats tentent actuellement de remédier à cette absence d'infrastructures dans les administrations de défense.

Au niveau de l'éducation, les Etats tentent de remédier au manque de formation des acteurs de la lutte contre la cybercriminalité. Dans certains des Etats comme la Côte-d'Ivoire, se créent des écoles de formation aux Technologies de la communication pour adapter ses élites de demain au contexte international. Ces étudiants formés dans cette école appelée Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC) pourront constituer des experts en ce domaine et aider les agents de défense notamment. Il s'agit d'une initiative naissante et plusieurs recommandations peuvent être formulées au regard de la composition des programmes. Par exemple, les cours de droit peuvent être suffisamment axés sur la protection des infrastructures de communication et inculquer ainsi des méthodes certes techniques mais également juridiques. Se fonder sur des cas de cybercriminalité comme exercices d'application pourrait être formateur et plus imagé.

---

novembre 2011 ; voir également, article d'**Arsène SODJINOU**, Séminaire régionale sur la lutte contre la cybercriminalité à Cotonou : vers des reformes en vue d'une sécurisation des Tic, cf. Journal La nouvelle tribune du 22 novembre 2011. Egalement pour un aperçu du séminaire voir http://www.ambassade-benin.fr/la-france-au-benin-pour-parler-de-cybercriminalite/

[792] Cf. http://www.francopol.org/archives/activites-anterieurs/2012/04-12-12/index.php

[793]Cf.:http://xibaaru.com/depeches/fraudes-sur-les-cartes-bancaires-400-policiers-et-gendarmes-formes-par-luemoa/

L'école ESATIC est une structure sous-régionale et fait intervenir de ce fait des Etats comme le Burkina Faso et le Bénin. Elle entretient même des partenariats avec les écoles de Bretagne en France. Ces échanges universitaires sont un gage de réussite et montre encore une fois que la mutualisation des efforts pour combattre la cybercriminalité à tous les plans est nécessaire.

B- La répression transfrontalière de la cybercriminalité

Par répression transfrontalière, il faut envisager les techniques d'abord régionales au sein de l'Afrique de l'ouest puis internationales entre la partie ouest-africaine de l'Afrique et l'Union Européenne quant à la répression de la cybercriminalité.

Sur quel fondement en pratique un cybercriminel nigérian dont les actes auront été dirigés en direction du Royaume- Uni par exemple pourrait-il être sanctionné ? Sous un autre angle, un proxénète installé en Pologne, ayant via les réseaux sociaux recruté des jeunes femmes au Sénégal, à destination de l'Angleterre, pour les obliger à se prostituer, dans ce pays peut-il être poursuivi ?

Ces hypothèses caricaturales (et qui pourtant existent) sont un support pour traiter des questions d'entraide judiciaire et de collaboration inter- régionale dans le cadre de la cybercriminalité.

a- Les entraides régionales en Afrique de l'Ouest

Au niveau de l'Afrique de l'Ouest, les différents dispositifs mis en place entre l'UEMOA et la CEDEAO ainsi que les actes uniformes de l'OHADA sont des supports facilitant le règlement des questions relatives à l'entraide. Il est vrai que la législation est jeune en matière de cybercriminalité mais elle existe.

Ainsi, les domaines peuvent être abordés sous divers angles : le blanchiment de capitaux, la coopération des autorités douanières, l'entraide judiciaire avec notamment la reconnaissance des décisions de justice.

Sur la question de la coopération judiciaire, l'article 33 de la Directive portant lutte contre la cybercriminalité dans l'espace de la CEDEAO dispose que « *lorsqu'ils sont saisis par un autre Etat membre, les Etats membres doivent coopérer à la recherche et à la*

constatation de toutes les infractions pénales prévues ou définies par la présente directive ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. »

Cette disposition traduit clairement l'exigence faite aux Etats membres de la CEDEAO de s'entraider en matière d'infractions cybercriminelles. D'ailleurs, cette exigence est étendue au plan international puisque l'alinéa 2 de la Directive précise que « *cette coopération est mise en œuvre dans le respect des instruments internationaux pertinents et des mécanismes sur la coopération internationale en matière pénale* ». De ce point de vue il convient de s'interroger sur l'existence de mandat ouest-africain d'une manière générale d'abord et ensuite de façon spéciale concernant la cybercriminalité.

Sur le plan général, il est possible de confirmer l'existence de mandat ouest africain ou d'accord sur ce point notamment s'agissant des douanes. Depuis la mise en place des accords de coopération entre Etats ouest-africains, accords ayant pour but de faciliter l'intégration régionale, l'objectif de mettre fin aux barrières politiques et économiques entre les Etats est pratiquement atteint. La liberté de circulation des personnes et des marchandises par rapport à ces accords est instaurée malgré les difficultés pratiques dans les faits. Théoriquement, la « liberté des personnes et des marchandises est assurée ». En matière de douane, les Etats membres de la zone CEDEAO sont parvenus à établir des tarifs extérieurs communs.

Le bémol reste la mise en place d'un système douanier automatisé dans cette zone ouest- africaine. En d'autres termes, les buts visés ne sont pas encore réellement atteints, d'un point de vue général. Il est donc difficile à ce stade de préciser et de garantir la fluidité des services de douanes s'agissant des actes cybercriminels.

De ce qui précède, il apparaît que les Etats ouest- africains ont plusieurs domaines qui se présentent à eux au plan de la mutualisation de leurs efforts en matière de lutte contre la cybercriminalité. Cette mise en commun des forces ne doit pas pour autant les conduire à écarter les possibilités d'échanges avec les Etats de l'Union européenne. C'est en cela que l'analyse des possibilités entre les deux espaces communautaires doit être analysée.

b- Les possibilités entre Union-Européenne Afrique de l'Ouest

Comment l'Union européenne et l'Afrique de l'Ouest peuvent s'entraider sur le plan de la sanction de la cybercriminalité. C'est la question de la coopération internationale de la lutte contre la cybercriminalité qui implique le traitement des extraditions possibles de criminels. Prenons l'exemple de l'extradition intervenue lors de l'arrestation du chef de file des agresseurs d'Ilan ALIMI. Il a fallu la coordination des services de police de Côte-d'Ivoire et de France pour arrêter l'individu pourtant basé en Côte-d'Ivoire. Il est certain que si les connexions internet dans le cybercafé n'avaient pas été retransmises, les agents de police n'auraient jamais pu arrêter le criminel.

Par ailleurs, sans accord d'extradition existant entre la France et la Côte-d'Ivoire, Issouf FOFANA, le criminel, n'aurait jamais pu être extradé de la Côte-d'Ivoire. En appliquant ce cas à des actes de cybercriminalité dont la preuve est rapportée, il devient envisageable d'imaginer la possibilité d'une entraide intercontinentale. Reste à savoir s'il existe en dehors de la Convention de Budapest, des fondements juridiques de l'extradition ou de la collaboration inter-Union européenne et Ouest-Afrique ?

Conclusion de la deuxième partie

La répression de la cybercriminalité en Afrique de l'Ouest se fait au fur et à mesure des évolutions technologiques sur ce continent à une exception près. Les infractions perpétrées en direction du continent européen se multiplient et ont une longueur d'avance sur la progression des législations africaines.

Dans une certaine mesure, l'Afrique de l'Ouest essaie de rattraper son retard en s'inspirant au plan des dispositions légales des sanctions déjà élaborées et appliquées au sein de l'Union Européenne. Cette assertion découle de la nature mais surtout de l'origine de certains actes qualifiés de cybercriminels. Ces infractions concernées, de par leur caractère transfrontière, exigent de les traiter en amont et en aval grâce à plusieurs interrogations: d'où elles proviennent ? Qui sont leurs cibles et comment en appréhender les auteurs complices et tout individu concerné ?

D'un point de vue des structures mises en place pour lutter contre la cybercriminalité, un effort considérable est fait depuis les années 2008 avec la mise en place dans la plupart des Etats d'organismes et d'institutions en charge de cette lutte. Sur ce plan, l'Afrique de l'Ouest est à féliciter. De nombreux progrès ont été faits aussi bien au niveau de la législation que des actions menées pour mettre un terme au fléau cybercriminel.

Sous l'angle des mécanismes employés, la sanction de la cybercriminalité passe par des entités de terrain comme le Joint Cybercrime Act Taskforce en Europe, ou la Plateforme de Lutte contre la Cybercriminalité ou encore la Brigade de Lutte contre la Cybercriminalité en Afrique de l'Ouest.

S'agissant des relations que l'Afrique de l'Ouest entretient avec l'Union Européenne, il faut également constater que si d'une part, l'Europe semble souvent être la cible des cybercriminels, d'autre part, les moyens sont mis en œuvre pour qu'il en aille autrement.

Des formations dans les deux sens sont organisées de même que des échanges intercontinentaux s'opèrent. En d'autres termes, la coopération bilatérale (si on considère les deux espaces étudiés comme des parties) fonctionne. Elle n'est pas uniquement infractionnelle, elle est également juridictionnelle, institutionnelle. Elle pêche certes à certains points de vue de par ses imperfections mais elle est perfectible.

La difficulté de réprimer ou de sanctionner la cybercriminalité n'est pas seulement limitée au fait que toutes les lois africaines ne sont pas encore élaborées. Elle tient surtout à la complexité de cet ensemble d'infractions : la cybercriminalité est en effet une boîte de Pandore qui contient une multitude de comportements répréhensibles. Elle est de plus variable d'un espace à l'autre. Les infractions commises au sein même de chaque espace diffèrent : cette diversification est source de difficulté quant à légiférer sur des comportements aussi divers.

Par ailleurs, le fait que les personnes qui commettent les infractions aient la possibilité d'échapper aux poursuites grâce à la virtualité des supports (le multimédia et les autres composantes) complexifie d'avantage la répression de la cybercriminalité.

La nomenclature des sanctions contre la cybercriminalité doit, de ce fait, s'adapter à la nature complexe des infractions elles-mêmes. Se limiter à certaines pratiques traditionnelles de répression comme les amendes pécuniaires ou encore les privations de liberté ne suffit plus. Il ne faut toutefois pas que les libertés des individus soient battues en brèche. Elles doivent être respectées. Or, sous couvert de ce respect, des limites à la sanction efficace naissent. Comment trouver le juste milieu, la proportionnalité ?

D'une certaine manière, certains projets de législation, à l'instar de la proposition de règlement européen contre la cybercriminalité proposent des normes adéquates et dissuasives. Cependant, face à l'évolution des technologies, le caractère dissuasif recherché à travers les normes doit être continuellement réaffirmé à travers des adaptations et des révisions.

Les différentes techniques mises en place notamment pour se protéger des cyber attaques montrent que la répression n'implique pas uniquement la sanction. Elles supposent également d'avoir mis les moyens en place pour éviter d'être une victime des actes cybercriminels. Toutefois, toutes ces mesures prises ne sont pas toujours efficaces. Il en est de même des lois punissant les actes de la cybercriminalité. Elles ne sont pas toujours coordonnées. Si bien que se dessinent les difficultés des peines non harmonisées ou encore des incriminations qui ne concordent pas d'un Etat à l'autre.

Toutes ces difficultés légales essaient d'être corrigées par la pratique notamment avec les organismes mis en place aussi bien au niveau européen qu'africain. La diversité

des organisations privées et publiques au service de la lutte contre la cybercriminalité souligne le caractère délicat de ce combat. Il n'a pas de limite comme d'ailleurs la cybercriminalité elle-même : à la fois virtuelle et réelle. Virtuelle parce que les infractions cybercriminelles empruntent les réseaux et voies numériques et réelles dans la mesure où les conséquences sont subies au quotidien par exemple sur les cartes bancaires, au niveau des données falsifiées pour ne retenir que ces deux exemples.

La mise en place des différentes structures est un marqueur de l'amplitude prise par le fléau de la cybercriminalité. Tous les secteurs sont touchés et de ce fait aucun d'entre eux ne doit être ignoré par le législateur. Si la répression de la cybercriminalité nécessite de comprendre les infractions composant cette forme particulière de criminalité, souvent commise en bande organisée, c'est parce que la cybercriminalité porte atteinte à la sécurité de toutes les couches composant les Etats. Qu'il s'agisse des administrations, des secteurs privés, de la vie des ménages ou des entreprises, aucune couche n'est épargnée. Et ce constat vaut aussi bien pour l'Union européenne que pour l'Afrique de l'ouest. Ce constat est d'ailleurs mondial. C'est pourquoi la collaboration entre les deux espaces étudiés est fondamentale pour parvenir à une répression efficace.

CONCLUSION GENERALE

Au terme de cette étude, on peut, dans une très large mesure, appréhender la cybercriminalité d'abord comme un ensemble d'infractions contre la haute technologie. Elle est surtout spécifique aux réseaux électroniques et numériques.

Ensuite, la commission du « *cybercrime* »[794] est alternativement le fait d'un individu isolé ou d'une bande organisée. La seconde hypothèse, fait intervenir au moins deux acteurs à des niveaux différents.

Enfin, doit être soulignée l'ambivalence de la nature de la cybercriminalité.

D'une part, on note que la cybercriminalité peut se manifester uniquement dans les limites territoriales d'un Etat. A titre d'illustration, un conjoint jaloux, qui espionne son épouse en accédant à son compte de messagerie électronique, commet un crime qui n'est pas en principe transfrontalier. En l'espèce, la réalisation du crime dont il s'agit ne fait nullement apparaître des circonstances de lieux renvoyant à d'autres espaces hors du cadre national, sous réserve de l'éventualité de l'hébergement des données personnelles de l'épouse, par un site situé à l'étranger.

D'autre part, le cybercrime se présente comme un phénomène transfrontalier. Les auteurs et leurs complices peuvent se trouver dans deux ou plusieurs Etats, ainsi que nous l'avons vu antérieurement avec l'analyse de la jurisprudence de la Chambre Criminelle de la Cour de cassation du 21 mars 2012 sur les faux sites d'enchères publiques.

Dans la logique de ce qui précède, la répression de la cybercriminalité doit se faire à l'aune des infractions en cause et surtout de la zone géographique considérée. C'est pourquoi, on observe que les sanctions prennent des formes variées. On doit aussi ajouter que le caractère transfrontalier de certaines de ces infractions ne fait pas obstacle à la prise en compte des particularismes de chaque Etat.

---

[794] Le *cybercrime* est un terme forgé par nous. Par ce vocable, nous entendons le crime commis via les réseaux cybernétiques ; le mot *cybercrime* étant utilisé en anglais pour désigner la cybercriminalité de façon générale.

Le champ d'application des lois est inévitablement élargi et nécessite des précisions et des éclaircissements pour chacune des évolutions.

La cybercriminalité dépasse le seuil des réseaux numériques et électroniques puisqu'elle prend une part importante dans les objets connectés[795]. Encore une fois, les modifications des habitudes sont des portes ouvertes aux actes malveillants. Dans ce contexte, les objets connectés tels que les montres, notamment de luxe, sont de nouvelles cibles de contrefaçons ou de détournement de la part de personnes mal intentionnées. Il s'agit là d'un nouveau domaine dont il faudra tenir compte pour les lois à venir. Cela soulève la question d'éventuelles adaptations sans fin dans le domaine de la cybercriminalité.

La problématique de l'adaptation sans fin de l'encadrement de la lutte contre la cybercriminalité est la première difficulté qui s'ajoute à la technicité de la matière à encadrer.

La seconde difficulté tient à la nature même de l'espace, théâtre des activités illicites, le cyberespace. Il n'est pas un terrain simple à cerner. C'est un espace à la fois réel et virtuel. De ce fait, l'encadrement juridique est difficile à réaliser puisque le cyberespace ne connaît pas de frontière. Or, l'une des particularités de la norme juridique est de réguler les questions en tenant compte des repères géographiques (c'est ce qui se passe avec la détermination des règles de compétence territoriales des juges par exemple).

La troisième complication est celle de la sanction des Etats dès lors que ses services sont eux-mêmes en infraction. Sous cet angle, l'Etat apparaît par l'intermédiaire de ses services (par exemple des agents de police en charge de la sécurité intérieure, et d'enquêtes) comme un cybercriminel. La question est celle de la limite : lorsque les services étatiques effectuent des actes qui dépassent leurs compétences et font d'eux des acteurs cybercriminels, l'Etat est-il toujours en mesure de sanctionner ? La limite de la proportionnalité conduit ainsi à s'interroger sur les conditions des sanctions dans ce cas. Pourquoi les Etats attendent-ils à chaque fois la censure de la Cour européenne des Droits

[795] Comme exemple d'objets connectés, on peut citer les montres.

de l'Homme alors qu'ils possèdent, dans la plupart des cas tous les éléments pour réaliser que leurs agents sont en dehors du cadre légal ?

L'exemple de la France le 18 septembre 2014 avec la sanction du STIC dans la décision de la Cour européenne des Droits de l'Homme du 2014 en est une illustration.

La protection contre la cybercriminalité doit d'abord provenir des personnes physiques ou morales elles-mêmes. Le cybercriminel peut en effet se servir aussi de la négligence constatée dans le comportement des personnes sur la toile. Il s'agit du *devoir individuel de sécurité informatique*. Au bout du compte, la protection assurée par l'Etat contre le phénomène de la cybercriminalité n'intervient qu'après. L'usage des réseaux sociaux doit de ce fait, être mesuré de la part des internautes. La responsabilité de ces usagers en dépend. Cette mesure est également une prise de conscience de la part des détenteurs de ces données à caractère personnel, souvent délaissées au motif de liberté d'expression, de communication, d'échange et de changement de mode de vie (on est passé à l'ère numérique et par conséquent, on vit essentiellement sur les réseaux électroniques au point d'en oublier trop souvent la vie réelle).

Il est certain que les pouvoirs publics et les prestataires de services électroniques et numériques ont une grande responsabilité en matière de confidentialité des données, notamment lorsque ces dernières doivent circuler sur les réseaux, sont inter-changées ou interconnectées. L'obligation pesant ainsi sur les institutions précitées n'exonère pas les usagers ou les internautes, quel que soit leur statut, d'un minimum de prudence.

La répression de la cybercriminalité n'est pas une science pénale accomplie. Elle est jeune aussi bien dans les Etats de l'Union européenne que dans ceux de l'Afrique de l'Ouest. Il y a une grande quantité de tâtonnements : tant au niveau des législations que des applications pratiques. Plusieurs sommets internationaux ou autres rassemblements de professionnels, sous forme de fora (comme le Forum International de la Cyber sécurité par exemple) se tiennent et constituent des lieux d'échanges. Ici, les professionnels en charge de la lutte contre la cybercriminalité confrontent souvent leurs expériences. Dans le même ordre d'idée, des centres de formations des policiers, des professionnels du droit et des professionnels de l'informatique sont créés. Des sessions d'échanges entre les différentes structures en charge du contrôle des données (à caractère personnel,

institutionnelles ou autres) sont mises en place. La conjugaison de tous ces efforts traduit la mutualisation des efforts.

Dans la lutte contre la forme transfrontalière de la cybercriminalité, l'appréhension puis la répression dans le cadre d'un Etat isolé constitueraient des démarches incongrues. En d'autres termes, les Etats africains et européens ont compris l'intérêt de mettre en commun les connaissances et les efforts pour combattre la cybercriminalité. La mutualisation des efforts est à tous les plans : normatif, technique, dans la poursuite des enquêtes et dans l'appréhension des cybercriminels.

S'agissant du plan technique, sécuriser les informations transitant sur les réseaux entre peu à peu dans les habitudes. Mais il reste encore du travail sur ce point. Certaines personnes ayant recours aux réseaux numériques ne se sentent pas encore directement concernées.

Pour ce qui est de l'aspect normatif, le fait que plusieurs Etats non membres du Conseil de l'Europe veuillent adopter la Convention pour la lutte contre la cybercriminalité est un signe de convergence vers l'éradication de cette lutte. Quant à l'appréhension coordonnée des cybercriminels, les Convention Eurojust, Europol, Interpol et les Conventions d'entraide en matière d'extradition jouent un rôle essentiel qu'il convient d'entretenir. Ces institutions sont des gages de la mutualisation des efforts pour lutter efficacement contre la cybercriminalité.

Les hésitations qui surviennent aujourd'hui permettront de cerner davantage les questions. Elles favoriseront, si elles sont bien exploitées, l'éradication du fléau.

L'Afrique de l'Ouest a accusé un retard au démarrage de la lutte contre la cybercriminalité. Au moment où notre analyse de la situation est présentée, le continent africain en est à la collaboration avec l'Union européenne notamment par l'intermédiaire de missions, de formations de professionnels des polices et des gendarmeries des pays ouest-africains par de professionnels de l'OCLCTIC ou encore d'autres structures internationales.

D'autres initiatives comme les réunions des différentes autorités en charge des données personnelles au niveau de l'Afrique notamment au Burkina Faso ou encore au Togo avec la Commission Nationale Informatique et Libertés sont à souligner dans ce cadre. Ces

réunions sont des moyens de sensibilisation non seulement des institutions publiques et privées mais également des populations contre le phénomène de la cybercriminalité. De ce point de vue, des adaptations des expériences européennes peuvent être faites afin de mieux appréhender les problématiques de lutte contre la cybercriminalité sur le continent africain.

L'Afrique de l'Ouest n'est pas la seule à tirer profit de ces communications. L'Union européenne et ses ressortissants en bénéficient. Les résultats de ces partages d'expérience sont notables au niveau de la qualité des réseaux ou encore dans les processus de transfert de données. Au niveau des réseaux, les apports techniques permettent l'amélioration des connexions électroniques. Les flux et les échanges d'information en provenance de l'Afrique s'en retrouvent améliorés.

La lutte contre la cybercriminalité a fait naître de nouveaux concepts comme la cyber-sécurité, la cyberguerre, des concepts très utilisés aussi bien au quotidien que dans les discours politiques. Ces concepts ne sont pas abstraits et revêtent beaucoup de réalité grâce aux affaires de cyber-espionnage, d'écoutes de masse de la part des Etats ou encore des séries de piratages des sites internet des institutions[796], des enseignes de jeux électroniques comme le cas de Microsoft avec son jeu vidéo XBOX, dont les interfaces ont été piratées courant décembre 2014[797].

Toutes ces attaques quels que soient le domaine et la couche sociale montrent que la cybercriminalité est un phénomène réel dans le monde actuel mais potentiel dans la vie de chaque personne. Les technologies ne cessent d'évoluer et les attaques des cybercriminels se perfectionnent, se professionnalisent pour prendre des proportions inquiétantes. A en croire, la multiplication des actes cybercriminels, certains spécialistes en cyber-sécurité parlent de troisième guerre mondiale empruntant les canaux numériques. D'ailleurs, plusieurs Etats de l'Asie tels que la Chine sont souvent accusés

[796]Cf. **Barbara LEBLANC**, BERCY, victime d'une attaque informatique, article disponible sur http://www.usinenouvelle.com/article/bercy-victime-d-d-une-attaque-informatique.n147759.

[797]Cf. Journal Le Monde du 26 décembre 2014, Les serveurs des consoles Xbox et Playstation, victimes d'une attaque ?

de préparer une arme cybernétique. De telles accusations suscitent des attitudes méfiantes entre Etats, ce qui naturellement ne favorise pas une bonne coopération.

Pour l'heure, les Etats ouest-africains et ceux de l'Union européenne en sont à des collaborations, des échanges et des actes de coopération afin de lutter ensemble contre la cybercriminalité. Les expériences des deux communautés d'Etats sont réciproquement enrichissantes et les erreurs ou les éventuels échecs de l'Union européenne devront servir aux Etats ouest-africains, si ces derniers en font les lectures adéquates et adaptées.

BIBLIOGRAPHIE

OUVRAGES GENERAUX

ASCENSIO (H), DECAUX (E) et PELLET (A), Droit international pénal, éditions A. Pedone, Paris, 2012.

BEAUVALLET (O), les investigations judiciaires internationales, ouvrage collectif avec une préface de Jean PRADEL, éditions Berger Levrault, Mai 2014, 340 p.

BITAN (H), Droit et expertise des contrats informatiques, éd. Lamy Axe Droit.

BORDEAU (J), entreprises et marques, les nouveaux codes de langage, éd. EYROLLES, 2010, 286 p.

CARNEROLI (S), les contrats commentés du monde informatique, logiciels, bases de données, multimédias, internet, collection création informatique communication, éditions Larcier, Bruxelles, 2007.

CASSUTO (T), Une Europe, deux lois pénales, collection Macro droit/ Micro droit, éditions Bruylant, décembre 2012, 235 p.

CASTETS-RENARD (C), Droit de l'internet : droit français et européen, éditions Montchrestien, 2e éditions, Paris, 2012.

CLERGERIE (J-L), GRUBER (A) et RAMBAUD (P), L'Union Européenne, Précis de Droit public et science politique, édition Dalloz, 2014,1076 p.

CORTEN (O), Méthodologie du droit international public, éditions de l'Université de Bruxelles, Bruxelles, 2009.

DAVID (E), Eléments de droit pénal international et européen, Précis de la faculté de droit de l'Université Libre de Bruxelles, Bruylant, 2009/

DE BELLEFONDS (X-L), Le droit du commerce électronique, que sais-je, éditions presses universitaires de France (PUF), Paris, 2005.

DE BOISSIERE (J-B) et B. WARUSFEL, La nouvelle frontière de la technologie européenne, Calmann-Lévy, France, 1991.

DE COSTER (T), M. DEMOULIN, H. JACQUEMIN, E. MONTERO, M. VANDERCAMMEN, T. VERBIEST, Les Pratiques du commerce électronique, Cahiers du centre de recherches informatique et Droit, Bruylant, Bruxelles, 2007.

DE FROUVILLE (O), La preuve pénale, internationalisation et nouvelles technologies, Perspectives sur la Justice, La documentation française, Paris, 2007.

DEBBASCH (C), H. ISAR, X. AGOSTINELLI, Droit de la communication, audiovisuel, presse, Internet, 1ère édition, Dalloz, droit public et science politique, Paris, 2002.

DELMAS-MARTY (M), Les sources du droit international pénal : l'expérience des tribunaux pénaux internationaux et le statut de la Cour Pénale internationale, publié par l'unité de recherche de droit comparé, Société de Législation comparée, Paris, 2005. DELMAS-MARTY (M), M. PIETH, U. SIEBER, Les chemins de l'harmonisation pénale, Harmonising criminal law, UMR de droit comparé de Paris, volume 15, Société de législation comparée, Paris 2008.

DEVEZE (J), J. FRAYSSINET, A. LUCAS, le droit de l'informatique et de l'Internet, Paris, Presses Universitaires de France, 2001.

DOUTRELEPONT (C), P. VAN BINST, L. WILKIN, Libertés, droits et réseaux dans la société de l'information, groupe de recherche en Informatique et sciences humaines, collection de la faculté de droit, Université de Bruxelles, Bruylant, LGDJ, Paris, 1996.

DUPUY (P-M), Droit international Public, précis Dalloz, 8ème édition, Dalloz 2006. FAUCHOUX (V) et DEPREZ (P), Communication et commerce électronique : le droit de l'internet, éd. LITEC, Paris, 2008.

FINES (L), Les crimes invisibles, délits contemporains, dénonciation et temps de réaction, Liber, Montréal, 2013.

FLORE (D), Droit pénal européen : les enjeux d'une justice pénale européenne, Groupe De Boeck, éditions LARCIER, Bruxelles, 2009.

GHERNAOUTI-HELIE (S) et A. DUFOUR, De l'ordinateur à la société de l'information, collection que sais-je, 2e édition, PUF, Paris, 2001.

GIUDICELLI-DELAGE (G), STEFANO (M), TRICOT (J), L'intégration pénale indirecte : interactions entre droit pénal et coopération judiciaire au sein de l'Union européenne Unité mixte de recherche de droit comparé. Paris Association de recherches pénales européennes. France, DL 2005.

GIUDICELLI-DELAGE (G) et LAZERGES (C), Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne, Société de législation comparée, Collection : Unité mixte de recherche de droit comparé de Paris (Université de Paris I / CNRS UMR 8103), juillet 2012.

Groupe Revue Fiduciaire, Informatique et Libertés mode d'emploi, collection les essentiels RF, Belgique, DL 2007.

GUINCHARD (S) et BUISSON (J), Procédure pénale, LexisNexis, 10 ème édition, Paris, 2014.

HUDAULT (B), Traitement informatique et droit pénal des affaires, extrait de la collection des travaux de la faculté de Lille, 1977.

LAUDE (A), MATHIEU (B),TABUTEAU (D), Droit de la santé, 3ème édition mise à jour, Thémis, droit, Puf, Paris, 2012.

LE TOURNEAU (P), Contrats informatiques et électroniques, Négociations et rédaction des contrats informatiques et du numérique, 7e édition, collection Dalloz référence, Paris 2012.

MOREAU DEFARGES (P), La mondialisation, DL 1997, 4ème édition mise à jour 2002, Paris, PUF.

MOREILLON (L) et WILLI-JAYET (A), Coopération judiciaire pénale dans l'Union européenne, dossiers de droit européen collection dirigée par Christine KADDOUS et Pierre MERCIER, Helbing & Lichtenhahn Bruylant, LGDJ, Bruxelles, 2005.

NIBOYET M-L. et Geraud de Geouffre de la Pradelle, Droit international privé, 4é edition, LGDJ Lextenso Editions, 2013.

PIOTRAUT (J-L), Droit de la Propriété Intellectuelle, éd. Ellipses.

PRADEL (J) et DALLEST (J), La criminalité organisée en droit français, droit international et droit comparé, éditions LexisNexis, Paris, 2012.

PRADEL (J), CORSTENS (G), VERMEULEN (G), Droit pénal européen, Précis de droit privé, 3e édition, DALLOZ 2009.

ROGGEN (F), Actualité en droit pénal, 1ère édition, BRUYLANT, février 2012.

SERAGLINI (C) et J. ORTSCHEIDT, Droit de l'arbitrage interne et international, LGDJ Montchrestien Lextenso éditions, Paris, 2013.

WAUTELET (M), les cyberconflits, internet, autoroutes de l'information et cyberespace : quelles menaces ?, éditions Complexe, GRIP, Bruxelles, 1998.

WEYEMBERGH (A) et DE BIOLLEY (S), Comment évaluer le droit pénal européen ? Institut d'études européennes, éditions de l'Université de Bruxelles, 2006.

WITZ (C), le droit allemand, connaissance du droit, 2edeition, Dalloz, Paris, 2013.

ZIMMERMANN (R), La coopération judiciaire internationale en matière pénale, 3e édition, Bruylant, Bruxelles, 2009.

OUVRAGES SPECIALISES

OUVRAGES EN LANGUE FRANÇAISE

ABELLO A., La licence, instrument de régulation des droits de la propriété intellectuelle, LGDJ, Paris, 2008.

ALBITZ Paul et LIU Cricket traduction de Giles CARRÉ, DNS et BIND, Adminstration système et réseau, O'Reilly & Associates, 4ème edition, Paris 2001.

AMBLARD P., Régulation de l'Internet : l'élaboration des règles de conduite par le dialogue inter normatif, édition Bruylant, Bruxelles, 2004.

ARPAGIAN N., la cybersécurité, que sais-je, éditions presses universitaires de France, Paris, 2010.

ATELIN P., WIFI, solution de sécurisation, collection TechNote, ENI éditions, Saint Herblain, France, octobre 2006.

BA Abdoul, Internet, cyberespace et usages en Afrique, édition l'Harmattan, 2003. BALLE F., Médias & Sociétés, collection Domat politique, édition Montchrestien 15ème édition, Paris, 2011.

BAUDIN L., Les cyber-attaques dans les conflits armés, qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire, éditions L'Harmattan, Paris, 2014.

BAUDRAND V. & MARIE HENRY G., La mondialisation, collection Studyrama, Paris, 2006.

BECKET Brian, Introduction aux méthodes de la cryptologie traduit de l'anglais par Philippe Béguin, Philippe Klein et Éric Henault, publié à Paris, Milan, Barcelone : Masson, collection Logique, mathématiques, informatique, 1990.

BENISSAD H., Blanchiments de capitaux, aspects économiques et juridiques, Economica, Paris, 2014.

BENSOUSSAN A. et Le ROUX Y., Cryptologie et signature électronique : aspects juridiques, Hermès Sciences publications, Paris, 1999.

BERNHEIM-VAN DE CASTEELE L., Les principes fondamentaux de l'arbitrage, collection sous la direction de Francarbi, Bruylant, Bruxelles, 2012.

BLOCH L. et WOLFHUGEL C., Sécurité informatique : principes, méthodes à l'usage des DSI, RSSI et administrations, 3è édition, Eyrolles, Paris, 2011.

BOURCIER D., HASSET P., ROQUILLY C., Droit et Intelligence artificielle : une révolution de la connaissance juridique, collection Droit et Technologie, Paris : Romillat, 2000.

BOYER B., Cybertactique conduire la guerre numérique, préface du Contre-amiral Arnaud COUSTILLIERE, collection cyberespace et cyberdéfense dirigée par Nicolas ARPAGIAN, éditions NUVIS, Paris, 2014.

BRANCO Juan, Réponses HADOPI suivi d'un entretien avec Jean-Luc GODARD, éditions CAPRICI, collection actualité critique, Paris, 2011.

BUFFELAN-LANORE J-P., Le langage de l'administration et du cyberdroit, éditions de l'IRIJ, Paris 1998.

CARTAU Cédric, La sécurité du système d'information des établissements de santé, Presses de l'Ecole des Hautes Etudes en Santé Publique, 2012.

CHAMOUX J.P., Menace sur l'ordinateur, Seuil, Paris, DL 1986.

CHENEAU-LOCQUAY Annie, Les fractures numériques nord/sud en questions, CEAN-CNRS/ AFRICA'NTI, collection Cahier des sciences sociales sur les enjeux des technologies de la communication dans les sud, éditions L'Harmattan, DL 2004.

Conseil de l'Europe, La protection des données à caractère personnel collectées et traitées à des fins statistiques, adoptée par le Comité des Ministres du Conseil de l'Europe le 30 septembre 1997 et exposé des motifs, Strasbourg : Éd. du Conseil de l'Europe, 1998, Collection Références juridiques.

DE PRELLE Olivia, DOCQUIR Benjamin, FLAMEE Michel, GLAS Geert, HEREMANS Tom, LAURENT Philippe, VERGOTE Peter, Centre Belge d'Arbitrage et de mediation (CEPANI) , Les noms de domaine.be, éditions Bruylant, de Boecke 2013.

DERIEUX Emmanuel et GRANCHET Agnès, Lutte contre le téléchargement illégal: lois DADVSI et HADOPI, édition LAMY, France, 2010.

DERUELLE Jean, de la préhistoire à l'Atlantide des mégalithes : les leçons du Radiocarbone édition France-empire, 1990.

DEWULF G., SCHAUSS Marc, LESUISSE R., La maintenance de logiciel: aspects techniques et juridiques, cahiers du centre de recherches Informatique et droit, éditions Story-Scientia, Bruxelles, 1989.

DOSSE (S), KEMPF (O), MALIS (C), le cyberespace nouveau domaine de la pensée stratégique, collection cyberstratgéie, Economica, juin 2013.

DREYFUS N., Marque et internet, protection, valorisation, défense, collection ALamy Axe droit, Wolter Kluwer, France 2011.

DU MANOIR DE JUAYE T., Le droit de l'intelligence économique, édition LexisNexis, Paris, Litec, 2007.

FARCHY J., Internet et le droit d'auteur, la culture Napster, CNRS éditions, collection CNRS Communication, Paris, 2003.

FAYON D., Géopolitique d'Internet, qui gouverne le monde ? Préface de Joel de Rosnay, Economica, Paris, 2013.

FDIDA S., Des autoroutes de l'information au cyberespace, Collection DOMINOS, édition Flammarion, paris 1997.

FERAL-SCHUHL C., Cyberdroit, le droit à l'épreuve de l'internet, 6e éd. DALLOZ, Paris, 2010.

FILIOL E. & RICHARD P., Cybercriminalité, enquête sur les mafias qui envahissent le web, Dunod, Paris, 2006.

FILIOL E., les techniques virales avancées, éditions Springer, Collection IRIS, Paris, DL 2006.

FILIOL E., les virus informatiques : théorie, pratique et applications, collection IRIS, éditions Springer Verlag, 2004.

FOREST D. et KAUFMAN G., Droit de l'informatique, éditions Gualino-Lextenso, Paris, DL 2010.

FOREST D., Droit des données personnelles, Paris, éditions Gualino-Lextenso, DL 2011.

FRANCHIN F. et MONNET R., le business de la Cybercriminalité, Publication Lavoisier, Collection Management et informatique dirigée par Nicolas Manson, Paris, 2005.

GABAS J.J., L'Union européenne et les pays ACP : un espace de coopération à construire, GEMDEV, 1999, Paris.

GABAS J.J., Société numérique et développement en Afrique, usages et politiques publiques GEMDEV-KARTHALA, 2005.

GERBER F., de l'inutilité du juge d'instruction, Bourin Editeur, Paris, 2010

GIUDECELLI-DELAGE G. et MANACORDA S., avec la coordination de J. TRICOT, Cour de justice et Justice pénale en Europe, Association de recherches pénales européennes, Société de Législation comparée, Collection de l'UMR de Droit comparé de Paris, Paris, 2010.

GRENIER J-G., Dictionnaire d'informatique et d'internet, la maison du dictionnaire, Paris, 2000.

GUEDON J-C., la planète cyber internet et le cyberespace, découvertes Gallimard Techniques, mars 1996.

GUERRIER C. et MONGET M-C., Droit et sécurité des Télécommunications, collection Technique et scientifique des télécommunications, Springer-Verlag, Paris, 2000.

GUILLAUME Marc, L'empire des réseaux, éditions DESCARTES & Cie, Paris, 1999.

GUISNEL J., Guerres dans le Cyberespace, services secrets et internet, éditions la Découverte, Paris, 1995.

HUET J. et DREYER E., Droit de la communication numérique, Lextenso éditions LGDJ 2011.

JENCLOS J-Y., Droit pénal européen, dimension historique, Economica, Paris, 2009.

JEZ E. et BEAURAIN N., les noms de domaine de l'internet : aspects juridiques, éd. LITEC, collection Droit@Litec Maîtriser, Paris 2001.

KOSSI A.-V., la protection des données à caractère personnel à l'ère de l'Internet, Impact sur l'évolution du cadre normatif et nouveaux enjeux. Etat des lieux en France et en Allemagne, Publications Universitaires Européennes, Peter LANG, Frankfurt am Main 2011.

LAFOUASSE F., L'espionnage dans le droit international, nouveau monde éditions, Paris, 2012.

LAMERE J-M., LEROUX Y. et TOURLY J., la sécurité des réseaux, méthodes et techniques, édition DUNOD informatique, Paris, 1989.

LAURENT J., L'histoire secrète de Wikileaks, enquête sur la première grande affaire d'espionnage du XXIe siècle, Collection contre-enquête, DL 2011.

LEDJOU J-M. et RANDRIANASOLO-RAKOTOBE H., Des réseaux et des hommes, les Suds à l'heure des technologies de l'information et de la communication, éditions Gemdev-Karthala, Paris, 2013.

LEMESLE R-M., La convention de Lomé : Principaux objectifs et exemples d'action 1975-1995, 20e anniversaire de la coopération Union Européenne- Etats ACP, notes

africaines, asiatiques et caraïbes, Centre des Hautes études sur l'Afrique et l'Asie Modernes, Paris, 1995.

LEMOINE V., Le régime juridique des constatations policières sur internet, éditions l'Harmattan, Paris, 2014.

LEROY F., Réseaux sociaux et Cie, le commerce des données personnelles, Actes suds questions de société, 2013.

LOINTIER Pascal avec Anna Bakalova, Vesselin Bontchev, Vassil Habov et la participation de Bryan Clough et Paul Mungo et de Vladimir Kostov, À la poursuite de Dark Avenger : l'affaire des virus au goût bulgare, Paris : Dunod tech, 1993.

MARECHAL C., Concurrence et propriété intellectuelle, éd. Lexis Nexis, collection de l'institut de recherche en propriété intellectuelle, Paris 2009.

MARTIN D., la criminalité informatique Cybercrime : sabotage, piratage, etc. évolution et répression, éditions presses universitaires de France, Collection Criminalité internationale, 1997.

MASCALA C., A propos de la sanction, les travaux de l'IFR Mutation des Normes Juridiques n°6, LGDJ 2007.

MATHIEN M. et FULLSACK J., Ethique de la société de l'information, collection Médias, sociétés et Relations Internationales, publication du Centre d'Etudes et de Recherches Interdisciplinaires sur les Médias en Europe (CERIME), éditions Bruylant 2008.

MATTATIA F., Traitement des données personnelles, le guide juridique, la loi informatique et libertés et la CNIL, Jurisprudences, éditions EYROLLES, Paris, 2013.

MATTELART A., la globalisation de la surveillance : aux origines de l'ordre sécuritaire, éditions la découverte, 2008.

MOREILLON L. et A. WILLI-JAYET A., Coopération judiciaire pénale dans l'Union européenne, Collection dirigée par Christine KADDOUS et Pierre MERCIER, HELBING & LICHTENHAHN BRUYLANT LGDJ 2005.

OHMAE K., La triade, émergence d'une stratégie mondiale de la puissance, traduit de l'anglais au français par Chantal Pommier, titre d'origine « *Triad power : the coming shape of global competition*, édition Flammarion, Paris, 1985.

Ordre national des médecins Conseil National de l'ordre, Autoroutes de l'information et déontologie médicale, Masson, Paris, 1996.

OUATTARA A., La preuve électronique, étude de droit comparé Afrique, Europe, Canada, collection Horizons Juridiques Africains, Centre de Droit Economique, PUF d'Aix-Marseille, 2011.

PEDROT P., Traçabilité et Responsabilité, Economica, Paris, 2003.

PEREZ ASINARI M. V. et PALAZZI P., Défis du droit à la protection de la vie privée, perspectives du droit européen et nord-américain, cahiers du centre de recherches Informatique et Droit, édition Bruylant, Bruxelles, 2008.

PERRODET A., Etude pour un ministère public européen, L.G.D.J., Paris, 2001.

PIETTE-COUDOL Thierry, La signature électronique, éditions Litec, Paris, 2001.

PONCELLA P. et ROTH R., La fabrique du droit des sanctions pénales au Conseil de l'Europe, la documentation française, Paris, 2006.

QUEMENER M. et CHARPENEL Y., Cybercriminalité : droit pénal appliqué, édition Economica, 2010.

QUEMENER M. et PINTE J., Cybersécurité des acteurs économiques, risques, réponses stratégiques et juridiques, Hermès, Lavoisier, collection Cyberconflits et cybercriminalité, Paris, 2013.

QUEMENER M., Cybercriminalité : défi mondial, édition Economica, Paris, 2007

REFALO P-L., La sécurité numérique de l'entreprise, l'effet papillon du hacker, Eyrolles, Paris, 2013.

RUBISE P., L'assurance des risques techniques, les fondamentaux de l'Assurance, éditions l'Argus, Paris, 1999.

RUIZ FABRI H. et SOREL J-M., Indépendance et impartialité des juges internationaux, collection contentieux international, éditions A. PEDONE, Paris, 2010.

SAINT-LAURENT M., Cyberintimidation, des conséquences sans fin, les paroles s'envolent, mais les photos et les écrits restent ! BELIVEAU éditeur, Québec, Canada, 2012.

SCHULTZ T., Réguler le commerce électronique par la résolution des litiges en ligne, une approche critique, Cahiers du centre de recherches informatique et de droit, LGDJ, Paris, 2005.

SINGH Simon, histoire des codes secrets, de l'Egypte des pharaons à l'ordinateur quantique, traduit de l'anglais par Catherine Coqueret, titre d'origine « The code book », publié par Fourth Estate Limited, publication Paris J-C. Lattès, 1999.

SOUPIZET J-F., la fracture numérique Nord-Sud, collection « Nouvelles Technologies de l'Information et de la Communication », éditions Economica, Paris, 2005.

VENTRE David, Cyberattaque et Cyberdéfense, édition LAVOISIER, Hermès science, collection cyberconflit et cybercriminalité, Paris, 2011.

VIALOU T., l'art des cavernes, les sanctuaires de la préhistoire, collection Science et découvertes, édition du rocher Jean-Paul Bertrand Editeur, 1987.

VIRILIO Paul, la bombe informatique, édition Galilée, collection l'espace critique dirigée par Paul VIRILIO, Paris, 1998.

WARUSFEL Bertrand, Industrie, technologie et défense, Centre de recherches Droit et défense, la Documentation française, 1993.

WARUSFEL Bertrand, La propriété intellectuelle et l'internet, Dominos, Flammarion, 2001.

WARUSFEL Bertrand, Le renseignement français contemporain, aspects politiques et juridiques, L'Harmattan, Paris, 2003.

WEYEMBERGH A. et DE BIOLLEY S., Comment évaluer le droit pénal européen ?, Institut d'Etudes Européennes.

OUVRAGES PROPRES A L'AFRIQUE DE L'OUEST

ADJOVI Emmanuel V., Les instances de régulation des médias en Afrique de l'Ouest, le cas du Bénin éditions KHARTALA- FES, Paris, 2003.

AHOYO Christian Parfait, Pour une vraie économie numérique au Bénin, éditions Ouanilo, France, 2006.

BONJAWO J., Révolution numérique dans les pays en développement, l'exemple africain, Dunod, Paris 2011.

BUSKENS I., Les Africaines et les TIC : enquête sur les technologies, la question de genre et autonomisation, Paris : l'Harmattan ; Québec (Québec) : Presses de l'Université Laval ; Ottawa : Centre de recherches pour le développement international, DL 2011.

CODO L. C., Le Bénin dans les rapports ouest-africains, stratégie d'insertion, bilatéralisme sous régional et engagements régionaux, Centre d'Etude d'Afrique Noire, Institut d'Etudes politiques, Université de Bordeaux I, collection les « Multigraphiés » du CEAN, 1987.

DARLINGTON I.-J., Criminology: the study of crime, SIJ Publishers, Port-Harcourt, Nigeria, 1995.

DUFRENOT G., HOUESSOU E. et NONFODJI E., Politique budgétaire et dette dans les pays de l'UEMOA, Economica, Paris, 2007.

OSSAMA F., Les nouvelles technologies de l'information : enjeux pour l'Afrique subsaharienne, Paris, Montréal, l'Harmattan, 2001.

OBIARAERI NNAMDI ONYEKA, Law and policy on technology transfer to Nigeria, International Universities Press Limited, 1995.

OFORI-BOATENG J., The Ghana Law of Evidence, Waterville Publishing House, Accra, 1993.

SALL A., La justice de l'intégration, réflexion sur les institutions judiciaires de la CEDEAO et de l'UEMOA, éditions CREDILA, DL mai 2011.

THIAM Cheick Tidiane & Demba SY avec la collaboration de Renaud de la Brosse, Législations et pluralisme radiophonique en Afrique de l'Ouest, institut PANOS, centre de recherche, d'Etude et de Documentation, sur les Institutions et les Législations Africaines, L'Harmattan, Paris, 1997.

TOURE P. Assane, Le traitement de la cybercriminalité devant le juge: L'exemple du Sénégal, éditions L'Harmattan, mars 2014.

OUVRAGES EN ANGLAIS ET ALLEMAND

BLAKESLEE Melise R, Internet crimes, torts and scams: investigation and remedies, Royaume Uni, 2010.

BOISTER N., An introduction to transnational law, Oxford University Press, United Kingdom, 2012.

BRENNER S., cyberthreats: the emerging fault lines of the nation states, New-York, Oxford University Press, Royaume Uni, 2009.

BRENNER S., Cyberthreats and the decline of the nation-State, Routeledge, 2014.

CARR Indira, Computer crime, The international library of criminology, criminal justice and penology, second series, Ashgate, Surerey, England, 2009.

CASEY Eoghan, Digital evidence and computer crime, forensic science, computer and the Internet, second edition, Elsevier Academic Press, 2004.

DAVID Matthew, Peer to Peer and the music industry the criminalization of sharing, Sage publication, first publication, 2010 IN ASSOCIATION WITH Theory, Culture & Society.

HIRST M., Jurisdiction and the ambit of criminal law, Oxford University press, New-York, 2003.

GHERNAOUTI S., Cyberpower, crime, conflict and security in cyberspace, EPFL Press distributed by CRC Press, Lausanne, 2013.

JOFER Robert, Strafverfolgung im Internet,Europäische Hochschulschiiften, Peter Lang, Frankfurt am Main, 1999.

KOOPS B.J. and BRENNER Susan W., Cybercrime and jurisdiction, a global survey, T.M.C. ASSER PRESS, the Hague, 2006.

LIM E., The Clash between trade mark law and freedom of speech in cyberspace: does ICANN's UDRP strike the right balance? 2004.

LIM Eugene, The clash between trade marks law and freedom of speech in cyberspace: does INCANN's UDRP strike the right balance? LLM, University of Toronto, 2004.

LINDSAY D., International Domain Name Law, ICANN and the UDRP, Hart Publishing, USA, 2007.

NEWMAN R. C., Computer Forensics, evidence collection and Management, Auerbach publications, 2007.

PARKER Donn B., Fighting Computer Crime a new framework for protecting information, Wiley computer publishing, USA, 1998.

ROJAS Raùl and HASHAGEN Ulf, The first computers, History of computing, Editions Cambridge (Mass) MIT press, 2000.

ROLAND A. & SCHIMAN P., Strategic Computing: Darpa and the quest of machine, 1983-1993, collection History of computing, Cambridge, Mass: MIT Press, 2002.

SCHULTZ T., Information Technology and arbitration, a practitioner's guide, foreword by Gabrielle KAUFMANN-KOHLER, Kluwer Law International, United Kingdom, 2006.

SIEBER U., KASPERSEN R., VANDENBERGHE G., STUURMAN K., The legal aspects of computer crime and Security: a comparative analysis with suggestions for future international action, 1987.

TRAVIS H., Cyberspace Law censorship and regulation of the internet, Routledge Taylor & Francis Group, USA and Canada, 2013.

Van CUSTEM J. P., International Grouping of Accountants and Lawyers (E-Commerce in the world, aspects of comparative Law, éditions Bruylant, 2008.

VON DEM BUSSCHE Axel & STAMM Markus, Data Protection in Germany, Verlag C. H. Beck, German Law Accessible München, 2013.

WALL D. S., Crime and deviance in cyberspace, the international library of criminology, criminal justice and penology, second series, Ashgate, 2009.

WALL D. S., Cybercrime: the transformation of crime in the information age, collection crime and society series, Cambridge Malden Mass: polity, Royaume Uni, 2007.

ARTICLES

ARTICLES GENERAUX

ACKRICH (M) et MEADEL (C), e-Santé et Nouvelles technologies internet, Tiers nébuleux de la relation patient-médecin, les tribunes de la santé n° 29 – hiver 2010.

ADAM Nicolas, L'ICANN et la gouvernance d'Internet: une histoire organisationnelle. *Cahier de recherche*, 2007, vol. 7, p. 01.

AL-NEMRAT Ameer, Hamid JAHANKHANI, David S PRESTON, Global Security, Safety, and Sustainability Communications in Computer and Information Science Volume 92, 2010, pp 55-62, Cybercrime victimisations / Criminalisation and punishment, Springer Berlin Heidelberg.

CAPITANT (S) « La radio en Afrique de l'Ouest, un « média carrefour » sous-estimé ? », *Réseaux* 4/2008 (n° 150), p. 189-217.

CHARPENEL (Y), Cybercrime : Jurisprudence de la Cour de cassation, *Cahiers de la sécurité* n°6, oct. 2008, Institut National des Hautes Etudes de Sécurité.

CHENEAU-LOQUAY (A), L'Afrique au seuil de la révolution des Télécommunications, les grandes tendances de la diffusion des TIC, *Afrique contemporaine*, 2010/2 n° 234, p. 93-112.

GRANDE (E). Droit pénal et principe de légalité : la perspective du comparatiste in *Revue internationale de droit comparé*. Vol. 56 n°1,2004. pp. 119-129.

GRUNVALD (S), « Police et LOPPSI 2 : quels enjeux pour la justice pénale ? », *Archives de politique criminelle*, 2011/1 n°33, p. 63-78.

HAGUENAU (C), Sanctions pénales destinées à assurer le respect du droit communautaire, *Revue de Marché Commun de l'Union européenne*, avril 1993, p. 354-355.

IZORCHE (M-L) et DELMAS-MARTY (M), Marge nationale d'appréciation et internationalisation du droit. Réflexions sur la validité formelle d'un droit commun pluraliste, *Revue internationale de Droit comparé*, 2000, volume 52, n°4, p. 753-780.

PAILLOUX (P), Cyber défense, une agence à compétence nationale, *Revue de la Gendarmerie Nationale*, n° 234, mars 2010 p. 25 et s.

PESCATORE (P), « Le recours, dans la jurisprudence de la Cour de justice des Communautés européennes, à des normes déduites de la comparaison des droits des Etats membres » in *Revue internationale de droit comparé*, vol. 32 n°2, Avril-juin 1980. pp. 337-359.

TOZZO (E), « La réforme des médias publics en Afrique de l'Ouest, Servir le gouvernement ou le citoyen », *Politique africaine* 2005/1 n°97, p. 99-115.

David S. WALL, Digital Realism and the Governance of Spam as Cybercrime, *European Journal on Criminal Policy and Research*, December 2004, Volume 10, Issue 4, pp 309-335, Kluwer Academic Publishers.

ARTICLES SPECIALISES

ADEN (H), « Les effets au niveau national et régional de la coopération internationale des polices : un système spécifique de multi-level governance », *Cultures et Conflits*, [en ligne] http://conflits.revues.org/index899.html.

BELLAIS (R), les enjeux de la maîtrise de l'information dans la défense, *Réseaux*, 1998, volume 16 n°91 pp 121-133.

BELLANOVA (R), P. DE HERT, Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique, *Culture et conflit*, n°74 (été 2009) Sécurité et Protection des données.

BERNARDI (A), « Stratégies pour une harmonisation des systèmes pénaux européens », Archives de politique criminelle, 2002/1 n°24, p.195-233.

BIGOT (J-P), Dépolluer le numérique : le filtrage d'internet est souhaitable mais pas sans une réforme de sa gouvernance, Gazette du Palais 24 juillet 2010 n° 205, p. 15.

BURGORGUE-LARSEN (L), « les nouvelles technologies », Pouvoirs, 2009/3 n°130, P. 65-80.

DE LA CHAPELLE Bertrand, Souveraineté et juridiction dans le cyberespace in *Hérodote Revue de géographie et de géopolitique* 2014/1-2 (n° 152-153).

GRUBER (A), E- democracy : la loi « Informatique et libertés » en France, in Petites Affiches- 12 octobre 2005.

GRUBER (A), le système français de protection des données personnelles, in Petites Affiches n° 90 – 4 mai 2007.

DE FONTAINE VIVE (P), L'Europe et le capital-risque, Revue d'économie financière, 2008, volume 93, numéro 93, p.45-53.

ITEANU Olivier, « L'Icann, un exemple de gouvernance originale ou un cas de law intelligence ? », *Les Cahiers du numérique* 2/ 2002 (Vol. 3), p. 145-157.

LACROIX D., Ranger la terre. Le nommage des domaines est-il l'expression d'une stratégie des États-Unis de domination des réseaux ? in *Hérodote Revue de géographie et de géopolitique* 2014/1-2 (n° 152-153).

LAFRANCE (J-P.), Le laboratoire Internet, Réseaux, 1996, volume 14 n° 77, pp 171-183.

LEPREVOST (F) et WARUSFEL (B), Echelon : origines et perspectives d'un débat transnational, Annuaire Français de Relations Internationales, volume 2, 2001, Ed. Bruylant, p.865-888.

QUANTIN (C), G. COATRIEUX, M. FASSA, V. BRETON, P.de VLIEGER, K. BOURQUARD, N. LIPSZYC, J-Y. BOIRE, C. ROUX, F-A. ALLAERT, Gestion décentralisée des documents médicaux des patients, un système de recherches d'accès aux données.

POIDEVIN (B) et GELLES (V), Internet mobile, les applications iPhone et la LCEN, Expertises décembre 2010, n°353, p. 423-425.

RENUCCI (J-F), Convention EDH et criminalité organisée, Revue de science criminelle 2012 p. 902.

SIMON (J), J. ROBIENSKI, Property, Personality Rights and data protection with regard to biobanks -a layered system in Journal International de la bio-éthique, 2009, vol. 20, n°3.

SOULIER (J-L) et S. SLEE, La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques. Perspective française, Revue internationale de droit comparé, Vol. 54 N°2, Avril-juin 2002, pp 663-676.

STIG (S), Ordinateurs et droit (A propos d'un projet de loi suédois sur les ordinateurs), Revue internationale de droit comparé. Vol. 25 N°1, Janvier-mars 1973. pp. 55-67.

WARUFSEL (B) La sécurité de l'information, une exigence stratégique pour le développement de l'économie européenne », documentaliste/ Science de l'information, volume 28, n° 6, novembre/décembre 1991, p. 239.

WARUFSEL (B), Procédure pénale et technologies de l'information : De la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne, Revue Droit & Défense n° 1, 2002, p.17-22.

WARUFSEL (B), « La sécurité nationale, nouveau concept du droit français », in Les différentes facettes du concept juridique de sécurité – Mélanges en l'honneur de Pierre-André Lecocq, Lille2, décembre 2011, pp. 461-476.

WEILL (P-A), Etat de la législation et tendances de la jurisprudence relative à la protection des données personnelles en droit pénal français, Revue internationale de droit comparé, vol. 39 n° 3, Juillet- septembre 1987, pp 655-675.

ARTICLES DE PRESSE

Naissance d'une communauté Open Source contre la cybercriminalité, *le Journal du Net* publié le 09/12/2011, consulté le 21 décembre 2011.

Sécurité informatique: La menace vient de l'intérieur, Solange Ghernaouti-Hélie, PME *Private Bank*, consulté le 22 décembre 2011.

« Halte aux spams », Journal *Libération* du 10 août 2007, deuxième édition, n°8167

« Internet en Afrique, la fin du désert numérique » journal *Le Monde* du 18/02/2011

« Séminaire régional contre la cybercriminalité au Bénin: La France parfait la formation technique des forces de sécurité africaines », Journal *l'événement précis* du 22/11/11.

« Usurpation d'identité, soyez vigilant », Matmut info # 26, 3e trimestre 2013.

« Le PDG d'ACADOMIA défend le fichage » in Journal *France soir* du 28 mai 2010, article d'Alexandra GONZALEZ.

« La CNIL adresse un sévère avertissement à l'entreprise de soutien scolaire ACADOMIA », Journal Le Monde du Samedi 29 mai 2010, article de Luc Cédelle et Franck Johannès.

« Ecoutes : entre Washington et Berlin, le choc culturel », Journal Les Echos du 4 novembre 2013, article de Dominique MOÏSI, Professeur au King's College de Londres et Conseiller à l'IRFI.

« Angela Merkel, cible économique », Journal Direct Matin du 28 octobre 2013, article de Aurélie DELMAS.

« Le parquet national financier a pris des dossiers au parquet de Paris », E. Fn, Libération du lundi 1er septembre 2014.

COLLOQUES ET CONFERENCES

Actes du VIIIe Congrès de l'Association Française de droit pénal organisé du 28 au 30 novembre 1985 à l'Université de Grenoble, Le droit criminel face aux Technologies nouvelles de la Communication, Agence de l'informatique, Economica, Paris, 1986.

Colloque de l'Institut de Recherche en propriété Intellectuelle HENRI-DESBOIS : « le nouveau droit des marques », Paris juin 1991.

12e Colloque sur l'informatique juridique en Europe, Ljubjana (Slovénie), 2-4 octobre 1995 : Les registres informatisés dans le secteur public (en droit civil, pénal et administratif), Council of Europe, collection Informatique et droit.

Conférence interministérielle de l'OCDE : un monde sans frontière concrétiser le potentiel du commerce électronique 1998, Ottawa 7-9 octobre 1998, Direction de la Science de Technologie et de l'industrie, Comité de Paris, OCDE, 1998.

Protection de la vie privée dans la société de réseaux mondialisée : une conférence internationale de l'OCDE avec le soutien du comité consultatif économique et industriel auprès de l'OCDE, BIAC, collection les documents de travail de l'OCDE, Paris 16-17 février 1998.

Colloque de l'Institut de Recherche en propriété Intellectuelle HENRI-DESBOIS : commerce électronique et propriétés intellectuelles, Paris, novembre 2000.

Colloque organisé le 6 octobre 2000 par l'institut de Recherches Carré de malberg, La convention EUROPOL : l'émergence d'une police européenne ? Collection de l'université Robert Schuman, Presses Universitaires de Strasbourg, 2001.

Colloque de l'IRPI « la propriété intellectuelle en questions, regards croisés européens, Paris, juin 2005.

Colloque sur le mandat d'arrêt européen sous la direction de Marie-Elisabeth Cartier, collection droit de l'Union européenne dirigée par Fabrice PICOD, éditions Bruylant, Bruxelles, 2005.

Colloque du 27 novembre 2003 à l'Université Jean Moulin Lyon 3 sur la Sanction, édition l'harmattan, 2007.

La confiance en droit privé des contrats : actes du colloque, Université de Versailles Saint-Quentin- en –Yvelines, 22 juin 2007, organisé par le laboratoire DANTE avec les contributions de Laurent AYNES, Valérie-Laure BENABOU, Muriel Chagny, Dalloz, 2008.

Actes du colloque du programme de recherche Asphales, ACI-Informatique, Paris 22 et 23 novembre 2007, DE LAMBERTERIE Isabelle, KIRCHER Claude, LACOUR, Stéphanie la sécurité de l'individu numérisé: Réflexions prospectives et internationales, édition L'Harmattan, DL 2008.

Colloque de l'IRPI « contrefaçon sur internet : les enjeux du droit d'auteur sur le web 2.0, Paris, octobre 2008.

Actes de la conférence internationale des 11 et 12 février 2010 sur « Quelles perspectives pour un ministère public européen ? Protéger les intérêts financiers et fondamentaux de l'Union européenne, sous l'égide de la Cour de cassation, Dalloz, Paris, 2010.

Actes de la journée d'étude sur « Juge national, européen, international et droit pénal, le 24 juin 2011, Institut de sciences criminelles et de la justice. Bordeaux : BEAUVAIS P. ; DUBOS O. ; GOGORZA, A. (1976-...) ; MALABAT V., éditions CUJAS.

Colloque sous la direction de Laurent Couton, Pédagogie judiciaire et application des droits communautaire et européen, collection droit de l'Union européenne, éditions Bruylant, 1ère édition, février 2012.

Actes du colloque du 15 juin 2012- Dijon, la contrefaçon de médicaments : les premiers pas d'une réaction normative internationale, sous la direction de Clotilde JOURDAIN-FORTIER et Isabelle MOINR-DUPUIS, Université de Bourgogne- CNRS- Travaux du Centre de Recherche sur le Droit des marchés et des investissements internationaux, Lexisnexis.

ZEROUKI, DJOHEUR, L'espace pénal européen : à la croisée des chemins ? Actes de la journée d'études du 30 mai 2013 à l'Université Jean Monnet Saint-Étienne, Centre de recherches critiques sur le droit. Saint-Étienne, Collection : Les dossiers de la Revue de droit pénal et de criminologie 20, Bruxelles 2013.

WARUSFEL Bertrand, « Les implications juridiques et institutionnelles de la notion de sécurité nationale », intervention au colloque annuel de l'Association française du droit de la sécurité et de la défense (AFDSD), Université de Nice, 27-28 septembre 2013.

FAUVARQUE- COSSON B. et ZOLINSKY C., Colloque du 11 octobre 2013 : le *cloud computing*, l'informatique en nuage, société de législation comparée : Juin 2014.

Colloque international organisé pour le Centre de Recherches Droits et Perspectives du droit-DEMOGUE par les Pr. Gaël CHANTEPIE et DENIS VOINOT, par Mme Juliette SÉNÉCHAL et M. Nicolas DESRUMAUX-RANCHY : Télémédecine : enjeux médicaux et juridiques, 17 octobre 2014, Amphi Cassin (Campus moulins, Lille).

COLLOQUES PROPRES A L'AFRIQUE DE L'OUEST

Le rôle du droit dans le financement du développement et des investissements en Afrique : Actes du séminaire international organisé conjointement par le secrétariat d'Etat au plan des statistiques et de la coopération et l'Université de Bangui du 25 au 28 mai 1988, édité par Rolf KNIEPER, Gabriel NGOUAMENE et Serge PSIMHIS.

Actes du 2ème colloque africain sur la Recherche en Informatique CARI'94, 12-18 octobre 1994, Ouagadougou (Burkina Faso) éditeur scientifique, Joachim ORSTOM, Institut

français de Recherche Scientifique pour le développement en coopération, collection Colloques et séminaires, Paris, 1994.

Actes du Symposium de la CEDEAO sur le Développement (3-5 octobre 2010), sous la direction de Lambert Ngaladjo Bamba, John O. Igué et Kalilou Sylla : sortir du sous-développement : quelles nouvelles pistes pour l'Afrique de l'Ouest ? Aspects historiques, institutions et intégration régionale, préface de Victor J. GBEHO, publié aux éditions L'Harmattan

ETUDES ET RAPPORTS

OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, Paris, 1981.

OECD, Computer-related criminality: Analysis of legal policy in the OECD-area, Report DSTI/ ICCP 84.22 of 18 April 1986, p. 4.

Agence Judiciaire du Trésor, les NTI (Nouvelles Technologies de l'Information) et le droit de la preuve : éléments de réflexion, Publication du service juridique de l'Agence Judiciaire du Trésor, Août 1991.

Guides législatifs pour l'application de la convention des Nations Unies contre la criminalité transnationale organisée et des protocoles s'y rapportant, édition Office des Nations Unies.

G. TURKER, Protection des données et de la vie privée : problèmes et enjeux, OCDE, Politiques d'information, d'informatique et de communications, Paris, 1994.

Rapport de Commission Européenne sur La coopération UE-ACP en 1995, quel ajustement structurel ? Direction générale du Développement, Courrier ACP-UE, Tielt-Belgique, Juin 1996.

OCDE, Le commerce électronique : opportunités et défis pour les gouvernements, groupe d'experts du secteur privé sur le commerce électronique, Paris, 1997.

Lawrence Lessig : étude de la paternité d'une théorie normative du Cyberespace, Décembre 1999, S. DESROCHERS.

Les incidences économiques et sociales du commerce électronique : résultats préliminaires et programme de recherche, Paris, OCDE, 1999.

Etude de droit comparé en matière d'organismes de contrôle pour les interceptions de télécommunications réalisée par Claudine GUERRIER, étude réalisée avec le soutien de la mission de recherche « Droit et Justice », Janvier 2009.

Commerce électronique : engagements existants dans le cadre de l'AGCS pour la fourniture de service en ligne, direction des échanges, comité de changes, OCDE, Paris, 2000.

Protection de la vie privée en ligne : orientations politiques et pratiques de l'OCDE, Paris, 2003.

The interoperability of information systems in the Justice sector, Recommendation Rec. (2003) and explanatory memorandum, legal issues, Council of Europe Publishing, Editions du Conseil de l'Europe, 2004 (adopted by the Committee of the Ministers on 9 September 2003 at the 851st meeting of the Minister's Deputies).

Fabien JOBARD et Niklas SCHULZE-ICKING, Preuves hybrides, L'administration de la preuve pénale sous l'influence des techniques et des technologies (France, Allemagne, Grande-Bretagne), Centre de recherches sociologiques sur le droit et les institutions pénales, N° 96, 2004.

Rapport d'information n° 2623 sur les systèmes de surveillance et d'interception électroniques de M. Arthur PAECHT, déposé à la commission de la défense le 11 octobre 2000.

Understanding the digital divide, *OECD*, Paris, 2001.

Rapport de la Commission au Conseil et au Parlement Européen : Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE).

Bluetooth Security & Hacks, Chair for Communication Security, étude réalisée par Andreas BECKER, étude publiée le 16 août 2007.

Rapport d'information sur la cyber défense, Sénat, session extraordinaire de 2007/2008, Commission des affaires étrangères, de la défense et des forces armées, Roger ROMANI.

Les marchés noirs de la cybercriminalité, Compagnie Européenne d'Intelligence Stratégique, édition juin 2011.

Etude du modèle économique de sites ou services de streaming et de téléchargement direct de contenus illicites: rapport final à l'attention de la Haute autorité pour la diffusion des œuvres et protection des droits sur Internet, 2012, rapport effectué par l'Institut de l'audiovisuel et des télécommunications en Europe (France).

Rapport d'information n° 203 rédigé par le Sénateur Sophie JOISSAINS pour la Commission des affaires européennes : vers un parquet européen, 2012-2013.

The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law Council of Europe contribution to the Commonwealth Working Group on Cybercrime, Data Protection and Cybercrime Division Strasbourg, 27 February 2013.

Dossiers techniques : les virus informatiques espace Menaces, Groupe virus.

Programme mondial sur la sécurité de l'information : politique sur l'utilisation convenable des systèmes d'information et de communication, World Health Organization.

33ème rapport de la CNIL, Rapport d'activité 2012, édition 2013, La documentation Française.

Rapport annuel sur l'activité de la BEI en Afrique, dans les Caraïbes et le Pacifique ainsi que dans les pays et territoires d'outre-mer.

Rapport Annuel d'EUROJUST 2013.

BIGOT (R), CROUTTE (Patricia) Etude réalisée à la demande du Conseil général de l'Economie, de l'industrie, de l'Energie et des Télécommunications (CGEIEYT) et de l'Autorité de Régulation des communications Electroniques et des postes (ARCEP) : La diffusion des technologies de l'information et de la communication dans la société française (novembre 2013), CREDOC, collection des rapports n° 297.

Etude annuelle du Conseil d'Etat 2014, Le numérique et les droits fondamentaux : Documentation française, septembre 2014

LES RAPPORTS GOUVERNEMENTAUX

- Rapport au premier ministre D. De VILLEPIN rédigé par P. LASBORDES sur la sécurité des systèmes d'information, un enjeu majeur pour la France, 13 janvier 2006, publié à la Documentation Française, collection les Rapports officiels, 2006.

- Le risque numérique : en prendre conscience pour mieux le maîtriser, Rapport n° 721 (2012-2013) de MM. Bruno SIDO, sénateur et Jean-Yves LE DÉAUT, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 3 juillet 2013.

- Rapport du Conseil d'Etat : « Internet et les réseaux numériques », juillet 1998, collection La documentation française, collection Etudes du Conseil d'Etat, Paris, 1998.
- Rapport d'information sur la mondialisation, rapport de l'Assemblée Nationale n°1963, déposé par la Commission des affaires étrangères et présenté par M. Roland Blum, sous la 11e législature, Paris : Assemblée nationale, publié le 24 novembre.1999, p.83-99.

- Rapport d'information déposé par la Délégation de l'Assemblée Nationale pour l'Union européenne et présenté par le député Alain BARRAU, Rapport n° 1838 « Vers un espace judiciaire européen, les enjeux du Conseil européen extraordinaire de Tampere, 15-16 octobre 1999.

- Les documents de travail du sénat, série de législation comparée : l'interconnexion des fichiers administratifs, juin 1999 N° LC 59.

- Rapport d'information n°449 (2007-2008) sur la Cyber-défense : un enjeu de sécurité national, de M. Roger ROMANI fait au nom de la commission des affaires étrangères déposé le 8 juillet 2008.

- Rapport d'information du Sénat n°681, *au nom de la commission des affaires étrangères, de la défense et des forces armées sur la* cyber-défense, par M. Jean-Marie BOCKEL, Enregistré à la Présidence du Sénat le 18 juillet 2012.

- Rapport 2012 sur l'économie de l'information : l'industrie du logiciel dans les pays en développement, Conférence des Nations Unies sur le Commerce et le Développement (CNUCED).

- Rapport d´information au Sénat n° 477 fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, par André GATTOLIN, Dominique BAILLY, Pierre BERNARD-REYMOND et Mme Colette MÉLOT, Enregistré à la Présidence du Sénat le 17 avril 2014.

- Rapport sur la cybercriminalité *« Protéger les internautes »*, sous la direction de Marc ROBERT, présenté par le Groupe de travail interministériel, Juillet 2014.

PERIODIQUES ET REVUES

Business Intelligent Journal

EHIMEN O, BOLA A., *Cybercrime in Nigeria*, article paru dans le Business Intelligent Journal, Janvier 2010, volume 3 n°1.

Cahiers de la sécurité et de la Justice

CHARPENEL (Y), Cybercrime : Jurisprudence de la Cour de cassation, *Cahiers de la sécurité* n°6, oct. 2008, Institut National des Hautes Etudes de Sécurité.

WARUSFEL B., « Renseignement et état de droit », Cahiers de la sécurité, n° 13, INHESJ, juillet-septembre 2010, pp. 114-121.

WARUSFEL B., « L'entrée de l'Union européenne dans les champs de la défense et de la sécurité », Cahiers de la sécurité et de la justice, 1er semestre 2014, n° 27-28, pp. 189-198.

Le courrier, le magazine de la coopération au développement ACP-UE 2003

LOOTS Michel, *L'accès à l'information, un droit* fondamental, in Le courrier ACP-UE n° 201 de Novembre-décembre 2003, p. 32.

WAGNER Christophe**,** Où en sont les négociations sur les Accords de Partenariat économique entre les ACP et la CE, in Le courrier ACP-UE n° 201 de Novembre-décembre 2003, P. 21

International Journal of Cybercrime 2010-2013

JASON WARNER, "Understanding Cyber-crime in Ghana: A view from Below, in International Journal of Cyber Criminology, July 2011, Vol. p. 736-749.

Revue Communication Commerce électronique

Anne DEBET, *Précisions européennes sur les fondements légitimes des traitements de données personnelles,* Communication Commerce électronique n°3, Mars 2012, comm. 30.

L. DUONG GODEFROY, Vers une gouvernance juridique transnationale d'Internet, Communication Commerce électronique n°5, Mai 2014, étude 10.

Revue Droit et Défense

WARUSFEL B., les notions de défense et de sécurité en droit français, Revue Droit & Défense, n° 94/4, octobre 1994, pp. 11-20.

WARUSFEL B., *Procédure pénale et technologies de l'information : de la Convention sur la cybercriminalité à la Loi sur la sécurité quotidienne,* Revue Droit et Défense n° 2002/1, pp 17-22.

Revue Générale de Droit médical

- MATHIEU Daniel, LEUZZI-JOUCHART Coralie. In Le dossier médical : enjeux et perspectives. Acte de la journée d'études organisée le 18 avril 2014 à Lille par Lille 2 et le CHRU de LILLE. Revue Générale de droit médical, n° 53. décembre 2014. p. 19
- TILMAN, Laora, *La délicate question de la propriété des données de santé*, In Le dossier médical : enjeux et perspectives. Acte de la journée d'études organisée le 18 avril 2014 à Lille par Lille 2 et le CHRU de LILLE. Revue Générale de droit médical. n° 53. décembre 2014. p. 49.

Revue Droit Pénal

ROUMIER W., *Création d'un parquet européen : « carton jaune » à la Commission européenne,* Droit pénal n° 12, Décembre 2013, alerte 61.

Revue Europe

- *Vers l'institution d'un Parquet européen*, Europe n°7, juillet 2011, alerte 53.

- LABAYLE H., *Within you, without you : l'opt-out britannique en matière d'entraide répressive*, Europe n° 2, Février 2013, étude.

- *Proposition d'instauration d'un Parquet européen et de renforcement des garanties procédurales de l'Office de Lutte Anti-Fraude (OLAF)*, Europe n°8, Août 2013, alerte 47

- SIMON D., *La révolution du juge de l'Union : les premiers pas de la cybercitoyenneté*, Europe n°7, juillet 2014, étude 6.

Revue de la gendarmerie nationale

- Revue de la gendarmerie nationale, Revue trimestrielle décembre 2013 n°248 : les défis du cyberespace.

Revue HERMES

- PRZYSWA E. et GUARNIERI F., Viagra 2.0 et contrefaçon, HERMES, n°69, 2014, p. 183-185.

Revue LAENNEC

- BRODIN Marc, « Informatisation et confidentialité des données médicales », *Laennec*, 2007/1 Tome 55, p. 12-22.

Revue Française d'administration publique

- J. CHEVALIER, L'Etat régulateur, Revue française d'administration publique, 2004/3 no111, p. 473-482.

- L. CLUZEL, METAYER, Les télé services publics face au droit à la confidentialité des données, Revue Française d'administration publique 2013/2, n° 146, p405-418.

Revue internationale de l'intelligence économique

- M. QUEMENER, Le Procureur financier, architecte de la lutte contre la corruption et la délinquance économique et financière, in *Revue internationale d'intelligence économique*, 2014/1 (Vol. 6), p.27-35.

Revue Santé Publique

- Picard S. *et al.*, « Les aspects juridiques et éthiques de la protection des données issues du dossier médical informatisé et utilisées en épidémiologie : un point de la situation », *Santé Publique*, 2006/1 Vol. 18, p. 107-117.

Revue Sécurité et Stratégie

- WARUSFEL B., « La protection des réseaux numériques en tant qu'infrastructures vitales », Sécurité & Stratégie, n° 4, novembre 2010, pp. 31-39

Revue Les tribunes de la santé

- J. BERANGER, H. SERVY, P. LE COZ, Télémédecine sous X, pourquoi prolonger cette protection individuelle historique? Les Tribunes de la santé, n° 35, 2012/2, éditions Presses de Sciences politiques.
- E. PRZYSWA *et* F. GUARNIERI, Contrefaçon de médicaments sur Internet : prévenir une menace réelle sur la santé publique**,** Les Tribunes de la santé n° 40 2013/3, p. 77-83.

REPERTOIRES DE TEXTES DE JURISPRUDENCE

JURISPRUDENCE CITEE

Conseil constitutionnel

Conseil Constitutionnel décision n° 2006-540 décision parue au J.O. du 3 août 2006, p. 11541, n°63 -65.

Conseil Constitutionnel décision n° 2013-314 QPC du 14 juin 2013 publiée au JORF n°0138 du 16 juin 2013 page 10024 texte n° 31.

Cour de cassation

Chambre criminelle

Chambre criminelle de la Cour de Cassation, 22 septembre 2004, n° du pourvoi : 04-80285, Bulletin criminel 2004 n° 218 p. 777

Chambre Criminelle de la Cour de cassation, 5 Janvier 2005, n° 04-82.524, Bulletin Criminel n° 176.

Chambre criminelle de la Cour de cassation, 14 mars 2006, n° de pourvoi 05-83423, Bulletin criminel 2006, n ° 69 p. 267.

Chambre criminelle de la Cour de cassation, 7 févr. 2007, n° 06-87.753, FS-P+F, Cyril C. : Juris-Data n° 2007-037763.

Chambre Criminelle de la Cour de cassation, 3 octobre 2007, Bulletin criminel n° 236.

Chambre Criminelle de la Cour de cassation, 9 septembre 2008, n° de pourvoi 07-8728, non publié au Bulletin.

Chambre criminelle de la Cour de cassation, 27 octobre 2009, n° 09-82.346, bulletin n° 177.

Chambre criminelle de la Cour de cassation, 14 décembre 2010, n° de pourvoi 10-80088, non publié au Bulletin.

Chambre criminelle de la Cour de cassation, 22 novembre 2011, n° de pourvoir 11-84308, publié au Bulletin criminel n° 234.

Chambre criminelle de la Cour de cassation, 19 mars 2014, arrêt n° 1193, N/ R 12-87.416 FP-P+B+R+I, numéro de pourvoi 12.87-116, arrêt de cassation partielle avec renvoi

Chambre civile

Première chambre civile de la Cour de cassation, 9 décembre 2003, publié au bulletin 2003, I, n° 245, p. 195.

Chambre commerciale

Chambre commerciale de la Cour de Cassation, 23 novembre 2010, n° de pourvoi: 07-19543, non publié au Bulletin.

Cour d'appel

Cour d'appel de Paris, 9e chambre, 18 novembre 1992, JCP éd. Entreprise, 1994, I, n° 359.

Cour d'Appel de Paris, 4e ch., sect. A, 6 juin 2007, Sociétés Google Inc. et Google France c/ Axa et autres.

Cour d'appel de Paris, 14ème Chambre, section A Arrêt du 4 janvier 2006

Cour d'appel de Paris Pôle 1 - Chambre 3, arrêt du 28 juin 2011, RG n° 11/10112

Cour d'Appel de Paris pôle 5, chambre 12, arrêt du 24 octobre 2012

Cour d'Appel de Paris pôle 5, chambre 1, arrêt du 02 décembre 2014, TF1 et autres / Dailymotion.

Tribunal de Grande Instance

16ème Chambre correctionnelle du Tribunal de Grande Instance de Paris en date du 23 octobre 1992

Ordonnance des référés du TGI de Paris, 22 mai 2000.

Ordonnance du Tribunal de Grande Instance de Nanterre 1ère chambre, Section A Jugement du 24 mai 2000.

Tribunal Correctionnel

Tribunal correctionnel de Clermont Ferrand, 21 juin 2010

Jurisprudence américaine

Cour Suprême, International Shoe Co contre Washington, 3 déc. 1945, 326 US.310.

Jurisprudence belge

Chambre correctionnelle de Bruxelles :

Corr. Bruxelles, 6 janvier 2004

Chambre correctionnelle de Dendermonde :

Corr. Dendermonde, 7 juin 2004

Jurisprudence de la CEDH

CEDH, arrêt Klass et autres c. Allemagne du 6 septembre 1978, série A n° 28

CEDH, arrêt Malone c. Royaume-Uni du 2 août 1984, série A n° 82

Cour Européenne des droits de l'Homme rendue à la suite de la Requête n° 20605/92, Halford contre Royaume Uni, 25 juin 1997.

CEDH, 10 janvier 2013, 5è section, requête 40397/12, Neij et Sunde Kolmisoppi c. Suède.

CEDH, *arrêt Huvig c. France* du 24 avril 1990, série A n° 176-B

CEDH, *arrêt Kruslin c. France* du 24 avril 1990, série A n° 176-A.

CEDH, NIEMIETZ *c. Allemagne* du 16 décembre 1992, série A n° 251-B.

CEDH, 5ème section ,18 septembre 2014, affaire François X.

La CJUE

CJUE, Procédure pénale c. Guerrino Casati, 11 novembre 1981, aff. 203/80 au Recueil la jurisprudence de la CJUE 1981, 02595.

CJUE, Fiona Shevill c. Press Alliance, 7 mars 1995, aff. C-68/93 au Recueil la jurisprudence de la CJUE 1995, partie I-00415.

CJUE, eDate Advertising c. Martinez, 25 octobre 2011, affaire C-509/09 et C- 161/10 publiée au Recueil de la jurisprudence de la CJUE 2011, partie I- 10269.

CJUE, 24 nov. 2011, aff. Jtes C-468/10 et C-469/10, ASNEF, FECEMD c/ Administracion del Estado.

CJUE, Football Dataco Ltd c. Sportradar GmbH, du 18 octobre 2012, affaire C-173/11.

CJUE, Football Dataco e. a. 1er mars 2012, aff. C-604/10, non encore publié au Recueil.

CJUE, The British Horseracing Board et autres, 9 novembre 2004, aff. C-203/02, Recueil la jurisprudence de la CJUE, partie I-10415, points 45 46 51 et 67.

CJUE, Wintersteiger, 19 avril 2012, aff. C-523/10, non encore publié au Recueil, point 25.

JURISPRUDENCE AFRICAINE

Jurisprudence ivoirienne

Tribunal de Commerce d'Abidjan, 6 juin 2014, Association SUKYO MAHIKARI CÔTE D'IVOIRE contre BICICI.

Jurisprudence du Sénégal

Tribunal des Flagrants délits, jugement n° 3375/2009 du 29 juillet 2009, Ministère Public Ndèye Astou Kaloga contre Mamadou Fam.

Tribunal Régional Hors Classe de Dakar, Ministère Public et Alioune Samb ès qualité de DG de la Société PNEU MECA contre Aboulaye BA, Jugement n°4241/09 du 18 septembre 2009.

Tribunal Hors Classe de Dakar, Jugement du 21 janvier 2010, Ministère Public contre Fulgence BAHI.

Cour d'appel de Dakar

Chambre correctionnelle de la Cour d'appel de Dakar, Ministère public contre Bocar THIAM- Crédit Lyonnais Sénégal, arrêt n°555 du 24 juillet 2009.

RECUEILS DE JURISPRUDENCES

J. PRADEL et A. VARINARD, Les Grands arrêts du droit criminel, tome1 éd. DALLOZ

J. PRADEL et A. VARINARD, Les Grands arrêts du droit criminel, tome 2, le procès, la sanction, 2ème édition DALLOZ

Internet : la Jurisprudence de la Cour Européenne des Droits de l'Homme, Division de la Recherche, 2011.

A.CASSESE, D. SCALIA, V. THALMANN, Les Grands arrêts de droit international pénal, Dalloz 2010.

Répertoire communautaire, Dalloz septembre 2003.

E. ZOLLER, les Grands arrêts de la Cour Suprême des Etats-Unis.

TEXTES DE LOIS

Textes internationaux

Convention de lutte contre la cybercriminalité du 23 novembre 2001, série des Traités.

International Standards on the Protection of Personal Data and Privacy" the Madrid Resolution, 5 novembre 2009.

Résolution de l'ONU 45/95 du14 décembre 1990 adoptant les principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel et sur les Principes de Paris concernant le statut et le fonctionnement des institutions nationales pour la protection et la promotion des droits de l'homme, adoptés par Résolution 48/134 de l'Assemblée Générale de l'ONU le 20 décembre 1993

Textes de l'Union Africaine

Convention de l'Union Africaine sur la cyber-sécurité et la protection des données à caractère personnel, adoptée par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014.

Charte Africaine des Droits de l'Homme et des Peuples, adoptée par la dix-huitième Conférence des Chefs d'état et de Gouvernement le 27 Juin 1981 à Nairobi au Kenya et entrée en vigueur le 27 octobre 1986.

Textes de la CEDEAO

- Traité CEDEAO révisé, Communauté Economique des Etats de l'Afrique de l'Ouest, Presses de l'UB (Lomé- Togo) 1995.

- Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

- Acte additionnel A/SA 1/01/10 du 16 février 2010 de la CEDEAO relatif à la protection des données à caractère personnel

- Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques

- Acte additionnel A/SA 1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre règlementaire du secteur des technologies de l'information et de la communication (TIC)

Textes de l'UEMOA

-Traité du 10 janvier 1994 créant l'Union Économique et Monétaire Ouest Africaine, révisé le 29 janvier 2003

- Règlement 15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement

-Directive relative à la lutte contre le blanchiment de capitaux dans les Etats membres de l'UEMOA : Directive n°07/2002/CM/UEMOA du 19 septembre 2002.

- Loi uniforme n° 2004-09 du 6 février 2004 relative à la lutte contre le blanchiment des capitaux dans les Etats membres de l'UEMOA (JORS, n° 6154 du 27 mars 2004, p. 505)

- La directive 01/2006/CM/UEMOA relative à l'harmonisation des politiques de contrôle et de régulation du secteur des télécommunications :

- La directive n°02/2006/CM/UEMOA relative à l'harmonisation des régimes applicables aux opérateurs de réseaux et fournisseurs de services

- La Directive n°03/2006/CM/UEMOA relative à l'interconnexion des réseaux et services de télécommunications

- La Directive n°04/2006/CM/UEMOA relative au service universel et aux obligations de performance du réseau

- La Directive n°05/2006/CM/UEMOA relative à l'harmonisation de la tarification des services de télécommunications

- La Directive n°06/2006/CM/UEMOA organisant le cadre général de coopération entre les autorités nationales de régularisation en matière de télécommunications

Textes de l'OHADA

Acte uniforme relatif au droit des sociétés commerciales et du groupement d'intérêt économique en date du 30 janvier 2014 (entré en vigueur le 05 mai 2014).

Recommandations

Recommandation n° R (95)13 adoptée par le Comité des Ministres du Conseil de l'Europe le 11 septembre 1995 et exposé des motifs : Problèmes de procédure pénale liés à la technologie de l'information, éditions du Conseil de l'Europe, Strasbourg, 1996.

Recommandation Rec. (2000)19 et exposé des motifs adoptée par le Comité des Ministres du Conseil de l'Europe le 6 octobre 2000 sur Rôle du Ministère public dans le système de Justice pénale, Références juridiques, Strasbourg, 2001.

Textes nationaux

Bénin

Loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin disponible sous le lien : http://www.afapdp.org/wp-content/uploads/2012/01/Bénin-LOI-SUR-PROTECTION-DES-DONNEES-A-CARACTERE-PERSONNEL-20092.pdf

Burkina Faso

Loi n°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel au Journal Officiel n° 26 du 24 juin 2004.

Côte-d'Ivoire

Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel publiée au JORCI du 08 août 2013 p 474- 482.

Loi n° 2013-451 relative à la lutte contre la cybercriminalité publiée au Journal Officiel de la République de Côte-d'Ivoire édition complémentaire n° 32 du lundi 12 août 2013, p. 450-457.

Loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques publiée au JORCI du 12 septembre 2013 p 583-588.

Ordonnance n° 2012-293 du 21 mars 2012 publiée au Journal Officiel de la République de Côte-d'Ivoire n°8, 54ème année du 14 août 2012, p. 137-163

Ghana

- Data Protection Act, 2012, act 843.
- Electronic Transaction Act, act 772.

Nigeria

- Nigerian Communications Commission Draft Lawful Interception of Communications Regulations, Made Pursuant to the Provisions of the Nigerian Communications Act 2003.
- Economic and Financial Crimes Commission Act, 2004.
- Computer Security and Critical Information Infrastructure Protection Bill, 2005
- Advance Fee Fraud and other Fraud Related Offences Act, 2006.
- Nigerian Communications Act 2003, Licensing Regulations 2013.

Sénégal

- Loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel, publiée au Journal Officiel du Sénégal n° 6406 du Samedi 3 mai 2008.

- Loi n° 2011-01 du 24 février 2011 portant Code des Télécommunications publiée au Journal official de la République du Sénégal numéro 6576 du lundi 14 mars 2011.

MELANGES

Mélanges Raynaud.

Mélanges offerts à PRADEL

THESES ET MEMOIRES

MEMOIRES

AVILLAT A., Certification et signature électronique : les clés de l'internet de confiance, Université Paris 2 Assas, Mémoire de DESS déposé le 04 juin 2002.

BRASIER A., Le commerce électronique : une opportunité pour l'Afrique, DESS Gestion Européenne et Internationale, Université Panthéon-Sorbonne, Paris, 2003.

BRISSET-GIUSTINIANI A., Aspects juridiques de l'émergence d'une sécurité européenne des réseaux et des systèmes d'information, mémoire dirigé par Philippe WOLF, Paris La Sorbonne, 2003- 2004.

COIRATON M., La procédure de résolution des conflits entre marques et noms de domaine mise en place par l'ICANN, sous la direction de Christophe CARON, Paris, 2000- 2001.

CONDE T., La responsabilité des hébergeurs, mémoire de DESS droit du Multimédia et de l'informatique sous la direction de Maître LEDIEU, Université Paris Panthéon-Assas, 2003-2004.

DE CARLO A., Le référencement payant face au droit des marques, mémoire sous la direction de Bertrand WARUSFEL, Université Panthéon-Assas Paris, septembre 2010.

De LONGEAUX A., L'ICANN est-il un organisme de gouvernance légitime des noms de domaine ? DESS Propriété intellectuelle 2003/2004.

JANOT P., le Réseau ECHELON, outil d'intelligence économique, mémoire de DEA sous la direction de Serge SUR, 2000/2001.

LACROIX E., L'utilisation de l'internet dans l'enseignement supérieur en Afrique Francophone : le cas du Burkina Faso, Université de Panthéon - Assas, Paris, 2003.

NGANGA J-L., La régionalisation des échanges commerciaux interafricains (dans la CEDEAO, le COMESA et la CEEAC) sous la direction de M. Olivier AUDEOUD, Université de Nanterre, Paris X, Septembre 2004.

RAULT R., la mise en ligne des données de santé : le cas du dossier médical personnel, mémoire dirigé par Agathe LEPAGE, Professeur à l'Université de Paris II, 2004-2005.

REKIK, M., le juge du contrat électronique international, Mémoire sous la direction de M. ELLOUMI, Université de Sfax, décembre 2013.

RICHARD J., Le droit face aux divulgations des failles de sécurité informatique, sous la direction de Bertrand WARUSFEL, Professeur à l'Université de Paris Descartes et Lille II, 2010-2011.

TIXIER M., Les règles de conflits de droit international privé français et allemand appliquées aux cybers délits, mémoire sous la direction de Xavier TRAIN, UFR des sciences juridiques de Nanterre.

THESES

ALBRIEUX S., La responsabilité du Fournisseur de Moyens de Communication électronique, Université Panthéon-Assas, Paris II, Thèse de Droit privé, 2004.

ARNAL J., Cybercriminalité et droit pénal, Université de Montpellier I, Thèse de droit privé, 2008.

ARNAUD F., les politiques de partenariat de la Banque Européenne d'Investissement, Université de Lille III, 2006.

BACHOUE PEDROUZO G., Le contrôle juridictionnel de la coopération intergouvernementale dans l'Union européenne, contribution au processus de juridictionnalisation de l'Union, Université de Pau et des Pays de l'Adour, 2012.

BERTE S., L'intention en droit pénal, Université de Paris 10, Thèse de droit, 2005

BOURGEOS C., l'anonymat et les technologies de l'information, Université de Paris Descartes, 2003.

CASILE J-F., Le code pénal à l'épreuve de la délinquance informatique, Thèse de droit et de Science politique, Presses Universitaires d'Aix-Marseille, 2002.

CHAMPY G., La fraude informatique, thèse de droit, Aix-Marseille III, 1990.

CHAWKI M., Combattre la cybercriminalité, Université de Lyon 3, Texte remanié de Thèse de doctorat, Lyon 3, 2006.

CHAWKI M., le droit pénal à l'épreuve de la cybercriminalité, Université de Lyon 3, Texte imprimé étude comparative de la politique criminelle face aux N.T.I.C., 2006.

CHEVALLIER-GOVERS C., De la coopération à l'intégration policière dans l'Union Européenne, thèse de droit public, Université de Panthéon-Assas, Paris II, sous la direction de Mario BETTATI, 20 mai 1998.

CHILSTEIN D., Droit pénal international et lois de police, essai sur l'application dans l'espace du droit pénal accessoire, Université de Panthéon –Assas, thèse soutenue publiquement en 2001 et publiée chez Dalloz, Nouvelle Bibliothèque de thèses, 2003

CONCHON E., Définition et mise en œuvre d'une solution d'émulation de réseaux sans fil, Institut Polytechnique de Toulouse, soutenue en octobre 2006.

DEMARCHI Jean-Raphaël, Les preuves scientifiques et le procès pénal, thèse de droit soutenue le 30 septembre 2010, Université de Nice-Sophia Antipolis, sous la direction de Mme Coralie AMBROISE - CASTEROT.

DEVERGRANNE, La propriété informatique, Université de Panthéon Assas, sous la direction de Jérôme HUET, Paris, 2007.

DIALLO Amadou, la dimension politique du partenariat UE/ACP depuis l'accord de Cotonou : les défis, enjeux et perspectives, thèse de droit sous la direction de Albert BOURGI, Université de Reims Champagne Ardenne, 2008.

EL CHAER N., la criminalité informatique devant la justice pénale, Université de Poitiers, thèse sous la direction de Jean PRADEL, 2003.

FAGEAUD P., la preuve informatique en droit français : les aspects juridiques de l'inforensique, ANRT, Université de Limoges, 2007.

GASSIN R., La protection pénale d'une nouvelle universalité de fait en droit français : le système de traitement automatisé de données, 1988.

GINDRE E., L'émergence d'un droit pénal de l'Union Européenne, Université de Paris I-Panthéon - Sorbonne, thèse soutenue el 10 décembre 2008, publiée à LGDJ, Collection des Thèses, DL 2009.

GOUROUZA Z., Le traitement de la criminalité économique et financière dans l'espace UEMOA. Etude comparative AVE, 2008.

GUEDJE L., Essai sur la répression des infractions sur les biens en droit d'Afrique francophone : cas du Bénin, Thèse soutenue en 2006 à l'Université de Perpignan.

ICKOWICZ J., le droit face à la dématérialisation de l'œuvre d'art : une analyse juridique de l'art contemporain.

JABER A., les Infractions commises sur Internet, édition L'Harmattan.
LACROIX E., Internet et la communication locale : cas de l'image des villes d'Afrique subsaharienne, thèse en sciences de l'information et de la communication sous la direction de Francis BALLE, Université Panthéon-Assas, Paris,

LAJUS-THIZON E., l'abus en droit pénal, préface de Philippe CONTE, Nouvelle Bibliothèque de Thèses, Dalloz, 2011.

LE MONNIER DE GOUVILLE P., Le juge des libertés et de la détention, thèse soutenue le 23 juin 2011 à l'Université de Paris Panthéon-Assas II, sous la direction de Monsieur REBUT.

LO Mouhamadou, L'administration électronique et le droit public, Thèse de droit public, Université de Paris 1, 2004.

MATTATIA F., la protection des données à caractère personnelles face aux usages illicites, déloyaux et frauduleux, 2010.

MEIER MARSELLA C., L'effectivité du processus répressif dans le traitement de la cybercriminalité (enquête sur le système judiciaire français), édition CUJAS.

MIGNARD J-P., Cybercriminalité et cyber-répression : entre désordre et harmonisation mondiale, édition CUJAS, 2004.

NGUIMBI A-C., La réorientation des relations commerciales UE-ACP du fait de la convention de Cotonou, thèse dirigée par Jean-Claude GAUTRON, Université de Montesquieu, Bordeaux IV, présentée et soutenue le 12 février 2009.

PRAO YAO N'GROUMA SERAPHIN, La dimension monétaire du développement, une application à deux pays de l'UEMOA : La Côte-d'Ivoire et le Sénégal, 2009.

RAOUH D., Contribution à la recherche sur l'identification, la typologie, la problématique et les méthodologies correctives des erreurs en matière de risques informatiques : application au problème de l'assurance, Université de Paris 2, 12 juillet 1990 sous la direction de M. J. DONIO.

RODRIGUE L., Les aspects juridiques de la régulation européenne des réseaux, collection Droit administratif sous la direction de Jean-Bernard AUBY, éditions BRUTLANT, Bruxelles 2012.

VERGUCHT P., La répression des délits informatiques dans une perspective internationale, 1996, Montpellier.

RESSOURCES ELECTRONIQUES

Un choc inévitable ? Mohamed CHAWKI and Martin FORRAT, consulté en ligne sur http://hebdo.ahram.org.eg/arab/ahram/2004/4/7/echa0.htm consulté le 21 décembre 2011

« Piratage d'Areva: des hackers complotistes ou des espions industriels? » Consulté en ligne sur http://www.slate.fr/story/45521/espionnage-areva-complot-hacker-stuxnet

Alain François LOUKOU, « Les mutations dans le secteur des télécommunications en Côte d'Ivoire et leurs implications », Revue française des sciences de l'information et de la communication [En ligne], 3 | 2013, mis en ligne le 30 juillet 2013, consulté le 28 octobre 2014.

PAGES ET SITES INTERNET

http://www.belgium.be/fr/justice/organisation/cours/cour_de_cassation/
http://www.cairninfo.org
http://www.cnil.fr
http://www.cnpd.public.lu
http://www.interpol.int

http://content.met.police.uk/Home

http://www.echr.coe.int , consultée le 16 décembre 2011.

http://www.enisa.europa.eu , consultée le 26 janvier 2012

http://www.datenschutz.de

http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

http://www.gesetze-im-internet.de

http://www.justice.gouv.fr/

http://www.lamyline.fr

http://www.legalis.net

http://www.legifrance.gouv.fr

http://www.lexisnexis.fr

http://www.societesdelinformation.net

http://www.oecd.org

http://www.parliament.uk

http://www.persee.org

http://www.securite-informatique.gouv.fr

http://www.who.int

http://www.who.int/goe/publications/ehealth_series_vol4/en/

http://www.who.int/goe/publications/ehealth_series_vol5/en/index.html

ANNEXES

Annexe 1 : Entretien en anglais avec Dr Joan DZENOWAGIS de l'OMS

Entretien avec Dr Joan DZENOWAGIS de l'OMS

Anmonka TANO-BIAN:

Good Morning Dr Joan Dzenowagis,

Thank you for your email.

I want to give you more information about my research.
My general topic is the cybercrime sanction. I compare the European Union system and the West Africa System.

I deal with hacking, phreaking, phishing and all fields, which need the information System. I threat the security of data:

In this way, the entire domains, which use the information system, are concerned. That's why some fields such as financial, money laundering, data protection especially individual data health are included in my work.
I would like to know if there are laws or standards written by the World Health Organization (WHO), in order to protect the data.

For example, we have the electronic medical records. I'm looking for information about such kind of exchangeable files through hospital.

One of my concerns is: "Are there rules to protect data in order to avoid their misappropriation or embezzlement?

And, if a data thief occurs, what sanctions can be applied?
It's my pleasure to have had this exchange with you and I would be very happy to continue discussing directly with you on these matters.

Thank you and best regards.

Réponses de Dr DZENOWAGIS de l'OMS

Several comments for you:

1. **WHO does not create laws or regulations**, as this is the function of governments? Most governments have laws and regulations that protect personal AND health information. This protection is sometimes found under HEALTH laws, or under NATIONAL INFORMATION policies, or both.

2. **EHRs and EMRs are not usually categorized separately from other health information/data.** Although there are specific risks due to the health information being

in digital form, nevertheless it is still concerning health information about citizens, which is usually covered under existing laws, and extended to the electronic space.

3. Having said that, there are now moves by some governments to **reinforce or create new legislation** that protects a citizen's information that CAN BE USED for health – see for example the draft regulation in the European Union that covers data privacy (see link below). This is controversial and is likely to affect medical research, consent for participation in research, and other things.

4. One of WHO's functions is **to provide "norms and standards" in the area of public health**. Unfortunately we do not, at this time, have norms and standards for this area. At some point we will need to address this. Meantime, below please see a link to 3 reports we have on eHealth (legal frameworks, safety and security, and patient information).

5. You will note that in 2005, resolution WHA58.28 urges Member States to

"…***Consider long-term strategic plans for the development and implementation of eHealth services including patient information systems. It calls on governments to form national eHealth bodies to provide guidance in policy and strategy, data security, legal and ethical issues, interoperability, cultural and linguistic issues, infrastructure, funding, as well as monitoring and evaluation. WHO recommends that Member States establish a national-level body for eHealth, supported by the ministry of health, as an instrument for implementing the WHA eHealth resolution. The body should include a division responsible for the governance of eHealth data interoperability standards and patient data privacy and security." (from GOe report on Management of Patient Information)***

http://www.who.int/goe/publications/ehealth_series_vol4/en/ Safety and security on the Internet (documents extrêmement important cf. p 12 et suivantes).

http://www.who.int/goe/publications/ehealth_series_vol5/en/index.html Legal frameworks for eHealth

http://www.who.int/goe/publications/ehealth_series_vol6/en/index.html Management of patient information

http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Article 29 Working party of the proposed EU Data Protection regulation.

I hope this is useful as a starting point. If you would like to discuss by phone, please feel free to send me a note and we can fix a time to talk.

Annexe 2 : Convention de Budapest de Lutte contre la cybercriminalité en Europe du 23 Novembre 2001

Série des Traités n° 185

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits

dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité

dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit:

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

c l'expression «fournisseur de services» désigne:

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par

l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution

ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

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

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

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

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

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

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

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

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a sur un pouvoir de représentation de la personne morale;

b sur une autorité pour prendre des décisions au nom de la personne morale;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale

peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;

b à toutes les autres infractions pénales commises au moyen d'un système informatique; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises

aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au

maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b réaliser et conserver une copie de ces données informatiques;

c préserver l'intégrité des données informatiques stockées pertinentes;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations

raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un

quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un

quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:

a sur son territoire; ou

b à bord d'un navire battant pavillon de cette Partie; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide

en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie

requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b Les autorités centrales communiquent directement les unes avec les autres;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être

directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:

a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser:

a l'autorité qui demande la conservation;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e la nécessité de la mesure de conservation; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la

Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

a apport de conseils techniques;

b conservation des données, conformément aux articles 29 et 30;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une

période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

– de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24);

– de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30);

– du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en œuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter:

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

a toute signature;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;

e tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

Annexe 3 : Convention de l'Union Africaine sur la cyber sécurité et la protection des données à caractère personnel

AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE
UNIÃO AFRICANA

P.O. Box: 3243, Addis Ababa, Ethiopia, Tel.: +251-115 18 24 02 Fax: +251-115 18 24 50
Email: dinfrastructure@africa-union.org / yankeyka@africa-union.org / YedalyM@africa-union.org

LC12490

CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SECURITE ET LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

[AUCyC]

PROJET DE CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SECURITE ET LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

PREAMBULE

Les États membres de l'Union africaine :

Guidés par l'Acte Constitutif de l'Union africaine adopté en 2000;

Considérant que la présente Convention portant adoption d'un cadre juridique **sur la cyber sécurité** et la protection des données à caractère personnel prend en charge les engagements actuels des États membres de l'Union Africaine aux plans sous régional, régional et international en vue de l'édification de la Société de l'Information ;

Rappelant qu'elle vise à la fois à définir les objectifs et les grandes orientations de la société de l'Information en Afrique et à renforcer les législations actuelles des États membres et des Communautés Économiques Régionales (CER) en matière de Technologies de l'Information et de la Communication.

Réaffirmant l'attachement des États membres aux libertés fondamentales et aux droits de l'homme et des peuples contenus dans les déclarations, conventions et autres instruments adoptés dans le cadre de l'Union Africaine et de l'Organisation des Nations Unies ;

Considérant que la mise en place d'un cadre normatif sur la cyber sécurité et la protection des données à caractère personnel tient compte des exigences de respect des droits des citoyens, garantis en vertu des textes fondamentaux de droit interne et protégés par les Conventions et Traités internationaux relatifs aux droit de l'Homme particulièrement la Charte africaine des droits de l'Homme et des Peuples ;

Convaincus de la nécessité de mobiliser l'ensemble des acteurs publics et privés (États, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.) en faveur de la cybersécurité.

Réitérant les principes de l'Initiative Africaine de la Société de l'Information (AISI) et du Plan d'Action Régional Africain pour l'Économie du Savoir (PARAES) ;

Conscients qu'elle est destinée à régir un domaine technologique particulièrement évolutif et en vue répondre aux attentes exigeantes des nombreux acteurs aux intérêts souvent divergents, **la présente convention** détermine les règles de sécurité essentielles à la mise en place d'un espace

numérique de confiance pour les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité ;

Ayant à l'esprit que les principaux défis au développement du commerce électronique en Afrique sont liés à des problèmes de sécurité dont notamment :

- les insuffisances qui affectent la réglementation en matière de reconnaissance juridique des communications de données et de la signature électronique ;
- l'absence de règles juridiques spécifiques protectrices des consommateurs, des droits de propriété intellectuelle, des données à caractère personnel et des systèmes d'informations ;
- l'absence de législations relatives aux téléservices et au télétravail ;
- l'application des techniques électroniques aux actes commerciaux et administratifs ;
- les éléments probants introduits par les techniques numériques (horodatage, certification, etc.).
- les règles applicables aux moyens et prestations de cryptologie ;
- l'encadrement de la publicité en ligne ;
- l'absence de législations fiscale et douanière appropriées au commerce électronique.

Convaincus que ce constat justifie l'appel à la mise en place d'un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain ; que l'objet de cette convention vise donc à assurer la sécurité et le cadre juridique nécessaires à l'émergence de l'économie du savoir en Afrique.

Soulignant que sur un autre plan, la protection des données à caractère personnel ainsi que de la vie privée se présente donc comme un enjeu majeur de la société de l'information, tant pour les pouvoirs publics que pour les autres parties prenantes ; que de cette protection nécessite un équilibre entre l'usage des technologies de l'information et de la communication et la protection de la vie privée des citoyens dans leur vie quotidienne ou professionnelle tout en garantissant la libre circulation des informations.

Préoccupés par l'urgence de la mise en place d'un dispositif permettant de faire face aux dangers et risques nés de l'utilisation de l'informatique et des fichiers sur les individus dans le souci de respecter la vie privée et les libertés tout en favorisant la promotion et le développement des TIC dans les pays membres de l'Union Africaine ;

Considérant que l'ambition de la présente convention est de répondre aux besoins de législation harmonisée dans le domaine de la cybersécurité dans les États membres de l'Union africaine ; qu'elle vise à mettre en place, dans chaque État partie, un dispositif permettant de lutter contre les atteintes à la vie privée

susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel ; qu'elle garantit, en proposant un type d'ancrage institutionnel, que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant également en compte les prérogatives des États, les droits des collectivités locales, les intérêts des entreprises ; tout en prenant en compte les meilleures pratiques reconnues au niveau international.

Considérant que la protection pénale du système de valeurs de la société de l'information s'impose comme une nécessité dictée par des considérations de sécurité ; qu'elle se manifeste essentiellement par le besoin d'une législation pénale appropriée à la lutte contre la cybercriminalité en général et au blanchiment de capitaux en particulier ;

Conscients qu'il est nécessaire, face à l'actualité de la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux informatiques et le développement de la société de l'information en Afrique, de fixer les grandes orientations de la stratégie de répression de la cybercriminalité, dans les pays membres de l'Union Africaine, en prenant en charge leurs engagements actuels aux plans sous régional, régional et international ;

Considérant que la présente Convention vise en droit pénal substantiel à moderniser les instruments de répression de la cybercriminalité, par l'élaboration d'une politique d'adoption d'incriminations nouvelles spécifiques aux TIC, l'adaptation de certaines incriminations, des sanctions et du régime de responsabilité pénale en vigueur dans les États Membres à l'environnement des technologies de l'information et de la communication ;

Considérant qu'en outre, en droit pénal procédural, elle fixe d'une part le cadre de l'aménagement de la procédure classique relativement aux technologies de l'information et de la communication et précise d'autre part les conditions de l'institution de procédures spécifiques à la cybercriminalité.

Rappelant la **décision Assembly/AU/Decl.1(XIV)** de la 14ème session ordinaire de l'Assemblée des Chefs d'États et de Gouvernements de l'Union africaine sur les technologies de l'information et de la communication en Afrique : défis et perspectives pour le développement, tenu à Addis-Abeba (Éthiopie) du 31 janvier au 2 février 2010.

Tenant compte de la Déclaration d'Oliver Tambo adoptée par la conférence extraordinaire de l'Union Africaine des ministres en charge de la Communication et des Technologies de l'Information à Johannesburg le 05 novembre 2009.

Rappelant les dispositions de la Déclaration d'Abidjan adoptée le 22 Février 2012 et celle d'Addis-Abeba adoptée le 22 juin 2012 sur l'harmonisation des Cyber-législations en Afrique.

ONT CONVENU DE CE QUI SUIT :

Article 1 : Définitions

Au sens de la présente Convention, les différentes expressions suivantes sont définies comme suit :

Chiffrement : toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;

Code de conduite : ensemble des règles élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, des réseaux et des communications électroniques de la structure concernée et homologué par l'Autorité de protection.

Commerce électronique : l'acte d'offrir, d'acheter, ou de fournir des biens et des services via les systèmes informatiques et les réseaux de télécommunications comme le réseau Internet ou tout autre réseau utilisant des moyens électroniques, optiques ou d'autres supports analogues permettant des échanges d'informations à distance.

Commission : la Commission de l'Union Africaine

Communication au public par voie électronique : :toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ;

Communication électronique : toute transmission au public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;

(La présente) Convention : la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel.

Conventions secrètes : les clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;

Communication électronique indirecte : tout message de texte, de voix, de son, d'image envoyé via un réseau de communication électronique et stocké sur le réseau ou sur un terminal de communication jusqu'à réception dudit message.

Consentement de la personne concernée : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique.

Courrier électronique : tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

Cryptologie : la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;

Cryptologie (Moyens de): l'ensemble des outils scientifiques et techniques
(matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;

Cryptologie (Prestation de): toute opération visant la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;

Cryptologie (Activité de): toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie

Dépasser un accès autorisé : le fait d'accéder à un système d'information et d'utiliser un tel accès pour obtenir ou modifier des données dans une partie de l'ordinateur ou le titulaire n'est pas autorisé d'y accéder.

Destinataire d'un traitement des données à caractère personnel : toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter les données.

Dispositif de création de signature électronique : ensemble d'éléments logiciels ou matériels permettant la création d'une signature électronique

Dispositif de vérification de signature électronique : ensemble d'éléments logiciels ou matériels permettant la vérification d'une signature électronique

Dommage : toute atteinte à l'intégrité ou à la disponibilité des données, d'un programme, d'un système ou d'une information.

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité

Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

Données sensibles : toutes les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.

Données dans le domaine de la santé : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques précitées.

Double criminalité : une infraction punie à la fois dans l'État où un suspect est détenu et un État demandant que le suspect soit remis ou transféré.

État membre (ou États membres) : le (les) État(s) Membre(s) de l'Union Africaine

État partie (ou États parties) État membre (ou les États membres) qui a (ont) ratifié ou accéder à la présente Convention

Fichier de données à caractère personnel : tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Information : tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, ou autre ;

Infrastructure critique de TIC/Cyberespace : Infrastructure TIC/cyber qui est essentielle aux services vitaux pour la sureté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique.

Interconnexion des données à caractère personnel : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement.

Mineur ou Enfant : toute personne physique âgée de moins de 18 ans au sens de la Charte Africaine sur les droits et le bien-être de l'Enfant et de la convention des Nations Unies sur les droits de l'enfant ;

Moyen de paiement électronique : moyen permettant à son titulaire d'effectuer des opérations de paiement électroniques en ligne.

Pornographie infantile : toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par autres moyens où :

(A) la production de telles représentations visuelles implique un mineur,

(B) ces représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non

(C) cette représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur engage dans un comportement sexuellement explicite.

Prestataire de services de cryptologie : toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

Personne concernée : toute personne physique qui fait l'objet d'un traitement des données à caractère personnel.

Prospection directe : tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ; elle vise aussi toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.

Raciste et xénophobe en matière des technologies de l'information et de la communication : tout matériel 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,

Responsable du traitement : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités.

Signature électronique : une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de procédé d'identification ;

Sous-traitant : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement.

Système informatique : Tout dispositif électronique, magnétique, optique, électrochimique ou tout autre dispositif de haut débit isolé ou interconnecté qui performe la fonction de stockage de données ou l'installation de communications. Ces communications sont directement liées à ou fonctionnent en association avec d'autre(s) dispositif(s) ;

Tiers : toute personne physique ou morale, publique ou privée, tout autre organisme ou association autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données.

Traitement des données à caractère personnel : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel.

UA : l'Union Africaine

CHAPITRE I: LES TRANSACTIONS ELECTRONIQUES

Section I: Le Commerce Électronique

Article 2 : Champ d'application du commerce électronique

1. Les États membres veillent à ce que l'activité de commerce électronique s'exerce librement dans tous les États parties qui ratifient ou adhèrent à la présente Convention à l'exclusion des domaines suivants :

   a) les jeux d'argent, mêmes sous forme de paris et de loteries, légalement autorisés ;
   b) les activités de représentation et d'assistance en justice ;
   les activités exercées par les notaires ou les autorités équivalentes en application des textes en vigueur.

2. Sans préjudice des autres obligations d'information prévues par les textes législatifs et réglementaires en vigueur dans les États membres de l'Union Africaine, les États Parties veillent à ce que toute personne qui exerce le commerce électronique est tenue d'assurer à ceux à qui est destinée la fourniture des biens ou la prestation de services un accès facile, direct et permanent utilisant un standard ouvert aux informations suivantes :

   a) s'il s'agit d'une personne physique, le prestataire doit indiquer ses nom et prénom et, s'il s'agit d'une personne morale, sa raison sociale; son capital, son numéro d'inscription au registre des sociétés ou association,
   b) l'adresse complète de l'endroit où elle est établie, son adresse de courrier électronique, ainsi que son numéro de téléphone ;
   c) si elle est assujettie aux formalités d'inscription des entreprises ou au répertoire national des entreprises et associations, le numéro de son inscription, son capital social et l'adresse de son siège social ;
   d) si elle est assujettie aux taxes, le numéro d'identification fiscal
   e) si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ainsi que la référence de l'autorisation;
   f) si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'État membre de l'Union Africaine dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite.

3. Toute personne physique ou morale qui exerce l'activité de commerce électronique doit, même en l'absence d'offre de contrat, dès lors qu'elle mentionne un prix, indiquer celui-ci

de manière claire et non ambiguë, et notamment si le prix inclut les taxes, les frais de livraison et autres charges.

Article 3 : La responsabilité contractuelle du fournisseur de biens ou de services électroniques

L'activité de commerce électronique est soumise à la loi de l'État partie sur le territoire duquel la personne qui l'exerce est établie, sous réserve de la commune intention de cette personne et de celle à qui sont destinés les biens ou services.

Article 4 : Publicité par voie électronique

1. Sans préjudice de l'article 3, toute publicité, sous quelque forme que ce soit, accessible par un service de communication en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée.

2. Les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celle de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie électronique, doivent être clairement précisées et aisément accessibles.

3. Les États parties de l'Union Africaine s'engagent à interdire la prospection directe via n'importe quelle forme de communication indirecte utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.

4. Nonobstant les dispositions de l'Article 4.2, la prospection directe par courrier électronique est autorisée si :

a) les coordonnées du destinataire ont été recueillies directement auprès de lui ;

b) le destinataire ayant donné son consentement au prospecteur d'être contacté par ses partenaires ;

c) la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

5. Les États Parties s'engagent à interdire l'émission, à des fins de prospection directe, des messages via n'importe quelle forme de communication indirecte, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci.

6. Les États Parties s'engagent à interdire la dissimulation de l'identité de la personne pour le compte de laquelle la publicité accessible par un service de communication en ligne est émise

Section II : Les obligations conventionnelles sous forme électronique

Article 5 : Les contrats électroniques

1. Les informations qui sont demandées en vue de la conclusion d'un contrat ou celles qui sont adressées au cours de son exécution peuvent être transmises par moyen électronique si leurs destinataires ont accepté l'usage de ce moyen. L'utilisation des communications électroniques est présumée recevable sauf si le bénéficiaire a déjà exprimé sa préférence pour un autre moyen de communication.

2. Le fournisseur qui propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les conditions contractuelles applicables directement ou indirectement, d'une manière qui permette leur conservation et leur reproduction conformément aux législations nationales.

3. Pour que le contrat soit valablement conclu, le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de sa commande notamment du prix avant de confirmer celle-ci pour exprimer son acceptation.

4. La personne qui offre ses produits et services doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

5. Il peut être dérogé aux dispositions des Articles 5.3 et 5.4 de la présente Convention dans les conventions conclues entre professionnels (B2B).

6. a. Toute personne physique ou morale exerçant l'activité définie au premier alinéa de l'Article 2.1 de la présente Convention est responsable de plein droit à l'égard de son cocontractant de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci.

b. Toutefois, elle peut s'exonérer de tout ou partie de sa responsabilité

en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit au cocontractant, soit à un cas de force majeure.

Article 6 : L'écrit sous forme électronique

1. Sans préjudice des dispositions légales en vigueur dans l'État Partie, nul ne peut être contraint de poser un acte juridique par voie électronique.

2. a. Lorsqu'un écrit est exigé pour la validité d'un acte juridique, chaque État Partie membre établit les conditions légales pour l'équivalence fonctionnelle entre les communications électroniques et les versions papiers, lorsque la réglementation interne en vigueur exige un écrit pour la validité d'un acte juridique.

   b. Lorsque l'écrit sur papier est soumis à des conditions particulières de lisibilité ou de présentation, l'écrit sous forme électronique doit répondre à des exigences équivalentes.

   c. L'exigence d'un envoi en plusieurs exemplaires est réputée satisfaite sous forme électronique si l'écrit peut être reproduit sous une forme matérielle par le destinataire.

3. Il est fait exception aux dispositions de l'Article 6.2 de la présente Convention pour :

   a) les actes sous seing privé relatifs au droit de la famille et des successions ; et

   b) les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale en conformité avec les législations nationales, sauf s'ils sont passés par une personne pour les besoins de sa profession.

4. La remise d'un écrit sous forme électronique est effective lorsque le destinataire, après en avoir pris connaissance, en accuse réception.

5. Eu égard à leurs fonctions fiscales, les factures doivent faire l'objet d'un écrit permettant d'assurer la lisibilité, l'intégrité et la pérennité du contenu. L'authenticité de l'origine doit également être garantie.
   Parmi les méthodes susceptibles d'être mises en œuvre pour atteindre les finalités fiscales de la facture et assurer que ses fonctions ont été satisfaites figure la réalisation de contrôles de gestion qui établiraient une

   piste d'audit fiable entre une facture et une livraison de biens ou de services.

   Outre le type de contrôles de gestion décrits au § 1er, les méthodes

suivantes constituent des exemples de technologies permettant d'assurer l'authenticité de l'origine et l'intégrité du contenu d'une facture électronique:

a. une signature électronique qualifiée, telle que définie à l'article 1 ;

b. un échange de données informatisées (EDI), compris comme le transfert électronique, d'un ordinateur à un autre, de données commerciales et administratives sous la forme d'un message EDI structuré conformément à une norme agréée, pour autant que l'accord relatif à cet échange prévoie l'utilisation de procédures garantissant l'authenticité de l'origine et l'intégrité des données. ».

6. L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier et a la même force probante que celui-ci, 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.

Section III : La sécurisation des transactions électroniques

Article 7 : Assurer la sécurité des transactions électroniques

1. a. Le fournisseur doit permettre à ces clients d'effectuer leurs paiements en utilisant un moyen de paiement électronique approuvé par l'État selon la réglementation en vigueur de chaque État Partie.

b. Le fournisseur de biens ou prestataire de services par voie électronique qui réclame l'exécution d'une obligation doit en prouver l'existence et, lorsqu'il se prétend libéré, doit prouver que l'obligation est inexistante ou éteinte.

2. Lorsque les dispositions légales des pays membres n'ont pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens possibles le titre le plus vraisemblable, quel qu'en soit le support.

3. a. La copie ou toute autre reproduction d'actes passés par voie électronique à la même force probante que l'acte lui-même lorsqu'elle est certifiée conforme par des organismes agréés par une autorité - de l'État Partie.

b. La certification donne lieu, le cas échéant, à la délivrance d'un certificat de conformité.

4. a. Une signature électronique créée par un dispositif sécurisé que le

signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat numérique est admise comme signature au même titre que la signature manuscrite.

b. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée par un dispositif sécurisé de création de signature, qu'elle garantit l'intégrité de l'acte et que l'identification du signataire en est assurée.

CHAPITRE II : LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Section I: la protection des données à caractère personnel

Article 8: L'objet de la présente Convention sur les données à caractère personnel

1. Chaque État partie s'engage à mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel.

2. Ce dispositif doit garantir que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant en compte les prérogatives de l'État, les droits des collectivités locales et les buts pour lesquels les entreprises ont été créées.

Article 9: Le champ d'application de la Convention

1. Sont soumises à la présente Convention :

   a) Toute collecte, tout traitement, toute transmission, tout stockage ou toute utilisation des données à caractère personnel effectués par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé ;
   b) Tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'Article 9.2 de la présente Convention ;
   c) Tout traitement mis en œuvre sur le territoire d'un État Partie de l'Union Africaine ;
   d) Tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

2. La présente Convention ne s'applique pas :

   a) aux traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion

b) aux copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

Article 10 : Les formalités préalables à la mise en œuvre des traitements des données à caractère personnel

1. Sont dispensés des formalités préalables :

a) les traitements mentionnés à l'Article 9.2 de la présente Convention;

b) les traitements ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;

c) les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers.

2. En dehors des cas prévus à l'Article 10.1 ci-dessus et aux Article 10.4 et 10.5 de la présente Convention, les traitements de données à caractère personnel font l'objet d'une déclaration auprès de l'autorité de protection.

3. Pour les catégories les plus courantes de traitement des données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'autorité nationale de protection établit et publie des normes destinées à simplifier ou à exonérer l'obligation de déclaration.

4. Sont mis en œuvre après autorisation de l'autorité nationale de protection :

a) les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;

b) les traitements des données à caractère personnel portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ;

c) les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers, telle que définie à l'Article 15 de la présente Convention les traitements portant sur un numéro national d'identification ou tout autre identifiant de la même nature ;

d) les traitements des données à caractère personnel comportant des données biométriques ;

e) les traitements des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques.

5. Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont décidés par acte législatif ou réglementaire pris après avis motivé de l'autorité nationale de protection.

Ces traitements portent sur :

a) la sûreté de l'État, la défense ou la sécurité publique ;

b) la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

c) le recensement de la population ;

d) les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle.

6. Les demandes d'avis, les déclarations et les demandes d'autorisations doivent préciser :

a) l'identité et l'adresse du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire d'un pays membre de l'Union Africaine, celles de son représentant dûment mandaté ;

b) la ou les finalités du traitement ainsi que la description générale de ses fonctions ;

c) les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements

d) les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

e) la durée de conservation des données traitées ;

f) le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

g) les destinataires habilités à recevoir communication des données ;

h) la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

i) les dispositions prises pour assurer la sécurité des traitements et des données ;

j) l'indication du recours à un sous-traitant ;

k) les transferts de données à caractère personnel envisagés à destination d'un pays tiers non membre de l'Union Africaine, sous réserve de réciprocité.

7. L'autorité nationale de protection se prononce dans un délai fixe à compter de la réception de la demande d'avis ou d'autorisation. Toutefois, ce délai peut être prorogé ou non sur décision motivée de l'autorité nationale de protection.

8. L'avis, la déclaration ou la demande d'autorisation peut être adressé à l'autorité nationale de protection par voie électronique ou par voie postale.

9. L'autorité nationale de protection peut être saisie par toute personne, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

Section II : Le cadre institutionnel de la protection des données à caractère personnel

Article 11: Statut, composition et organisation des autorités nationales de protection des données à caractère personnel

1. a. Chaque État Partie s'engage à mettre en place une autorité chargée de la protection des données à caractère personnel.

b. L'autorité nationale de protection est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Convention.

2. L'autorité nationale de protection informe les personnes concernées et les responsables de traitement de leurs droits et obligations.

3. Sans préjudice aux dispositions de l'article– 11.6, chaque État Partie détermine la composition de l'autorité nationale chargée de la protection des données à caractère personnel.

4. Des agents assermentés, conformément aux dispositions en vigueur dans les États parties, peuvent être appelés à participer à la mise en œuvre des missions de vérification. .

5. a. Les membres de l'autorité nationale de protection sont soumis au secret professionnel conformément aux textes en vigueur dans chaque pays membre.

b. Chaque autorité nationale de protection établit un règlement intérieur qui précise, notamment, les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers.

6. La qualité de membre d'une autorité nationale de protection est incompatible avec la qualité de membre du Gouvernement, de l'exercice des fonctions de dirigeants d'entreprise, de la détention de participation dans les entreprises du secteur des technologies de l'information et de la communication.

7. a. Sans préjudice des législations nationales, les membres des autorités nationales de protection jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction.

b. Dans l'exercice de leur attribution, ils ne reçoivent d'instruction d'aucune autorité.

8. Les États parties s'engagent à doter les autorités nationales de protection des moyens humains, techniques et financiers nécessaires à l'accomplissement de leur mission.

Article 12: Attributions des autorités nationales de protection

1. Les autorités nationales de protection sont chargées de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Convention dans les États Partis de l'Union africaine.

2. Les autorités nationales de protection s'assurent que les Technologies de l'Information et de la Communication ne comportent pas de menace au regard des libertés publiques et de la vie privée des citoyens. A ce titre, elles sont chargées de :

   a) répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;
   b) informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;
   c) autoriser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;
   d) recevoir les formalités préalables à la création de traitements des données à caractère personnel ;
   e) recevoir les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci ;
   f) informer sans délai l'autorité judiciaire pour certains types d'infractions dont elles ont connaissance ;
   g) procéder, par le biais de son personnel ou autre expert requis, à des vérifications portant sur tout traitement des données à caractère personnel;
   h) prononcer des sanctions, administratives et pécuniaires, à l'égard des responsables de traitement ;
   i) mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;
   j) conseiller les personnes et organismes qui font les traitements des données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements ;
   k) autoriser les transferts transfrontaliers de données à caractère personnel ;
   l) faire des suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données;
   m) mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel de pays tiers ;
   n) participer aux négociations internationales en matière de protection
   o) des données à caractère personnel ;
   établir, selon une périodicité bien définie, un rapport d'activités remis aux autorités compétentes de l'État Partie.

3. Les autorités nationales de protection peuvent prononcer les mesures suivantes :

   a) un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente Convention ;
   b) une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

4. Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, Les autorités nationales de protection peuvent prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

   a) un retrait provisoire de l'autorisation accordée ;
   b) le retrait définitif de l'autorisation ;
   c) une amende pécuniaire.

5. En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel entraîne une violation de droits et libertés fondamentaux, les autorités nationales de protection, après procédure contradictoire, peuvent décider :

   a) l'interruption de la mise en œuvre du traitement ;
   b) le verrouillage de certaines données à caractère personnel traitées ;
   c) l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente Convention.

6. Les sanctions et décisions prises par les autorités nationales de protection sont susceptibles de faire l'objet d'un recours.

Section III: Les obligations relatives aux conditions de traitements de données à caractère personnel

Article 13: Les principes de base gouvernant le traitement des données à caractère personnel

Principe 1 : Le principe de consentement et de légitimité du traitement des données à caractère personnel

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement. Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :

a) au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
b) à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement

ou le tiers auquel les données sont communiquées;

c) à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

d) à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Principe 2 : Le principe de la licéité et de la loyauté du traitement des données à caractère personnel

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Principe 3 : Le principe de finalité, de pertinence, de conservation du traitement des données à caractère personnel

a) Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

b) Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

c) Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

d) Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Principe 4: Le principe d'exactitude des données à caractère personnel

Les données collectées doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Principe 5: Le principe de transparence des données à caractère personnel

Le principe de transparence implique une information obligatoire de la part du responsable du traitement portant sur les données à caractère personnel.

Principe 6: Le principe de confidentialité et de sécurité des traitements de données à caractère personnel

a. Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

b. Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect des mesures de sécurité définies dans la présente Convention.

Article 14: les principes spécifiques relatifs au traitement de données sensibles

1. Les États Parties s'engagent à interdire la collecte et tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

2. L'interdiction visée à l'Article 14.1 ne s'applique pas pour les catégories de traitements suivantes lorsque :

a) le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;
b) la personne concernée a donné son consentement par écrit, quel que soit le support, à un tel traitement et en conformité avec les textes en vigueur ;
c) le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
d) le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
e) une procédure judiciaire ou une enquête pénale est ouverte ;
f) le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;
g) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée pendant la période précontractuelle ;
h) le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;
i) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
j) le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls

membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

3. Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche ou d'expression artistique ou littéraire est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou chercheur, dans le respect des règles déontologiques de ces professions.

4. Les dispositions de la présente Convention ne font pas obstacle à l'application des dispositions des législations nationales relatives à la presse écrite ou au secteur de l'audiovisuel ainsi que du code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

5. Aucune décision impliquant une appréciation sur le comportement d'une personne ou produisant des effets juridiques à l'égard d'une personne ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

6. a. Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un État non-Partie de l'Union Africaine que si cet État assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

   b. La précédente interdiction ne s'applique pas lorsqu'avant tout transfert des données à caractère personnel vers ce pays tiers, le responsable du traitement doit préalablement solliciter l'autorisation de l'autorité nationale de protection.

Article 15: L'interconnexion des fichiers comportant des données à caractère personnel

L'interconnexion des fichiers visée à l'Article 10.4 de la présente Convention doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements. Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit en outre tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Section IV : Les droits conférés à la personne dont les données font l'objet d'un traitement

Article 16: Droit à l'information

Le responsable du traitement doit fournir à la personne physique dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

a) son identité et, le cas échéant, celle de son représentant;
b) la ou les finalités déterminées du traitement. auquel les données sont destinées ;
c) les catégories de données concernées ;
d) le ou les destinataires auxquels les données sont susceptibles d'être communiquées ;
e) le fait de pouvoir demander à ne plus figurer sur le fichier ;
f) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;
g) la durée de conservation des données ;
h) l'éventualité de tout transfert de données à destination de pays tiers.

Article 17 : Droit d'accès

Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement sous forme de questions :

a) les informations permettant de connaître et de contester le traitement ;
b) la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement ;
c) la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
d) des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont

communiquées.

Article 18: Droit d'opposition

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le

compte de tiers à des fins de prospection et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Article 19: Droit de rectification et de suppression

Toute personne physique peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Section V : Les obligations du responsable de traitement de données à caractère personnel

Article 20: Les obligations de confidentialité

Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Article 21 : Les obligations de sécurité

Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Article 22: Les obligations de conservation

Les données à caractère personnel ne doivent pas être conservées au-delà de la période requise pour les fins en vue desquelles elles ont été recueillies et traitées.

Article 23: Les obligations de pérennité

a. Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

b. Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

CHAPITRE III – PROMOTION DE LA CYBERSECURITE ET LUTTE CONTRE LA CYBERCRIMINALITE

Section I : Mesures de Cyber sécurité à prendre au niveau national

Article 24: Cadre de la cyber sécurité nationale

1. Politique nationale

Chaque État Partie s'engage en collaboration avec les parties prenantes, à se doter d'une politique nationale de cyber sécurité qui reconnaisse l'importance de l'infrastructure essentielle de l'information (IEI) pour la nation, qui identifie les risques auxquels elle est confrontée en utilisant une approche tous risques et qui définit dans les grandes lignes la façon dont les objectifs seront mis en oeuvre.

2. Stratégie nationale

Les États Parties s'engagent à adopter les stratégies qu'ils jugent appropriées et suffisantes pour mettre en œuvre la politique nationale de cyber sécurité, spécifiquement dans le domaine de la réforme législative et du développement, de la sensibilisation et du développement des capacités, du partenariat public-privé et de la coopération internationale, pour ne citer que ceux-ci. Les stratégies devront établir des structures organisationnelles et se fixer des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cyber sécurité, tout en posant les bases d'une gestion effective des incidents et de la coopération internationale.

Article 25: Mesures légales

1. Législations contre la cybercriminalité

Chaque État Partie s'engage à adopter les mesures législatives et/ou réglementaires qu'il jugera efficaces en considérant comme infractions criminelles substantielles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes technologies de l'information et de la communication et les données qu'ils traitent et des infrastructures réseau sous-jacentes, ainsi que les mesures procédurales qu'il jugera efficaces pour rechercher et poursuivre les contrevenants. Les États Parties s'engagent à prendre en considération le choix du langage utilisé dans les meilleures pratiques internationales.

2. Les autorités réglementaires nationales

Chaque État Partie s'engage à adopter les mesures législatives et/ou réglementaires qu'il jugera nécessaires pour conférer la responsabilité spécifique aux institutions - qu'elles soient nouvellement créées ou préexistantes – ainsi qu'aux officiels désignés de ces institutions, afin de leur impartir l'autorité

statutaire et la capacité légale à agir dans tous les aspects de l'application de la cyber sécurité, y compris mais sans s'y limiter, la réponse aux incidents et la coordination **et la coopération** en matière de justice réparatrice, les investigations en criminalistique, la poursuite, etc.

3. Droits des citoyens

En adoptant des mesures législatives et/ou réglementaires en matière de cyber sécurité ou en créant le cadre d'application de celle-ci, chaque État Partie veillera à ce que les mesures adoptées n'entravent pas les droits des citoyens garantis en vertu de la constitution nationale, droits internes et protégés par les conventions internationales, particulièrement la Charte africaine des droits de l'Homme et des Peuples, ainsi que les droits fondamentaux tels que le droit à la liberté d'expression, le droit au respect de la vie privée et le droit à une instruction équitable, entre autres.

4. Protection des infrastructures critiques

Chaque État Partie s'engage à adopter des mesures législatives et/ou réglementaires qu'il jugera nécessaires pour identifier les secteurs considérés comme sensibles pour sa sécurité nationale et le bien-être de l'économie et des systèmes technologies de l'information et de la communication désignés pour fonctionner dans ces secteurs comme constituant des infrastructures critiques de l'information, en proposant à cet égard une sanction plus sévère pour les activités criminelles sur les systèmes TIC dans ces secteurs et également des dispositions pour améliorer la vigilance, la sécurité et la gestion.

Article 26 : Système national de la cyber sécurité

1. Culture de cyber sécurité

a) Chaque État Partie s'engage à promouvoir la culture de la sécurité chez toutes les parties prenantes – gouvernements, entreprises et société civile – qui développent, possèdent, gèrent, mettent en service et utilisent les systèmes et les réseaux d'information. La culture de la sécurité devra mettre l'accent sur la sécurité dans le développement des systèmes et des réseaux d'information et sur l'adoption de nouvelles façons de penser et de se comporter lors de l'utilisation des systèmes d'information et lors des communications ou des transactions à travers les réseaux.

b) Dans le cadre de la promotion de la culture de sécurité, les États Parties peuvent adopter les mesures suivantes : mettre en place un plan de cyber sécurité pour les systèmes gérés par **leurs gouvernements** ; élaborer et mettre en œuvre des programmes et des initiatives de sensibilisation sur la sécurité pour les utilisateurs des systèmes et des réseaux ; inciter au développement d'une culture de la sécurité dans les entreprises ; favoriser l'engagement de la société civile ; lancer un programme de sensibilisation nationale détaillé et complet pour les internautes, les petites entreprises, les écoles et les enfants.

2. Rôle des gouvernements

Chaque État Partie s'engage à être le garant d'un leadership pour le développement de la culture de la sécurité à l'intérieur de ses frontières. Les États membres s'engagent à sensibiliser, assurer l'éducation et la formation ainsi que la diffusion des informations au public.

3. Partenariat Public-Privé

Chaque État Partie s'engage à développer un partenariat public-privé en tant que modèle afin d'engager l'industrie, la société civile et le monde universitaire dans la promotion et le renforcement d'une culture de la cyber sécurité.

4. Éducation et Formation

Chaque État Partie s'engage à adopter des mesures de renforcement des capacités afin de proposer des formations couvrant tous les domaines de la cyber sécurité aux différents acteurs de la Société de l'information et à fixer des normes pour le secteur privé.

Les États Parties s'engagent à promouvoir le renforcement technique des professionnels des technologies de l'information et de la communication à l'intérieur et à l'extérieur des instances gouvernementales par le biais de la certification et de la normalisation des formations ; la catégorisation des qualifications professionnelles et le développement et la distribution de matériel en fonction des besoins.

Article 27 : Structures nationales de suivi de la cyber sécurité

1. Gouvernance de la cyber sécurité

a) Chaque État Partie s'engage à adopter des mesures nécessaires pour mettre en place un dispositif institutionnel approprié pour une prise en charge de la gouvernance de la cyber sécurité.

b) Les mesures préconisées au titre du paragraphe 1 du présent article doivent établir un fort leadership et un engagement dans les divers aspects de la cyber sécurité des institutions et des groupes professionnels compétents de l'État Partie. À cet égard, les États Parties s'engagent à prendre des dispositions pour:

i) établir une responsabilité claire en matière de cyber sécurité à tous les niveaux du gouvernement en définissant précisément les rôles et les responsabilités ;

ii) exprimer un engagement manifeste en matière de

cybersécurité, qui soit public et transparent ;

iii) encourager le secteur privé, en sollicitant son engagement et sa participation dans des initiatives dirigées par le gouvernement aux fins de promouvoir la cybersécurité.

c) La gouvernance de la cybersécurité devra être établie en fonction d'un cadre national qui soit en mesure de répondre aux défis perçus et à toute question relative à la sécurité de l'information au niveau national dans le plus grand nombre possible de domaines de la cybersécurité.

2. Le cadre institutionnel

Chaque État membre s'engage à adopter des mesures qu'il jugera nécessaires aux fins de créer des institutionscompétentes pour lutter contre la cybercriminalité ; de mener une veille, une réponse aux incidents et aux alertes ; d'assurer la coordination nationale et transfrontalière des problèmes de cybersécurité et également la coopération mondiale.

Article 28 : Coopération internationale

1. Harmonisation

Les États Parties s'engagent à garantir que les mesures législatives et/ou réglementaires adoptées pour lutter contre la cybercriminalité renforcent la possibilité d'harmonisation régionale de ces mesures et respectent le principe de la double incrimination.

2. Entraide judiciaire

Les États Parties qui n'ont pas de conventions d'assistance mutuelle en matière de cybercriminalité s'engagent à encourager la signature des conventions d'entraide judiciaire en conformité avec le principe de la double incrimination tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre les organisations des États membres sur une base bilatérale et multilatérale.

3. Échange d'informations

Les États Parties s'engagent à encourager la mise en place des institutions qui échangent des informations sur les cybermenaces et sur l'évaluation de la vulnérabilité telles que les équipes de réaction d'urgence en informatique (CERT : Computer Emergency Response Teams) ou les équipes de réaction aux incidents de sécurité informatique (CSIRTS : Computer Security Incident Response Teams).

4. Moyen de la coopération

Les États Parties s'engagent à se prévaloir de moyens existants pour la coopération internationale aux fins de répondre aux cybermenaces, à améliorer la cybersécurité et à stimuler le dialogue entre les parties prenantes. Ces moyens pourraient être internationaux, intergouvernementaux ou régionaux, ou basés sur des partenariats privés et publics. »

Section II : Dispositions pénales

Article 29 : Les infractions spécifiques aux Technologies de l'Information et de la Communication

1. Atteintes aux systèmes informatiques

Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait :

a) d'accéder ou de tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé ;
b) d'accéder ou de tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé avec l'intention de commettre une nouvelle infraction ou faciliter une telle infraction ;
c) de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique ;
d) d'entraver, fausser ou tenter d'entraver ou de fausser le fonctionnement d'un système informatique ;
e) d'introduire ou tenter d'introduire frauduleusement des données dans un système informatique ;
f) d'endommager ou de tenter d'endommager, d'effacer ou tenter d'effacer, de détériorer ou tenter de détériorer, d'altérer ou tenter d'altérer, de modifier ou tenter de modifier frauduleusement des données informatiques.

Les États Parties s'engagent par ailleurs à :

g) adopter des règles qui imposent aux vendeurs de produits des technologies de l'information et de la communication de faire réaliser, par des experts et des chercheurs en sécurité informatique indépendants, un essai de vulnérabilité et une évaluation de la garantie de sécurité, et de divulguer aux consommateurs toutes les vulnérabilités décelées dans les produits ainsi que les solutions recommandées pour y remédier.
h) prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait sans droit, de produire, vendre, importer, détenir, diffuser, offrir, céder ou mettre à disposition un équipement, un programme informatique, tout dispositif ou

donnée conçue ou spécialement adaptée pour commettre des infractions ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique.

2. Atteintes aux données informatisées

Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait de :

a) intercepter ou 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.
b) introduire, altérer, effacer ou supprimer intentionnellement et sans droit des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.
c) en connaissance de cause, faire usage des données obtenues de manière frauduleuse.
d) obtenir 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.
e) même par négligence, procéder ou faire procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre.
f) participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente convention.

3. Infractions se rapportant au contenu

1. Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait de :

a) produire, enregistrer, offrir, fabriquer, de mettre à disposition, de diffuser, de transmettre une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.
b) procurer ou de procurer à autrui, d'importer ou de faire importer, d'exporter ou de faire exporter une image ou une

représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

c) posséder une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.
d) faciliter et donner l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.
e) créer, télécharger, diffuser ou de mettre à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.
f) Commettre une menace 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
g) Proférer une insulte commise par le biais d'un système informatique 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 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.
h) Nier délibérément, d'approuver ou de justifier des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

2. Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale les infractions prévues par la présente Convention.

Lorsqu'elles ont été commises en bande organisée, elles seront punies du maximum de la peine prévue pour l'infraction concernée.

3. Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires pour faire en sorte qu'en cas de condamnation, que les tribunaux nationaux puissent prononcer la confiscation des matériels équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions mentionnées dans cette Convention.

4. Infractions se rapportant aux mesures de sécurisation des échanges électroniques

Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires pour faire en sorte que la preuve numérique en

matière pénale soit admise à établir les infractions aux lois pénales internes sous réserve qu'elle soit apportée au cours des débats et discutée devant le juge et que puisse être dûment identifiée la personne dont elle émane et qu'elle soit établie et conservée dans des conditions de nature à en garantir l'intégrité.

Article 30 : L'adaptation de certaines infractions aux Technologies de l'Information et de la Communication

1. Atteintes aux biens

a) Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction les atteintes juridiques aux biens, à savoir le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le chantage portant sur les données informatiques.

b) Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en circonstance aggravante l'utilisation des technologies de l'information et de la communication en vue de commettre des infractions comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux.

c) Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'inclure expressément « les moyens de communication numérique par voie électronique » à l'image d'Internet dans l'énumération des moyens de diffusion publique prévus dans leurs textes pénaux.

d) Les État Parties s'engagent à prendre des mesures législatives criminelles nécessaires en vue de restreindre l'accès aux systèmes protégés qui ont été considérés comme infrastructure critique de la défense nationale en raison des données critiques de sécurité nationale qu'ils contiennent.

2. Responsabilité pénale pour les personnes morales

Les État Parties s'engagent à prendre des mesures législatives nécessaires pour faire en sorte que les personnes morales autres que l'État, les collectivités locales et les établissements publics puissent être tenues pour responsables des infractions prévues par le présente Convention, commises pour leur compte par leurs organes ou représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 31 L'adaptation de certaines sanctions aux Technologies de l'Information et de la Communication

1. Sanctions pénales

a) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que les infractions prévues par la présente

Convention soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

b) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que les infractions prévues par la présente Convention soient passibles de peines appropriées selon sa législation nationale.

c) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte qu'une personne morale déclarée responsable au sens de la présente Convention, soit passible de peines effectives, proportionnées et dissuasives, qui comprennent des amendes pénales.

2. Autres sanctions pénales

a) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte qu'en cas de condamnation pour une infraction juridiction d'instruction ou de jugement saisi puisse prononcer à titre accessoire des peines complémentaires.

b) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte qu'en cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, le juge puisse ordonner à titre complémentaire obligatoire la diffusion au frais du condamné, par extrait, de la décision sur ce même support, et selon des modalités précisées dans les législations des États Membres.

c) Les État Parties s'engagent à prendre des mesures législatives nécessaires pour faire en sorte que la violation du secret stocké dans un système d'information soit punie des mêmes peines applicables au délit de violation du secret professionnel.

3. Droit procédural

a) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire d'un État Partie, sont utiles à la manifestation de la vérité, la juridiction saisie puisse opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

b) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que lorsque le autorité judiciaire en charge de l'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, soient

copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés, selon des modalités prévues dans les législations des États Parties.

c) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que les autorités judiciaires puissent, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par la présente Convention.

d) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le autorité judiciaire en charge de l'instruction puisse faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou une toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret.

e) Les État Parties s'engagent à prendre des mesures nécessaires pour faire en sorte que si les nécessités de l'information l'exigent le autorité judiciaire en charge de l'instruction puisse utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques 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, en application de moyens techniques existant sur son territoire ou ceux des États Parties, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

CHAPITRE IV: DISPOSITIONS FINALES

Article 32 : Mesures à prendre au niveau de l'Union Africaine

Le Président de la Commission informe l'Assemblée en ce qui concerne la mise en œuvre et le suivi de mécanisme opérationnel de la présente Convention.
Le mécanisme de suivi à mettre en place veillera à :

a) promouvoir et encourager sur le continent l'adoption et l'application de mesures de renforcement de la cybersécurité dans les téléservices et de lutte contre la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;
b) rassembler des documents et des informations sur les besoins en cybersécurité ainsi que sur la nature et l'ampleur de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;
c) élaborer des méthodes pour analyser les besoins en cybersécurité ainsi que sur la nature et l'ampleur de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace et diffuser l'information, et sensibiliser l'opinion publique sur les effets négatifs de ces phénomènes ;
d) conseiller les gouvernements Africains sur la manière de promouvoir la cybersécurité et de lutter contre le fléau de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace au niveau national ;
e) recueillir des informations et procéder à des analyses sur la conduite et le comportement délictueux des usagers des réseaux et des systèmes d'informations opérant en Afrique, et diffuser ces informations auprès des autorités nationales compétentes ;
f) élaborer et promouvoir l'adoption de codes de conduite harmonisés à l'usage des agents publics en matière de cybersécurité ;
g) établir des partenariats avec la Commission et la Cour africaines des droits de l'homme et des peuples, la société civile africaine, les organisations gouvernementales, intergouvernementales et non gouvernementales, afin de faciliter le dialogue sur la lutte contre la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;
h) soumettre des rapports réguliers au Conseil Exécutif de l'Union Africaine sur les progrès réalisés par chaque État partie dans l'application des dispositions de la présente Convention ;
i) s'acquitter de toute autre tâche relative à la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace que peuvent lui confier les organes délibérants de l'Union africaine.

Article 33 : Dispositions de sauvegarde

Les dispositions de la présente Convention ne peuvent être interprétées de manière non conforme aux principes pertinents du droit international, y compris

le droit coutumier international.

Article 34 : Règlement des différends

1. Tout différend né de l'application de la présente Convention est réglé à l'amiable, par voie de négociation directe entre les États Parties concernés.

2. Si le différend ne peut être réglé par voie de négociation directe, les États Parties s'efforcent de le régler par d'autres moyens pacifiques, y compris les bons offices, la médiation et la conciliation, ou tout autre moyen pacifique agréé par les Parties. À cet égard, les États Parties sont encouragés à recourir aux procédures et mécanismes de règlement des différends mis en place dans le cadre de l'Union.

Article 35 : Signature, ratification et adhésion

La présente Convention est ouverte à tous les États membres de l'Union, pour signature, ratification et adhésion, conformément à leurs procédures constitutionnelles respectives.

Article 36 : Entrée en vigueur

La présente Convention entre en vigueur trente (30) jours après la réception, par le Président de la Commission de l'Union africaine, du quinzième (15ème) instrument de ratification ou d'adhésion.

Article 37 : Amendement

1. Tout État Partie peut soumettre des propositions d'amendement ou de

2. Les propositions d'amendement ou de révision sont soumises au Président de la Commission de l'Union africaine, qui les transmet aux États Parties dans un délai de trente (30) jours suivant leur réception.

3. La Conférence de l'Union, sur recommandation du Conseil exécutif de l'Union, examine ces propositions à sa prochaine session, sous réserve que tous les États Parties en aient été notifiés trois (3) mois au moins avant le début de la session.

4. La Conférence de l'Union adopte les amendements, conformément à son Règlement intérieur.

5. Les amendements ou révisions entrent en vigueur conformément aux dispositions de l'article 36 ci-dessous.

Article 38 : Dépositaire

1. Les instruments de ratification ou d'adhésion sont déposés auprès du Président de la Commission de l'Union africaine.

2. Tout État Partie peut dénoncer la présente Convention en notifiant, par écrit, son intention un (1) an à l'avance au Président de la Commission de l'Union africaine.

3. Le Président de la Commission de l'Union africaine notifie aux États membres toute signature de la présente Convention, le dépôt de tout instrument de ratification ou d'adhésion, ainsi que son entrée en vigueur.

4. Le Président de la Commission notifie également aux États membres les demandes d'amendement ou de retrait de la Convention, ainsi que les réserves à celle-ci.

5. Dès l'entrée en vigueur de la présente Convention, le Président de la Commission de l'Union africaine l'enregistre auprès du Secrétaire général de l'Organisation des Nations unies, conformément à l'article 102 de la Charte des Nations unies.

6. La présente Convention, rédigée en quatre (4) textes originaux en Arabe, en Anglais, en Français et en Portugais, tous les quatre (4) textes faisant également foi, est déposée auprès du Président de la Commission de l'Union africaine, qui en transmet une copie certifiée conforme à chaque État membre dans sa langue officielle.

EN FOI DE QUOI, NOUS, Chefs d'État et de gouvernement de l'Union africaine, ou nos représentants dûment autorisés, avons adopté la présente Convention.

Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014

Annexe 4 : Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace CEDEAO.

COMMUNAUTE ECONOMIQUE DES ETATS
DE L'AFRIQUE DE L' OUEST

ECONOMIC COMMUNITY OF
WEST AFRICAN STATES

SOIXANTE SIXIEME SESSION ORDINAIRE DU CONSEIL DES MINISTRES

Abuja, 17 – 19 Août 2011

DIRECTIVE C/DIR/1/08/11 PORTANT LUTTE CONTRE LA CYBERCRIMINALITE DANS L'ESPACE DE LA CEDEAO

LE CONSEIL DES MINISTRES,

VU les Articles 10, 11 et 12 du Traité de la CEDEAO tel qu'amendé, portant création du Conseil des Ministres et définissant sa composition et ses fonctions ;

VU les articles 27, 32 et 33 dudit Traité relatifs à la science et à la technologie, et aux domaines des communications et des télécommunications ;

VU l'article 57 dudit Traité relatif à la coopération judiciaire et juridique qui prescrit que les Etats membres s'engagent à promouvoir la coopération judiciaire en vue d'harmoniser les systèmes judiciaires et juridiques;

VU l'Acte additionnel A/SA 1/01/07 du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication (TIC)

VU l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO ;

VU l'Acte Additionnel A/SA.2/01/10 relatif aux transactions électroniques dans l'espace CEDEAO ;

VU la Convention A/P1/7/92 de la CEDEAO relative à l'entraide judiciaire en matière pénale ;

VU la Convention A/P1/8/94 de la CEDEAO relative à l'Extradition ;

VU l'Accord de coopération en matière de police criminelle entre les Etats membres de la CEDEAO qui prescrit la mise en commun des compétences et partage d'expérience par les services de sécurité en vue d'accélérer de façon efficace les enquêtes policières ;

CONSIDERANT que l'utilisation des Technologies de l'Information et de la Communication entre autres l'Internet ou la cybernétique a engendré la recrudescence d'actes répréhensibles de tous ordres ;

NOTANT que la cybercriminalité est un phénomène nouveau qui nécessite la définition des infractions spécifiques, lesquelles doivent être rattachées consubstantiellement aux infractions classiques, tels que le vol, l'escroquerie, le recel, le chantage en raison de la nature du préjudice causé au moyen de l'utilisation de l'Internet ;

CONSCIENT que les actes répréhensibles commis au moyen de l'Internet nécessitent donc une qualification au plan légal et une répression appropriée en raison de la gravité des préjudices qu'ils engendrent ;

DESIREUX d'adopter un cadre de répression pénale en vue de lutter efficacement contre la cybercriminalité, ainsi que de permettre une coopération diligente et viable à l'échelle internationale;

APRES AVIS du Parlement de la CEDEAO en date du 23 Mai 2000

PRESCRIT :

CHAPITRE I

DISPOSITIONS GENERALES

Article Premier:

Définitions

Au sens de la présente Directive, les expressions ci-dessous sont définies comme suit:

communication électronique : toute mise à disposition au public ou à une catégorie du public par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;

données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

raciste et xénophobe en matière de TIC : 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, de l'affiliation ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou incite à de tels actes ;

mineur : toute personne âgée de moins de dix huit (18) ans au sens de la Convention des Nations Unies sur les droits de l'enfant ;

pornographie infantile : 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 ;

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.

Technologies de l'information et de la communication (TIC) : technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

Article 2.

Objet

La présente Directive a pour objet d'adapter le droit pénal de fond et la procédure pénale des Etats Membres de la CEDEAO au phénomène de la cybercriminalité.

Article 3 :

Champ d'application

La présente Directive s'applique à toutes les infractions relatives à la cybercriminalité dans l'espace CEDEAO, ainsi qu'à toutes les infractions pénales dont la constatation requiert la collecte d'une preuve électronique

CHAPITRE II:

INFRACTIONS SPECIFIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Constituent des infractions au sens de la présente Directive :

Article 4:

Accès frauduleux à un système informatique

Le fait pour toute personne d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un système informatique.

Article 5:

Maintien frauduleux dans un système informatique

Le fait pour toute personne de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique.

Article 6:

Entrave au fonctionnement d'un système informatique

Le fait pour toute personne d'entraver, de fausser, de tenter d'entraver ou de fausser le fonctionnement d'un système informatique.

Article 7:

Introduction frauduleuse de données dans un système informatique

Le fait pour toute personne d'introduire ou ***de*** tenter d'introduire frauduleusement des données dans un système informatique.

Article 8:

Interception frauduleuse de données informatiques

Le fait pour toute personne d'intercepter ou de tenter d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Article 9:

Modification frauduleuse de données informatiques

Le fait pour toute personne d'endommager ou de tenter d'endommager, d'effacer ou tenter d'effacer, de détériorer ou de tenter de détériorer, d'altérer ou de tenter d'altérer, de modifier ou de tenter de modifier frauduleusement des données informatiques.

Article 10:

Falsification de données informatiques

Le fait pour toute personne de produire ou de fabriquer un ensemble de données numérisées par l'introduction, la suppression ou l'effacement frauduleux de données informatiques 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.

Article 11

Fraude informatique

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.

Article 12:

Traitement frauduleux de données à caractère personnel

Le fait pour toute personne, même par négligence, de procéder ou faire procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par la loi sur les données à caractère personnel prévue à cet effet dans chaque Etat Membre.

Article13:

Usage de données falsifiées

Le fait pour toute personne, en connaissance de cause, de faire usage de données falsifiées.

Article 14:

Disposition d'un équipement pour commettre des infractions

Le fait pour toute personne, sans motif légitime de produire, de vendre, d'importer, de détenir, de diffuser, d'offrir, de céder ou de mettre à disposition un équipement, un programme informatique, tout dispositif, donnée, un mot de passe, un code d'accès ou des données informatiques similaires adaptées pour commettre des infractions telles que définies par la présente Directive

Article 15:

Participation à une association formée ou à une entente en vue de commettre des infractions informatiques

Le fait pour toute personne de participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente Directive.

Article 16

Production d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de produire, ***d'***enregistrer, ***d'***offrir, de mettre à disposition, de diffuser, de transmettre une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 17:

Importation ou exportation d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de se procurer ou de procurer à autrui, d'importer ou de faire importer, d'exporter ou de faire exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 18:

Possession d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de posséder une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatiques.

Article 19:

Facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur

Le fait pour toute personne de faciliter l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 20:

Disposition d'écrits ou d'images de nature raciste ou xénophobe par le biais d'un système informatique

Le fait pour toute personne de créer, de télécharger, de diffuser ou de mettre à disposition sous quelque forme que ce soit des écrits, des messages, des photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

Article 21:

Menace par le biais d'un système informatique

Toute menace commise 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, la filiation, la religion, l'origine nationale ou ethnique, dans la mesure où cette appartenance sert de prétexte à une telle menace.

Article 22:

Injure commise par le biais d'un système informatique

Toute injure commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'origine nationale ou ethnique, la religion, la filiation dans la mesure où cette appartenance sert de prétexte à une telle injure.

Article 23:

Négationnisme

Tout fait intentionnel de nier, d'approuver ou de justifier par le biais d'un système informatique, des actes constitutifs de génocide ou de crimes contre l'humanité .

CHAPITRE III:

ADAPTATION DES INFRACTIONS CLASSIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Article 24:

Circonstances aggravantes

Le fait d'utiliser les TIC ou d'agir en bande organisée en vue de commettre des infractions de droit commun comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le

terrorisme, le blanchiment de capitaux constitue une circonstance aggravante de ces infractions au sens de la présente Directive

Article 25:

Atteinte portant sur les logiciels et programmes informatiques

Constitue une infraction, au sens de la présente Directive, le fait de commettre un vol, une, escroquerie, un recel, un abus de confiance, une extorsion de fonds, un acte de terrorisme, ou une contrefaçon portant les données informatiques, les logiciels et les programmes.

Article 26: Infractions de presse commises *par des moyens de* communication électronique

Les infractions de presse commises par un moyen de communication électronique au sens de la présente Directive, sont soumises aux dispositions relatives aux infractions de presse applicables dans les Etats membres.

Article 27:

Responsabilité pénale des personnes morales autres que publiques

Toute personne morale à l'exception de l'Etat, des collectivités locales et des établissements publics, est tenue pour responsable des infractions prévues par la présente Directive, lorsqu'elles sont commises pour son compte par ses représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes fait

CHAPITRE IV: SANCTIONS

Article 28:

Peines principales

1. Les Etats membres sanctionnent les faits infractionnels prévus par la présente Directive. Les sanctions sont proportionnées et dissuasives.

2. Toute personne morale déclarée responsable au sens de la présente Directive, est passible de peines proportionnées et dissuasives, qui comprennent des amendes pénales et civiles.

Article 29:

Peines complémentaires

1. En cas de condamnation pour une infraction commise par le biais d'un support de communication électronique, la juridiction de jugement compétente peut prononcer des peines complémentaires.

2. En cas de condamnation, la juridiction compétente peut prononcer la confiscation des matériels, des équipements, des instruments, des programmes informatiques ou *des* données ainsi que des sommes ou produits résultant de l'infraction et appartenant au condamné.

3. Les décisions de condamnation sont publiées dans le journal officiel des Etats membres et sur un support électronique aux frais du condamné

CHAPITRE V: REGLES DE PROCEDURE

Article 30:

Perquisition ou accès à un système informatique

Les autorités nationales compétentes peuvent opérer des perquisitions ou saisies ou accéder à tout système informatique pour la manifestation de la vérité

Toutefois, lorsque la saisie du support électronique ne paraît pas souhaitable, les données, de même que celles qui sont nécessaires à la compréhension du système, font l'objet de copies sur des supports de stockage informatique et sont placés sous scellés.

Article 31

Conservation rapide des données informatiques archivées

Si les nécessités de l'information l'exigent et lorsqu'il y a des raisons de craindre la disparition des données informatiques archivées valant preuve, l'autorité compétente fait injonction à toute personne de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, dans un délai déterminé par chaque Etat membre.

Article 32

Mode de preuve:

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 conservé dans des conditions de nature à en garantir l'intégrité.

Article 33

Coopération judiciaire

1. Lorsqu'ils sont saisis par un autre Etat membre, les Etats membres doivent coopérer à la recherche et à la constatation de toutes les infractions pénales prévues ou définies par la présente Directive ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale.

2. Cette coopération est mise en œuvre dans le respect des instruments internationaux pertinents et des mécanismes sur la coopération internationale en matière pénale.

CHAPITRE VI: DISPOSITIONS FINALES

Article 34:

Publication

La présente Directive sera publiée par la Commission dans le Journal Officiel de la Communauté dans les trente (30) jours de sa date de signature par le Président du Conseil des Ministres. Il sera également publié par chaque Etat Membre, dans son Journal Officiel trente (30) jours après que la Commission le lui notifie

Article 35 :

Mise en œuvre

1. Les Etats Membres adoptent les dispositions législatives, réglementaires et administratives

nécessaires pour se conformer à la présente Directive au plus tard le 1er janvier 2014.

2. Lorsque les Etats Membres adoptent les dispositions visées au paragraphe 1 du présent article,

celles-ci contiennent une référence à la présente Directive ou sont accompagnées d'une telle référence lors de leur publication officielle.

3. Les Etats Membres communiquent à la Commission de la CEDEAO les mesures ou dispositions qu'ils adoptent pour se conformer à la présente Directive.

4. Les Etats Membres de la Communauté notifient les difficultés de mise en œuvre de la présente Directive au Président de la Commission qui en fait rapport au Conseil des Ministres, qui, à son tour, prend les mesures appropriées en vue d'assurer la mise en œuvre effective de la présente Directive.

FAIT A ABUJA, LE 19 AOUT 2011

POUR LE CONSEIL, LE PRESIDENT,

…… S.E. OLUGBENGA ASHIRU

Annexe 5 : Acte additionnel A/SA.1/01/10 au Traité CEDEAO relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO

COMMUNAUTE ECONOMIQUE DES ETATS DE L'AFRIQUE DE L'OUEST

ECONOMIC COMMUNITY OF WEST AFRICAN STATES

TRENTE SEPTIEME SESSION DE LA CONFERENCE DES CHEFS D'ETAT ET DE GOUVERNEMENT

Abuja, 16 Février 2010

ACTE ADDITIONNEL A/SA.1/01/10 RELATIF A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS L'ESPACE DE LA CEDEAO

LES HAUTES PARTIES CONTRACTANTES,

VU les Articles 7, 8 et 9 du Traité Révisé de la CEDEAO tel qu'amendé, portant création de la Conférence des Chefs d'Etat et de Gouvernement et définissant sa composition et ses fonctions ;

VU le Protocole Additionnel A/SP.1/06/06 portant amendement du Traité Révisé de la CEDEAO ;

VU l'article 4 paragraphe g dudit Traité qui énonce l'adhésion des Etats Membres au respect, à la promotion et à la protection des droits de l'homme et des peuples conformément aux dispositions de la Charte Africaine des Droits de l'Homme et des Peuples ;

VU les articles 27, 32 et 33 dudit Traité relatifs à la Science et à la Technologie, et aux domaines des Communications et des Télécommunications ;

VU l'article 57 dudit Traité relatif à la coopération judiciaire et juridique qui prescrit que les Etats membres s'engagent à promouvoir la coopération judiciaire en vue d'harmoniser les systèmes judiciaires et juridiques;

VU l'Acte Additionnel A/SA 1/01/07 du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des Politiques et du Cadre Réglementaire du secteur des Technologies de l'Information et de la Communication (TIC) ;

CONSIDERANT les progrès importants réalisés dans les domaines des Technologies de l'Information et de la Communication (TIC) ainsi que de l'Internet dont l'utilisation inappropriée dans la vie quotidienne pose des problèmes relativement à la vie privée et professionnelle des utilisateurs ;

CONSCIENTES qu'une technologie telle que l'Internet et ses facilités de profilage et de traçage des individus constitue un vecteur favorable de collecte et de traitement des données à caractère personnel ;

CONSCIENTES également que l'utilisation croissante des technologies de l'information et de la communication peut être préjudiciable à la vie privée et professionnelle des utilisateurs ;

NOTANT que nonobstant l'existence des législations nationales relatives à la protection de l'intimité des citoyens dans leur vie quotidienne ou professionnelle et à la garantie de la libre circulation des informations, il s'avère important de combler un vide juridique créé par la naissance de ce nouvel instrument de communication qu'est l'Internet ;

CONSCIENTES de la nécessité de combler ce vide juridique et de créer en conséquence un cadre légal harmonisé dans le traitement des données à caractère personnel ;

DESIREUSES d'adopter un Acte Additionnel relatif à la protection des données à caractère personnel ;

APRES AVIS du Parlement de la Communauté en date du 23 Mai 2009;

SUR RECOMMANDATION de la Soixante troisième Session Ordinaire du Conseil des Ministres, tenue à Abuja les 20 et 21 Novembre 2009;

CONVIENNENT DE CE QUI SUIT:

CHAPITRE I

DISPOSITIONS GENERALES

Article 1er **Définitions**

Au sens du présent Acte Additionnel, on entend par :

Autorité de protection : l'autorité nationale administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions du présent Acte additionnel ;

Code de conduite : les chartes d'utilisation élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologué par l'Autorité de protection;

Consentement de la personne concernée: toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique;

Destinataire d'un traitement des données à caractère personnel: toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter les données;

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

Données sensibles : toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites; aux sanctions pénales ou administratives;

Données dans le domaine de la santé: toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques précitées;

Fichier de données à caractère personnel: tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

Interconnexion des données à caractère personnel : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement;

Personne concernée: toute personne physique qui fait l'objet d'un traitement des données à caractère personnel;

Prospection directe : toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services;

Responsable du traitement : personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités;

Sous-traitant: toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement;

Tiers : toute personne physique ou morale, publique ou privée, tout autre organisme ou association autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données.;

Traitement des données à caractère personnel: toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel.

CHAPITRE II:

CADRE JURIDIQUE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 2: Objet

Chaque Etat membre met en place un cadre légal de protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel, sous réserve de la protection de l'ordre public.

Article 3: Champ d'application

Sont soumises aux dispositions du Présent Acte Additionnel:

1) toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;

2) tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'article 4 du présent Acte additionnel;

3) tout traitement mis en œuvre sur le territoire d'un Etat Membre de l'UEMOA ou de la CEDEAO ;

4) tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Article 4: Exclusions

Le présent Acte additionnel ne s'applique pas aux traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques.

CHAPITRE III:

FORMALITES NECESSAIRES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 5: Formalité de déclaration

En dehors des cas prévus aux articles 6, 11 et 12 du présent Acte additionnel, les traitements de données à caractère personnel font l'objet d'une déclaration auprès de l'Autorité de protection.

Article 6: Traitements à caractère personnel pour le compte du service public

Les traitements des données à caractère personnel opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont décidés par acte législatif ou réglementaire pris après avis motivé de l'Autorité de protection.

Ces traitements portent sur:

1) la sûreté de l'Etat, la défense ou la sécurité publique ;

2) la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté;

3) le recensement de la population ;

4) les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;

5) le traitement de salaires, pensions, impôts, taxes et autres liquidations.

Article 7: Formalités de demandes d'avis et d'autorisations

Les demandes d'avis, les déclarations et les demandes d'autorisations doivent préciser :

1) l'identité et l'adresse du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire d'un Etat Membre de la CEDEAO et de l'UEMOA, celles de son représentant dûment mandaté ;

2) la ou les finalités du traitement ainsi que la description générale de ses fonctions ;

3) les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

4) les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5) la durée de conservation des données traitées ;

6) le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7) les destinataires habilités à recevoir communication des données ;

8) la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

9) les dispositions prises pour assurer la sécurité des traitements et des données ;

10) l'indication du recours à un sous-traitant ;

11) les transferts de données à caractère personnel envisagés à destination d'un pays tiers non membre de la CEDEAO ou de l'UEMOA, sous réserve de réciprocité.

Article 8: Délai

L'Autorité de protection se prononce dans un délai fixe à compter de la réception de la demande d'avis ou d'autorisation. Toutefois, ce délai peut être prorogé ou non sur décision motivée de l'Autorité de protection.

Article 9: Voie de l'avis ou de la demande d'autorisation

L'avis, la déclaration ou la demande d'autorisation peut être adressé à l'Autorité de protection par voie postale ou électronique.

Article 10: Exonération de l'obligation de déclaration

Pour les catégories les plus courantes de traitement des données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'Autorité de protection peut établir et publier des normes destinées à simplifier ou à exonérer l'obligation de déclaration.

Article 11: Dispense de formalités

Sont dispensés des formalités préalables prévues aux articles suivants :

1) les traitements mentionnés à l'article 4 du présent Acte additionnel;

2) les traitements ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;

3) les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers.

Article 12: Types de traitements à mettre en ceuvre après autorisation

Sont mis en œuvre après autorisation de l'Autorité de protection:

1) les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;

2) les traitements des données à caractère personnel portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ;

3) les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers, telle que définie à l'article 37 du présent Acte additionnel;

4) les traitements portant sur un numéro national d'identification ou tout autre identifiant de la même nature ;
5) les traitements des données à caractère personnel comportant des données biométriques ;

6) les traitements des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques.

Article 13: Saisine de l'Autorité de protection

L'Autorité de protection peut être saisie par toute personne, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

CHAPITRE IV:

CADRE INSTITUTIONNEL DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 14: Création

1) Dans l'espace CEDEAO, chaque Etat Membre met en place une Autorité de protection des données à caractère personnel. Les Etats Membres qui n'en disposent pas encore sont encouragés à en installer ;

2) L'Autorité de protection est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions du présent Acte additionnel.

Article 15: Composition

Chaque Etat Membre prend les dispositions nécessaires pour déterminer la composition de l'Autorité de protection. Cette autorité est composée de personnalités qualifiées pour leur connaissance en droit, en Informatique, et tout autre domaine de connaissance pour atteindre les objectifs tels que définis à l'article 2 du présent Acte additionnel.

Article 16: Incompatibilité

La qualité de membre d'une autorité de protection est incompatible avec la qualité de membre du Gouvernement, de l'exercice des fonctions de dirigeants d'entreprise, de la détention de participation dans les entreprises du secteur de l'informatique ou des télécommunications.

Article 17: Immunité

1) Les membres d'une Autorité de protection jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction.

2) Dans l'exercice de leur attribution, ils ne reçoivent d'instruction d'aucune autorité.

Article 18: Secret professionnel et règlement intérieur

1) Les membres de l'autorité de protection sont soumis au secret professionnel conformément aux textes en vigueur dans chaque Etat Membre.

2) Chaque Autorité de protection établit un règlement intérieur qui précise notamment les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers.

Article 19: Attributions de l'Autorité de protection des données à caractère personnel

1. L'Autorité de protection s'assure que les TIC ne comportent aucune menace aux libertés publiques et à la vie privée. A ce titre, elle doit :

a) informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;

b) répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;

c) informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;

d) autoriser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;

e) recevoir les formalités préalables à la création de traitements des données à caractère personnel ;

f) recevoir les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci ;

g) informer sans délai l'autorité judiciaire pour certains types d'infractions dont elle a connaissance ;

h) procéder, par le biais d'agents assermentés, à des vérifications portant sur tout traitement des données à caractère personnel ;

i) prononcer des sanctions, administratives et pécuniaires à l'égard d'un responsable de traitement ;

j) mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;

k) conseiller les personnes et organismes qui font les traitements des données à caractère personnel ou qui procèdent à des essais ou expériences ;

l) autoriser les transferts transfrontaliers de données à caractère personnel ;

m) faire des suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;

n) mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel de pays tiers ;

o) participer aux négociations internationales en matière de protection des données à caractère personnel ;

p) établir, selon une périodicité bien définie, un rapport d'activités remis soit au Président de la République, soit au Président de l'Assemblée nationale, soit au Premier ministre, soit au Ministre de la Justice ;

q) requérir des agents assermentés, conformément aux dispositions en vigueur dans les Etats membres de la CEDEAO, en vue de participer à la mise en œuvre des missions de vérification;

2. L'Autorité de protection peut en outre prononcer les mesures suivantes :

a) Un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant des présentes lignes directrices ;

b) une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

3) De même, en cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel entraîne une violation de droits et libertés, l'Autorité de protection, après procédure contradictoire, peut décider:

a) l'interruption de la mise en œuvre du traitement ;

b) le verrouillage de certaines données à caractère personnel traitées ;

c) l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions du présent Acte additionnel.

Article 20: Sanctions

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, l'Autorité de protection peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes:

1) un retrait provisoire de l'autorisation accordée ;

2) le retrait définitif de l'autorisation ;

3) une amende pécuniaire.

Article 21: Recours

Les sanctions et décisions prises par l'Autorité de protection sont susceptibles de faire l'objet d'un recours.

Article 22: Budget

Pour l'accomplissement de ses missions, l'Autorité de protection reçoit une dotation budgétaire de l'Etat.

CHAPITRE V:

PRINCIPES DIRECTEURS DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 23: Principe du consentement et de légitimité

1) Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement.

2) Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire:

a) au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

b) à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

c) à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

d) à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Article 24: Principe de licéité et de loyauté

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Article 25: Principe de finalité, de pertinence, de conservation

1) Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

2) Elles doivent être adéquates et pertinentes au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

3) Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

4) Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Article 26: Principe d'exactitude

Les données collectées doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Article 27: Principe de transparence

Le principe de transparence implique une information obligatoire de la part du responsable du traitement portant sur les données à caractère personnel.

Article 28: Principe de confidentialité et de sécurité

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Article 29: Principe du choix du sous traitant

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect des mesures de sécurité définies par le présent Acte additionnel.

Article 30: Principes spécifiques

Dans l'espace CEDEAO, il est interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Article 31: **Exceptions**

L'interdiction fixée à l'article précédent ne s'applique pas pour les catégories de traitements suivantes lorsque:

1) le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;

2) la personne concernée a donné son consentement par écrit, quel que soit le support, à un tel traitement et en conformité avec les textes en vigueur;

3) le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

4) le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;

5) une procédure judiciaire ou une enquête pénale est ouverte ;

6) le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;

7) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée pendant la période précontractuelle ;

8) le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

9) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;

10) le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Article 32: Le cas du traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche, d'expression artistique ou littéraire

Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche, d'expression artistique ou littéraire, est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique, d'exercice ou à titre professionnel, de l'activité de journaliste ou chercheur, dans le respect des règles déontologiques de ces professions.

Article 33: Application des dispositions des lois relatives à la Presse écrite ou au secteur de l'audiovisuel et du code pénal

Les dispositions du présent Acte additionnel ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

Article 34: Interdiction de prospection directe

Dans l'espace CEDEAO, il est interdit de procéder à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Article 35: **Fondement d'une décision de justice**

1) Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

2) Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Article 36: **Transfert des données à caractère personnel vers un pays non membre de la CEDEAO**

1) Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un pays non membre de la CEDEAO que si cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

2) Avant tout transfert des données à caractère personnel vers ce pays tiers, le responsable du traitement doit préalablement informer l'Autorité de protection.

Article 37: **Interconnexion des fichiers comportant des données à caractère personnel**

L'interconnexion des fichiers visée à l'article 12 du présent Acte additionnel doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements. Elle ne peut pas entrainer de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

CHAPITRE VI:

DROITS DE LA PERSONNE DONT LES DONNEES FONT L'OBJET D'UN TRAITEMENT

Article 38: **Droit à l'information**

Le responsable du traitement doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

1) son identité et, le cas échéant, celle de son représentant;
2) la ou les finalités déterminées du traitement auquel les données sont destinées ;
3) les catégories de données concernées ;
4) le ou les destinataires auxquels les données sont susceptibles d'être communiquées ;
5) le fait de pouvoir demander à ne plus figurer sur le fichier ;
6) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;
7) la durée de conservation des données ;
8) l'éventualité de tout transfert de données à destination de pays tiers.

Article 39: **Droit d'accès**

Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement, sous forme de questions:

1) les informations permettant de connaître et de contester le traitement ;

2) la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

3) la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

4) des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées.

Article 40: **Droit d'opposition**

1) Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

2) Elle a le droit, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Article 41: **Droit de rectification et de suppression**

Toute personne physique peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

CHAPITRE VII:

OBLIGATIONS DU RESPONSABLE DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Article 42: **Les obligations de confidentialité**

Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Article 43: **Les obligations de sécurité**

Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Article 44: **Les obligations de conservation**

Les données à caractère personnel doivent être conservées pendant une durée fixée par un texte réglementaire et uniquement pour les fins en vue desquelles elles ont été recueillies.

Article 45: **Les obligations de pérennité**

1) Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

2) Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

CHAPITRE VIII:

DISPOSITIONS FINALES

Article 46 : **Amendement et révision**

1) Tout Etat Membre, le Conseil des Ministres et la Commission de la CEDEAO peuvent soumettre des propositions en vue de l'amendement ou de la révision du présent Acte Additionnel.

2) Toutes les propositions d'amendement ou de révision sont soumises à la Commission de la CEDEAO qui les communique aux Etats membres trente (30) jours au plus tard après leur réception. Le Conseil des Ministres examine les propositions d'amendements ou de révisions à l'expiration d'un délai de trois (3) mois accordé aux Etats Membres pour émettre leurs observations.

3) Les amendements et révisions sont adoptés par le Conseil des Ministres et soumis à la Conférence des Chefs d'Etat et de Gouvernement pour approbation et signature. Lesdits amendements et révisions entrent en vigueur conformément aux dispositions de l'article 48 du présent Acte additionnel.

Article 47 : Publication

Le présent Acte additionnel est publié par la Commission dans le Journal Officiel de la Communauté dans les trente (30) jours de sa date de signature par la Conférence des Chefs d'Etat et de Gouvernement. Il est également publié par chaque Etat Membre dans son Journal Officiel trente (30) jours après que la Commission le lui notifiera.

Article 48 : Entrée en vigueur

1) Le présent Acte additionnel entre en vigueur dès sa publication dans le Journal Officiel de la Communauté et dans ceux de chaque Etat membre. Le présent Acte additionnel est annexé au Traité de la CEDEAO dont il est partie intégrante.

Article 49 : Autorité dépositaire

Le présent Acte additionnel est déposé à la Commission qui en transmet des copies certifiées conformes à tous les Etats Membres et le fait enregistrer auprès de l'Union Africaine, de l'Organisation des Nations Unies et auprès de toutes organisations régionales et internationales coopérant avec la CEDEAO et désignées par le Conseil, en vertu des articles 83, 84 et 85 du Traité Révisé de la CEDEAO.

EN FOI DE QUOI, NOUS, CHEFS D'ETAT ET DE GOUVERNEMENT DE LA COMMUNAUTE ECONOMIQUE DES ETATS DE L'AFRIQUE DE L'OUEST (CEDEAO), AVONS SIGNE LE PRESENT ACTE ADDITIONNEL.

FAIT A ABUJA, LE 16 FEVRIER 2010

EN UN SEUL ORIGINAL EN ANGLAIS, EN FRANCAIS ET EN PORTUGAIS, LES TROIS (3) TEXTES FAISANT EGALEMENT FOI.

S. E. M. Jean Marie EHOUZOU
Ministre des Affaires Etrangères,
De l'Intégration Africaine, de la Francophonie
Et des Béninois de l'Extérieur
Pour, et par ordre du Président de la
République du Bénin

S. E. M. Blaise COMPAORE
Président du Faso,
Président du Conseil des Ministres

S.E. M. José BRITO
Ministre des Affaires Etrangères
de la Coopération et des Communautés
Pour le Gouvernement
De la République du Cap Vert

S. E. M. Youssouf BAKAYOKO
Ministre des Affaires Etrangères
Pour, et par ordre du Président
de la République de Côte d'Ivoire

S. E. Aja Dr. Isatou NJIE-SAIDY
Vice-Présidente,
Pour, et par ordre du Président
de la République de la Gambie

S. E. M. John ATTA-MILLS
Président et Commandant en Chef
de la République du Ghana

S.E. Malam Bacai SANHA
Président
de la République de Guinée Bissau

S. E. Mme Ellen JOHNSON-SIRLEAF
Présidente de la République du Liberia

Dr. Badara ALOU-MACALOU
Ministre des Maliens de l'Extérieur et
de l'Intégration Africaine
Pour, et par ordre du Président
de la République du Mali

S. E. Dr. Goodluck Ebele JONATHAN
GCON,
Président par Intérim,
Commandant-en-Chef des Forces Armées
de la République Fédérale du Nigeria
Président en exercice de la CEDEAO

S. E. Me Abdoulaye WADE
Président de la République du Sénégal

S. E. M. Ernest Bai KOROMA
Président
de la République de Sierra Leone

S. E. M. Koffi ESAW
Ministre des Affaires Etrangères et
de l'Intégration Régionale
Pour, et par ordre du Président de la République Togolaise

Annexe 6 : Loi n°010-2004 /AN portant protection des données à caractère personnel du Burkina Faso (quelques dispositions)

BURKINA FASO

UNITE-PROGRES-JUSTICE

ASSEMBLEE NATIONALE

IVE REPUBLIQUE

TROISIEME LEGISLATURE

LOI N° 010-2004/AN

PORTANT PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'ASSEMBLEE NATIONALE

VU la Constitution ;

VU la résolution n°001-2002/AN du 05 juin 2002, portant validation du mandat des députés ;

a délibéré en sa séance du 20 avril 2004 et adopté la loi dont la teneur suit :

TITRE I : DISPOSITIONS GENERALES

Chapitre 1 : Définitions

Article 1 :

La présente loi a pour objet de protéger, au Burkina Faso, les droits des personnes en matière de traitement de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables.

Article 2 :

Constitue une donnée à caractère personnel, toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques propres à leur identité physique, psychologique, psychique, économique, culturelle ou sociale.

Article 3 :

Est dénommé traitement de données à caractère personnel, toute opération ou ensemble d'opérations effectuées à l'aide de procédés automatisés ou non par une personne physique ou morale, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction.

Article 4 :

Le responsable du traitement est la personne physique ou morale, publique ou privée, qui a le pouvoir de décider de la création des données à caractère personnel

Le destinataire d'un traitement de données à caractère personnel est toute personne physique ou morale, publique ou privée, autre que la personne concernée, habilitée à recevoir communication de ces données.

La personne concernée est la personne identifiable à laquelle se rapportent les données à caractère personnel.

Chapitre 2 : Principes fondamentaux

Article 5 .

Tout traitement de données à caractère personnel doit avoir reçu le consentement de la ou des personnes concernée(s), sauf dérogations prévues par la loi

Article 6 :

Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements, automatisés ou non, dont les résultats lui sont opposés

Article 7 :

Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéresse destiné à évaluer certains aspects de sa personnalite.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain, ne peut avoir pour seul fondement un traitement automatisé d'informations, donnant une définition du profil ou de la personnalité de l'intéressé

Chapitre 3 : Champ d'application

Article 8 :

La présente loi s'applique aux traitements automatisés ou non de données à caractere personnel contenues ou appelees a figurer dans les fichiers dont le responsable est établi sur le territoire du Burkina Faso, ou, sans y être établi, recourt à des moyens de traitement situés sur le territoire du Burkina Faso, a l'exclusion des données qui ne sont utilisées qu'à des fins de transit.

Article 9 :

Les dispositions de la présente loi ne s'appliquent pas aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique en vue du stockage automatique intermédiaire et transitoire des données à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations

Article 10 :

Les traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de la présente loi, à l'exception des articles 5, 13, 18, 20

L'examen de la demande de mise en œuvre de ces traitements par l'Autorité de contrôle prévue au titre III ci-dessous, est subordonné à l'avis favorable du Comité d'Ethique pour la recherche en santé.

Article 11 :

Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients ne sont pas soumis aux dispositions de la présente loi. Il en va de même des traitements permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinees à leur usage exclusif

TITRE II : MISE EN ŒUVRE DES TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

Chapitre 1 : Conditions générales

Article 12

Le responsable du traitement de données a caractère personnel a l'obligation de collecter et de traiter les données de manière loyale, licite et non frauduleuse

Article 13 :

Le responsable du traitement de données à caractère personnel a l'obligation d'informer la personne concernée de la finalité du traitement, des destinataires des données, du caractère obligatoire ou facultatif des réponses aux questions posées ainsi que des conséquences éventuelles d'un défaut de réponse

Ces dispositions ne s'appliquent pas à la collecte de données nécessaires a la constatation d'une infraction.

Article 14 :

Le traitement de données à caractère personnel ne peut se faire que dans les conditions suivantes :

- les données doivent être collectées pour des finalités déterminées, explicites et légitimes. En conséquence, les données ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées ;
- les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;
- les données doivent être conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées ou traitées. Au-delà de la durée nécessaire, les données ne peuvent être conservées sous une forme nominative qu'en vue de leur traitement à des fins historiques, statistiques ou de recherche.

Article 15 :

Le responsable du traitement doit mettre en œuvre toutes mesures techniques et d'organisation appropriées afin de préserver la sécurité des données, notamment protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé.

Article 16 :

Si une information a été transmise par erreur à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par l'Autorité de contrôle.

Les personnes concernées ont le droit de s'opposer, pour des raisons légitimes, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement.

Ce droit ne s'applique pas aux traitements désignés par acte réglementaire, prévu à l'article 18 ci-dessous.

Article 17 :

Les personnes concernées ont le droit de connaître les données conservées qui les concernent. Elles doivent pouvoir exercer ce droit sans délai ou frais excessifs

Lorsque l'exercice du droit d'accès s'applique à des informations à caractère médical, celles-ci ne peuvent être communiquées à l'intéressé que par l'intermédiaire d'un médecin qu'il désigne à cet effet.

S'il s'avère que des données sont incomplètes ou inexactes, les personnes concernées peuvent en demander la correction ou la rectification. Dans ce cas, le responsable du traitement est tenu de faire la correction ou la rectification et délivrer sans frais, copie de l'enregistrement modifié.

En ce qui concerne les traitements intéressant la sûreté de l'Etat, la défense, et la sécurité publique, la demande est adressée à l'Autorité de contrôle qui désigne un de ses membres relevant de la magistrature, pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de l'Autorité de contrôle. Il est notifié au requérant qu'il a été procédé aux vérifications et aux modifications éventuelles.

Article 18 :

Hormis le cas où ils doivent être autorisés par la loi, les traitements automatisés de données à caractère personnel opérés pour le compte de l'Etat, d'un établissement public, d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public, sont décidés par décret après avis conforme motivé de l'Autorité de contrôle prévue au titre III ci-dessous.

En cas d'avis défavorable de l'Autorité de contrôle, un recours peut être exercé devant le Conseil d'Etat.

Article 19 :

Les traitements de données à caractère personnel effectués pour le compte de personnes autres que celles soumises aux dispositions de l'article 18 ci-dessus, doivent préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de l'Autorité de contrôle.

Chapitre 2 : Dispositions particulières à certaines catégories de données

Article 20 :

Sauf dérogation prévue par la loi, il est interdit de collecter ou de traiter sans le consentement exprès de la personne concernée, des données à caractère personnel qui sont relatives à la santé de celle-ci ou qui font apparaître les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale ou les mœurs.

Article 21 :

Un traitement de données à caractère personnel peut être fait sans le consentement de la personne concernée, dans les cas suivants :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à la sauvegarde de la vie de la personne concernée ou de celle d'un tiers ;
- le traitement porte sur des données rendues publiques par la personne concernée ;

- le traitement est nécessaire, soit à l'exécution d'un contrat auquel la personne concernée est partie, soit à des mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire à la constatation d'une infraction, d'un droit, à l'exercice ou à la défense d'un droit en justice ;
- les traitements nécessaires aux fins de médecine préventive, de diagnostics médicaux, d'administration de soins ou de traitements, de gestion des services de santé, à condition qu'ils soient mis en œuvre par un membre d'une profession de la santé ou par une autre personne à laquelle s'impose, en raison de ses fonctions, le secret professionnel.

Article 22 .

Peuvent seuls procéder au traitement des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté :

- les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ;
- les personnes morales gérant un service public, après avis conforme de l'Autorité de contrôle ,
- les auxiliaires de justice, pour les strictes besoins de l'exercice des missions qui leur sont confiées.

Article 23 :

Toute divulgation ou exploitation commerciale des données de santé à caractère personnel est interdite.

Article 24 :

La transmission entre le territoire burkinabé et l'étranger, sous quelque forme que ce soit, de données à caractère personnel faisant l'objet d'un traitement automatisé régi par l'article 19 ci-dessus, ne peut être effectuée que si la transmission se fait dans le respect de la protection assurée par la présente loi.

Toutefois, en cas de circonstance exceptionnelle, la transmission peut être autorisée par décret après avis conforme de l'Autorité de contrôle

Article 25 ·

Les dispositions des articles 20, 22 et 24 ne s'appliquent pas aux données à caractère personnel traitées par les organes de presse écrite ou audiovisuelle dans le cadre des lois qui les régissent, si leur application aurait pour effet de limiter l'exercice de la liberté d'expression.

TITRE III : AUTORITE DE CONTROLE

Chapitre 1 : Création, composition et organisation

Article 26 :

Il est créé, une Autorité de contrôle dénommée Commission de l'informatique et des libertés (CIL) ci-après désignée la Commission. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations et en contrôlant les applications de l'informatique aux traitements des données à caractère personnel.

A cet effet, la Commission dispose d'un pouvoir réglementaire et d'un pouvoir de sanction qui seront précisés par décret.

Article 27 :

La Commission de l'informatique et des libertés est une autorité administrative indépendante.

Elle est composée de neuf (09) membres ainsi qu'il suit :

- un magistrat, membre du Conseil d'Etat, élu par ses pairs en assemblée générale ;
- un magistrat, membre de la Cour de cassation, élu par ses pairs en assemblée générale ,
- deux députés désignés par le Président de l'Assemblée nationale ;
- deux personnalités désignées par les associations nationales oeuvrant dans le domaine des droits humains ;
- deux personnalités désignées par les associations nationales de professionnels de l'informatique ;
- une personnalité désignée par le Président du Faso en raison de sa compétence.

Les membres de la Commission de l'informatique et des libertés sont nommés par décret en Conseil des ministres.

Article 28 .

Le mandat des membres de la Commission est de cinq (05) ans renouvelable une fois. A l'exception du président, les membres de la Commission n'exercent pas de fonction à titre permanent.

Les membres de la Commission sont inamovibles pendant la durée de leur mandat

Il ne peut être mis fin aux fonctions de membre qu'en cas de démission, d'empêchement constaté par la Commission dans les conditions qu'elle définit ou de faute grave

Les membres de la Commission sont soumis au secret professionnel conformément aux textes en vigueur.

Article 29 :

Le Président du Faso nomme, parmi les membres de la Commission de l'informatique et des libertés, le président de la Commission. Le président est secondé par un vice-président élu par la Commission.

Le président exerce ses fonctions à titre permanent jusqu'à l'épuisement de son mandat de membre de la Commission

Article 30 :

La qualité de membre de la Commission est incompatible :

- avec la qualité de membre du Gouvernement ,
- avec les fonctions de dirigeants d'entreprise concourant à la fabrication de matériel utilisé en informatique ou en télécommunication, à la fourniture des services en informatique ou en télécommunication ;
- avec la détention de participation dans les entreprises ci-dessus citées.

Article 31 :

Si en cours de mandat, le président ou un membre de la Commission cesse d'exercer ses fonctions, il est procédé à son remplacement dans le respect des formes et quotas définis aux articles 27 et 29.

Le mandat du successeur ainsi désigné est limité a la période restant à courir

Article 32 :

Les membres de la Commission, avant leur entrée en fonction, prêtent devant la Cour d'appel de Ouagadougou siégeant en audience solennelle, le serment dont la teneur suit : « Je jure solennellement de bien et fidèlement remplir ma fonction de membre de la Commission de l'informatique et des libertés, en toute indépendance et impartialité, de façon digne et loyale et de garder le secret des délibérations »

Articles 33 :

Les membres de la Commission jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.

Dans l'exercice de leurs attributions, les membres de la Commission ne reçoivent d'instruction d'aucune autorité.

Les informaticiens appelés, soit à donner des renseignements à la Commission, soit à témoigner devant elle, sont déliés en tant que de besoin de leur obligation professionnelle de discrétion

Article 34 :

Les membres de la Commission perçoivent des indemnités fixées par décret en Conseil des ministres.

Article 35 :

Les crédits nécessaires à la Commission pour l'accomplissement de sa mission sont financés par le budget de l'Etat ou par toute autre ressource qui pourrait lui être affectée.

La Commission ne peut recevoir de financement d'un individu, d'un organisme ou d'un Etat étranger que par l'intermédiaire des structures de coopération du Burkina Faso.

Toutefois, l'accomplissement de certaines formalités prévues aux articles 17, 18, 19 et 41 de la présente loi peuvent donner lieu à la perception de redevance.

Article 36 :

La Commission jouit de l'autonomie de gestion.

Le président de la Commission est l'ordonnateur du budget. Il applique les règles de gestion de la comptabilité publique.

Le contrôle des comptes financiers de la Commission relève de la Cour des comptes.

Chapitre 2 : Attributions de la Commission de l'informatique et des libertés

Article 37 :

Pour l'exercice de sa mission, la Commission :

a- prend des décisions individuelles ou réglementaires dans les cas prévus par la présente loi ;

b- peut, par décision particulière, charger un ou plusieurs de ses membres ou de ses agents, assistés le cas échéant d'experts, de procéder, à l'égard de tout traitement de données, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission ;

c- édicte, le cas échéant, des règles types en vue d'assurer la sécurité des systèmes ; en cas de circonstances exceptionnelles, elle peut prescrire des mesures de sécurité consistant notamment en la destruction des supports d'information ou en la suspension de l'autorisation ;

d- adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance ;

e- veille à ce que les modalités de mise en œuvre du droit d'accès et de rectification indiqué dans les actes et déclarations prévus aux articles 18 et 19 n'entravent pas le libre exercice de ce droit ;

f- reçoit les réclamations, pétitions et plaintes ,

g- se tient informée des activités industrielles, de services qui concourent à la mise en œuvre de l'informatique ,

h- se tient informée des effets de l'utilisation de l'informatique sur le droit à la protection de la vie privée, l'exercice des libertés et le fonctionnement des institutions democratiques ,

i- conseille les personnes et organismes qui ont recours au traitement automatisé d'informations nominatives ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements ;

j- répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions ;

k- propose au Gouvernement toutes mesures législatives ou reglementaires de nature à adapter la protection des libertés à l'évolution des procédés et techniques informatiques.

Article 38

Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de fichiers nominatifs doivent prendre toutes mesures utiles afin de faciliter la tâche de la Commission. Ils ne peuvent s'opposer à son action pour quelque motif que ce soit

Article 39

La Commission peut charger le président ou le vice-président d'exercer ses attributions en ce qui concerne l'application des articles 19 et 37 (d, e et f)

Article 40

La Commission de l'informatique et des libertés veille à ce que les traitements automatises ou non, publics ou prives, d'informations nominatives soient effectués conformement aux dispositions de la loi Elle peut prendre toutes mesures utiles a cet effet.

Article 41

Pour les categories les plus courantes de traitement de données à caractere public ou privé qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertes, la Commission etablit et publie des normes simplifiees inspirees des caracteristiques mentionnées à l'article 42 ci-dessous.

Pour les traitements de données répondant à ces normes, seule une déclaration simplifiée de conformité à l'une de ces normes est déposée auprès de la Commission Sauf décision particulière de celle-ci, le récépissé de déclaration est délivré sans délai. Dès réception de ce récépissé le demandeur peut mettre en œuvre le traitement de données. Il n'est exonéré d'aucune de ses responsabilités.

Article 42 :

La demande d'avis ou la déclaration doit préciser :

a- la personne qui présente la demande et celle qui a pouvoir de décider la création du traitement de données ou, si elle réside à l'étranger, son représentant au Burkina Faso ;

b- les caractéristiques, la finalité et s'il y a lieu, la dénomination du traitement de données ;

c- le service ou les services chargés de mettre en œuvre celui-ci ,

d- le service auprès duquel s'exerce le droit d'accès ainsi que les mesures prises pour faciliter l'exercice de ce droit ;

e- les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées ;

f- les informations nominatives traitées, leur origine et la durée de leur conservation ainsi que leurs destinataires ou catégories de destinataires habilités à recevoir communication de ces informations ;

g- les rapprochements, interconnexions ou toute autre forme de mise en relation de ces informations ainsi que leur cession à des tiers ;

h- les dispositions prises pour assurer la sécurité des traitements de données et des informations et la garantie des secrets protégés par la loi ;

i- si le traitement de données est destiné a l'expédition d'informations nominatives entre le territoire burkinabé et l'étranger sous quelque forme que ce soit, y compris lorsqu'il est l'objet d'opérations partiellement effectuées sur le territoire burkinabé à partir d'opérations antérieurement réalisées hors du Burkina Faso

Article 43 .

L'acte réglementaire prévu pour les traitements de données régis par l'article 18 ci-dessus précise notamment :

- la dénomination et la finalité du traitement de données ,
- le service aupres duquel s'exerce le droit d'accès ,
- les catégories d'informations nominatives enregistrées ainsi que les destinataires ou catégories de destinataires habilités a recevoir communication de ces informations

Des décrets peuvent disposer que les actes réglementaires relatifs à certains traitements de données intéressant la sûreté de l'Etat, la défense et la sécurité publique ne seront pas publiés.

Article 44 :

La Commission met à la disposition du public la liste des traitements de données, qui précise pour chacun d'eux :

- la loi ou l'acte réglementaire décidant de sa création ou la date de sa déclaration ;
- sa dénomination et sa finalité ;
- le service auprès duquel est exercé le droit d'accès ,
- les catégories d'informations nominatives enregistrées ainsi que les destinataires ou catégories de destinataires habilités à recevoir communication de ces informations.

Sont tenus à la disposition du public, dans les conditions fixées par décret, les décisions, avis ou recommandations de la Commission dont la connaissance est utile à l'application ou à l'interprétation de la présente loi.

Article 45 :

La Commission présente chaque année au Président du Faso, au Président de l'Assemblée nationale et au Président du Conseil constitutionnel, un rapport rendant compte de l'exécution de sa mission. Ce rapport est rendu public.

TITRE IV : SANCTIONS PENALES

Article 46 :

Le fait de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni d'un emprisonnement de trois (03) mois à cinq (05) ans et d'une amende de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA.

Article 47 .

Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité desdites informations, notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni d'un emprisonnement de trois (03) mois à cinq (05) ans et de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA d'amende

Article 48 :

Le fait de communiquer à des tiers non autorisés ou d'accéder sans autorisation ou de façon illicite aux données à caractère personnel est puni d'une peine d'emprisonnement de trois (03) mois à cinq (05) ans et de un million (1 000 000) à trois millions (3 000 000) de francs CFA d'amende.

Article 49 :

Est puni d'un emprisonnement de trois (03) mois à cinq (05) ans et de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA d'amende, le détournement de finalité d'une collecte ou d'un traitement de données à caractère personnel.

Article 50 :

Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré son opposition, lorsque cette opposition est fondée sur des raisons légitimes, est puni de trois (03) mois à cinq (05) ans d'emprisonnement et de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA d'amende.

En cas de traitement automatisé de données nominatives ayant pour fin la recherche dans le domaine de la santé, est puni des mêmes peines le fait de procéder à un traitement de données :

1. sans avoir préalablement informé individuellement les personnes concernées de leur droit d'accès, de rectification et d'opposition, de la nature des informations transmises et des destinataires des données ;
2. malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou, s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 51 :

Hors les cas prévus par la loi, le fait de mettre ou de conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales, ethniques ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes est puni de trois (03) mois à cinq (05) ans d'emprisonnement et de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté.

Article 52 :

Le fait, sans l'accord de la Commission de l'informatique et des libertés, de conserver des informations sous une forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration préalable à la mise en œuvre du traitement informatisé est puni de trois (03) mois à cinq (05) ans d'emprisonnement et de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA d'amende.

Article 53 :

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à l'honneur et à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir, est puni de trois (03) mois à cinq (05) ans d'emprisonnement et de un million (1 000 000) à trois millions (3 000 000) de francs CFA d'amende.

La divulgation prévue à l'alinéa precédent est punie de trois (03) mois à cinq (05) ans d'emprisonnement et de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA d'amende lorsqu'elle a ete commise par imprudence ou négligence.

Dans les cas prevus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit

Article 54 :

Est puni d'un emprisonnement de un (01) mois à un (01) an et de deux cent mille (200 000) a un million (1 000 000) de francs CFA d'amende, le fait d'entraver l'action de la Commission :

- soit en s'opposant aux vérifications sur place ,
- soit en refusant de communiquer à ses membres ou a ses agents, les renseignements et documents utiles a la mission qui leur est confiée ou en dissimulant ou en faisant disparaître lesdits documents ,
- soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements au moment où la demande a été formulée ou qui ne les présentent pas sous une forme directement intelligible

Article 55

Les dispositions des articles 46 a 54 sont applicables aux fichiers non automatisés ou mecanographiques dont l'usage ne releve pas exclusivement de l'exercice du droit a la vie privee

TITRE V : DISPOSITIONS DIVERSES

Article 56 .

Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données nominatives qu'ils détiennent dans le cadre d'un traitement automatisé de données autorisé par la Commission

Lorsque ces données permettent l'identification des personnes, elles doivent être codées avant leur transmission. Toutefois, il peut être dérogé à cette obligation lorsque le traitement de données est associé a des études de pharmacovigilance ou à des protocoles de recherche réalisés dans le cadre d'études coopératives nationales ou internationales ; il peut également y être derogé si une particularité de la recherche l'exige La demande d'autorisation comporte la justification scientifique et technique de la dérogation et, sauf autorisation motivée de la Commission donnee après avis du Comite d'éthique pour la recherche en santé, les données transmises ne peuvent être conservées sous une forme nominative au-delà de la duree nécessaire à la recherche.

La présentation des résultats du traitement de données ne doit en aucun cas permettre l'identification directe des personnes concernées

Les données sont reçues par le responsable de la recherche désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre leur traitement Ce responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci

Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel

Article 57 :

Les dispositions des articles 12, 13, 15, 18, 19, 22 et 25 relatives à la collecte, a l'enregistrement et à la conservation des donnees a caractere personnel sont applicables aux fichiers non automatises ou mécanographiques autres que ceux dont l'usage relève du strict exercice du droit à la vie privee

Article 58 :

Les dispositions de la présente loi ne font pas obstacle à celles de la loi n° 040/96/ADP du 08 novembre 1996, portant obligation de reponse et de secret statistique.

TITRE VI : DISPOSITIONS TRANSITOIRES ET FINALES

Article 59 :

A titre transitoire, les traitements de données régis par l'article 18 ci-dessus et déjà créés, ne sont soumis qu'à une déclaration auprès de la Commission dans les conditions prévues à l'article 42.

La Commission peut toutefois, par décision spéciale, faire application des dispositions de l'article 18 et fixer le délai au terme duquel l'acte réglementant le traitement de données doit être pris.

Article 60 :

A compter de la promulgation de la présente loi, tous les traitements de données devront répondre aux prescriptions de cette loi, dans les délais ci-après :

- trois (03) ans pour les traitements de données régis par l'article 18,
- six (06) mois pour les traitements de données régis par l'article 19.

Article 61 :

Des décrets pris en Conseil des ministres détermineront les modalités d'application de la présente loi.

Article 62 :

La présente loi qui abroge toutes dispositions antérieures contraires sera exécutée comme loi de l'Etat.

Ainsi fait et délibéré en séance publique
à Ouagadougou, le 20 avril 2004

Pour le Président de l'Assemblée nationale,
Le Deuxième Vice-Président

Dimfangodo Salifou SAWADOGO

Le Secrétaire de séance

Mamadou Christophe OUATTARA

Annexe 7 : Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la Cybercriminalité en Côte - d'Ivoire

Journal Officiel de la République de Côte-d'Ivoire du 12 Août 2013

PARTIE NON OFFICIELLE

PARTIE OFFICIELLE

ACTES PRESIDENTIELS

PRESIDENCE DE LA REPUBLIQUE

LOI n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.

CHAPITRE 1 : Définitions

L'ASSEMBLEE NATIONALE a adopté,

LE PRESIDENT DE LA REPUBLIQUE promulgue la loi dont la teneur suit :

Article premier. — Les définitions des instruments juridiques de la CEDEAO, de l'Union africaine ou de l'Union Internationale des Télécommunications prévalent pour les termes non définis par la présente loi.

Au sens de la présente loi, on entend par :

cybercriminalité, l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou un système d'information ;

atteinte à la dignité humaine, toute atteinte, hors les cas d'attentat à la vie, d'atteinte à l'intégrité ou à la liberté, qui a pour effet essentiel de traiter la personne comme une chose, comme un animal ou comme un être auquel serait dénié tout droit ;

communication électronique, toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen ;

données à caractère personnel, toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

données informatiques ou données, toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information ;

données relatives aux abonnés, toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir sur la base d'un contrat ou d'un arrangement de services :

— le type de service de communication, les dispositions techniques prises à cet égard et la période de service ;

— l'identité, l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de communication ;

données relatives au trafic, toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

données sensibles, toutes données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

infrastructures critiques, les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique et social des citoyens ou encore le fonctionnement continu des services de l'Etat ;

mineur, toute personne âgée de moins de dix-huit ans, conformément au Code pénal ;

pays tiers, tout Etat non membre de la CEDEAO ;

personne concernée, toute personne physique qui fait l'objet d'un traitement de données à caractère personnel ;

pornographie infantile, toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un enfant de moins de dix-huit ans se livrant à un agissement sexuellement explicite ou des images représentant un enfant de moins de quinze ans se livrant à un comportement sexuellement explicite ;

racisme et xénophobie en matière des TIC, 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 où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ;

SMS, le sigle anglo-saxon signifiant « short message service » (en français : service de message court) ;

surveillance, toute activité faisant appel à des moyens techniques ou électroniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ;

système d'information ou 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.

CHAPITRE 2

Objet et champ d'application

Art. 2. — La présente loi a pour objet de lutter contre la cybercriminalité.

Art. 3. — Sont soumis aux dispositions de la présente loi, les infractions relatives à la cybercriminalité, ainsi que les infractions pénales dont la constatation requiert la collecte d'une preuve électronique.

CHAPITRE 3

Infractions spécifiques aux technologies de l'information et de la communication

Art. 4. — Est puni de un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information.

Art. 5. — Est puni de un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système d'information.

Art. 6. — Est puni de un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information.

Art. 7. — Est puni de un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque introduit ou tente d'introduire frauduleusement des données dans un système d'information.

Art. 8. — Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information.

Art. 9. — Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques.

Art. 10. — Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque produit ou fabrique un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Art. 11. — Est puni de un à cinq ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque fait usage, en connaissance de cause, de données informatiques frauduleusement obtenues.

Art. 12. — Est puni de un à cinq ans d'emprisonnement et de 30.000.000 à 50.000.000 de francs CFA d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte au système d'information.

Art. 13. — Est puni de un an à deux ans d'emprisonnement et de 10.000.000 à 50.000.000 de francs CFA d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

— un équipement, un dispositif ou un programme informatique ;

— un mot de passe, un code d'accès ou des données informatiques similaires.

Art. 14. — Est puni de dix à vingt ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi. L'infraction ci-dessus définie est un délit.

Art. 15. — Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Art.16. — Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Art. 17. — Est puni de un à trois ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques.

Art. 18. — Est puni de un à cinq ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Art. 19. — Est puni de deux à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque utilise frauduleusement un ou des éléments d'identification d'une personne physique ou morale par le biais d'un système d'information.

Quiconque utilise, possède, offre, vend, met à disposition, transmet en toute connaissance de cause de fausses données d'identification est puni de deux ans à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende.

Quiconque réalise ou tente de réaliser de fausses données d'identification est puni de deux à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende.

Art. 20. — Est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 10.000.000 à 100.000.000 de francs CFA, quiconque ne respecte pas l'interdiction d'exercer la profession de prestataire de cryptologie ou l'obligation de retrait des moyens de cryptologie.

Art. 21. — Est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 10.000.000 de francs CFA, quiconque procède à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable par écrit à recevoir de telles prospections.

Art. 22. — Est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 10.000.000 de francs CFA, quiconque utilise des procédés illicites d'envoi de messages électroniques non sollicités sur la base de la collecte de données à caractère personnel.

Art. 23. — Est puni d'une peine d'emprisonnement de un mois à un an et d'une amende de 500.000 à 1.000.000 de francs, quiconque dissimule l'identité de la personne pour le compte de laquelle une offre commerciale est émise ou mentionne une offre sans rapport avec la prestation ou le service proposé.

Art. 24. — Est puni d'une peine d'emprisonnement de un à cinq ans et de 5.000.000 à 100.000.000 de francs CFA d'amende, quiconque procède au traitement de données à caractère personnel par un moyen frauduleux, déloyal ou illicite.

La peine d'amende ne peut être inférieure à 10.000.000 de francs CFA lorsque le traitement frauduleux, déloyal ou illicite a été faite en vue de l'envoi de messages électroniques non sollicités par une personne morale, autre que l'Etat.

Art. 25. — Est puni d'une peine d'emprisonnement d'un an à cinq ans et d'une amende de 5.000.000 à 100.000.000 de francs CFA, quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site Internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles.

La peine d'emprisonnement ne peut être inférieure à cinq ans et la peine d'amende ne peut être inférieure à 20.000.000 de francs CFA, lorsque les données à caractère personnel ou les informations confidentielles communiquées ont servi au détournement de fonds publics ou privés.

Art. 26. — Quiconque prend frauduleusement connaissance d'une information à l'intérieur d'un système d'information électronique, ou copie frauduleusement une information à partir d'un tel système, ou encore soustrait frauduleusement le support physique sur lequel se trouve une information, est coupable de vol d'information.

Quiconque commet un vol d'information est puni d'un emprisonnement de cinq à dix ans et de 3.000.000 à 5.000.000 de francs d'amende.

La tentative est punissable.

L'infraction ci-dessus définie est un délit.

Art. 27. — La peine est d'un emprisonnement de dix à vingt ans et d'une amende de 5.000.000 à 10.000.000 de francs CFA si le vol d'information ou la tentative de vol d'information a été commis accompagné d'une au moins des circonstances ci-après :

— avec des violences ayant entraîné des blessures ;

— avec effraction, escalade ou usage de fausse clé ;

— en réunion par au moins deux personnes ;

— avec usage frauduleux, soit d'un uniforme ou d'un costume d'un fonctionnaire public, civil ou militaire, soit d'un titre d'un fonctionnaire, soit d'un faux ordre d'une autorité civile ou militaire ;

— dans une maison habitée ou servant d'habitation ou dans les locaux professionnels ;

— avec l'usage d'un masque ;

— avec l'usage d'un véhicule pour faciliter son entreprise ou sa fuite ;

— la nuit.

Art. 28. — Le vol d'information ou la tentative de vol d'information est puni de vingt ans d'emprisonnement et de 10.000.000 de francs CFA d'amende, s'il est accompagné de l'une des circonstances ci-après :

— lorsque l'auteur ou le complice est porteur d'une arme apparente ou cachée ;

— lorsque l'auteur ou le complice a fait usage d'une arme ayant entraîné des blessures ou la mort de la victime.

Art. 29. — Lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles.

Art. 30. — Lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement.

Art. 31. — Est puni d'un emprisonnement de un à cinq ans et de 1.000.000 de francs CFA d'amende, quiconque de mauvaise foi, ouvre, supprime, retarde ou détourne des correspondances électroniques arrivées ou non à destination et adressées à un tiers, ou en prend frauduleusement connaissance.

Est puni des mêmes peines, quiconque de mauvaise foi, intercepte, détourne, utilise ou divulgue des correspondances électroniques émises, transmises ou reçues par la voie des télécommunications ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions.

Art. 32. — Les personnes condamnées pour les délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

— l'interdiction, pour une durée de cinq ans, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

— la confiscation du moyen qui a servi à commettre l'infraction ou qui était destiné à la commission de l'infraction ou du bien qui en est le produit ;

— la fermeture, pour une durée de cinq ans s'il y a lieu, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

— l'exclusion, pour une durée de cinq ans, des marchés publics ;

— l'interdiction, pour une durée de cinq ans, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

— l'affichage ou la diffusion de la décision prononcée, aux frais du condamné.

CHAPITRE 4

Atteintes à la propriété intellectuelle

Art. 33. — Sont punies d'une peine d'emprisonnement de un à dix ans et d'une amende de 500.000 à 100.000.000 de francs CFA, les atteintes à la propriété intellectuelle commises au moyen d'un système d'information.

Constitue une atteinte à la propriété intellectuelle :

— le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de représenter ou de mettre à la disposition du public sur un système d'information ou un support numérique ou analogique, intégralement ou partiellement une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin ;

— le fait, sans autorisation de l'auteur ou de ses ayants droit, de traduire ou d'adapter une œuvre de l'esprit par le biais d'un programme informatique ou de mettre cette traduction ou adaptation sur un système d'information ou un support numérique ou analogique à la disposition du public ;

— le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénaturer, de dénigrer une marque, une raison sociale, un nom commercial, un nom de domaine Internet ou tout autre signe distinctif appartenant à un tiers par le biais d'un système d'information ouvert au public ou par le biais d'un programme informatique ou sur un support numérique ou analogique ;

— le fait, en toute connaissance de cause, d'exploiter par reproduction ou par représentation une œuvre de l'esprit mise de façon illicite à disposition du public sur un réseau de communication électronique ;

— le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un bien ou un produit protégé par un brevet d'invention.

Art. 34. — Ne constituent pas une atteinte à la propriété intellectuelle lorsqu'elles sont réalisées par le biais d'un système ou un programme informatique ou électronique :

— les copies ou reproductions d'œuvres de l'esprit strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exclusion des copies des œuvres d'art destinées à être utilisées pour des fins identiques ou similaires à celles pour lesquelles l'œuvre originale a été créée ;

— les analyses et courtes citations, sous réserve que soient clairement indiqués le nom de l'auteur de l'œuvre et de la source, justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées ;

— la parodie et la caricature de l'œuvre originale réalisée sans intention de nuire à l'image et à l'honorabilité de l'auteur de ladite œuvre ;

— les copies ou reproductions provisoires présentant un caractère transitoire et accessoire lorsqu'elles sont une partie intégrante et essentielle d'un procédé technique et qu'elles ont pour objet de permettre la transmission ou l'utilisation licite de l'œuvre sur un système d'information ou électronique ;

— la reproduction et la représentation réalisée à des fins non lucratives par des personnes morales de droit public et par des établissements ouverts au public, tels que les bibliothèques, les services d'archives, les musées, les centres de documentation et les espaces culturels multimédias, en vue d'une consultation strictement personnelle de l'œuvre par des personnes atteintes d'une ou de plusieurs déficiences des fonctions motrices, physiques, sensorielles, mentales, cognitives ou psychiques dont le niveau d'incapacité est reconnu dans un certificat médical dûment établi ;

— la reproduction d'une œuvre, effectuée à des fins de conservation ou destinée à préserver les conditions de sa consultation sur place par des bibliothèques accessibles au public, par des musées ou par des services d'archives, sous réserve que ceux-ci ne recherchent aucun avantage économique ou commercial ;

— la reproduction et la représentation d'œuvre de l'esprit réalisée à des fins exclusivement pédagogiques par les enseignants et les chercheurs dans le cadre strict de leurs enseignements ou de leurs recherches pour leurs élèves et étudiants ou pour d'autres enseignants et chercheurs directement concernés, sous réserve que cette reproduction ou représentation ne donne lieu à aucune exploitation commerciale ou lucrative.

Art. 35. — L'auteur d'une œuvre de l'esprit ou ses ayants droit peuvent faire obstacle à la copie de l'œuvre en limitant le droit de copie reconnue par la présente loi, notamment, par la mise en œuvre de mesures techniques de protection lorsque la mise en œuvre du droit de copie porte atteinte à l'exploitation normale de l'œuvre ou cause un préjudice injustifié aux intérêts de l'auteur.

On entend par mesure technique de protection, toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction de contrôle des utilisations de l'œuvre ou de limitation des copies de l'œuvre considérée.

L'usager doit être clairement informé de l'existence des mesures techniques de protection sur l'œuvre qu'il acquiert ou utilise et sur les fonctions de ces mesures techniques, notamment si elles interdisent ou non l'usage de l'œuvre sur d'autres systèmes d'information ou d'exploitation.

Art. 36. — Le titulaire d'un service d'accès à internet ou à tout réseau de communication électronique est tenu de veiller à ce que cet accès ne soit pas utilisé à des fins manifestement illicites, notamment de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation de leurs auteurs ou leurs ayants droit. En cas de non-respect de cette obligation, il peut être poursuivi pour complicité par fourniture de moyen.

CHAPITRE 5

Agissements illicites sur les réseaux de communication électronique

Art. 37. — L'organisation des jeux d'argent sur les réseaux de communication électronique est placée sous un régime de droits exclusifs de l'Etat concédés à un nombre restreint d'opérateurs.

Art. 38. — Est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 5.000.000 à 100.000.000 de francs CFA, quiconque sans autorisation, organise des jeux d'argent illicites en ligne caractérisés par la tenue de jeux de hasard, de loterie illicite, de publicité de loterie prohibée, de prise de paris illicite sur les réseaux de communication électronique.

Art. 39. — Sont interdits les transferts d'argent par cartes de paiement ou par virement ou par tout autre moyen de paiement effectués par des personnes physiques ou morales dans le cadre de jeux d'argent illicites sur les réseaux de communication électronique.

Les établissements bancaires ou financiers exerçant sur le territoire national veillent au respect de cette interdiction. Ces établissements notifient aux autorités compétentes toute violation constatée ou tentative de violation de cette interdiction.

Art. 40. — Est puni d'une peine d'emprisonnement de cinq ans et d'amende de 5.000.000 à 10.000.000 de francs CFA, quiconque ne respecte pas l'interdiction de transfert d'argent.

La peine encourue par la personne morale responsable est le double de l'amende prévue pour la personne physique ayant commis l'infraction.

Si le transfert est effectué à destination de l'étranger, l'infraction commise constitue également une infraction à la réglementation régissant les relations financières extérieures et elle est punie sans préjudice des dispositions de la loi relative au contentieux des infractions au contrôle des changes.

Art. 41. — Les juridictions nationales sont compétentes pour constater ou punir les infractions lorsque les activités de jeux d'argent illicites sont offertes à partir du territoire national ou sont accessibles aux utilisateurs des réseaux de communication électronique à partir du territoire national et qu'il existe un lien suffisant, substantiel ou significatif entre la prestation illicite offerte aux utilisateurs des réseaux de communication en ligne et le territoire national, notamment, par la langue utilisée, la monnaie employée, les produits proposés, le nom de domaine utilisé par le site proposant ladite prestation.

CHAPITRE 6

Responsabilité des prestataires techniques de service en ligne

Art. 42.— L'accès au service internet à partir d'un cybercafé situé sur le territoire national est soumis à l'identification préalable des usagers.

Les exploitants de cybercafé sont tenus de procéder à cette identification suivant les modalités fixées par décret.

Art. 43. — Le mineur de moins de dix ans ne peut accéder à un cybercafé qu'accompagné d'un adulte.

L'accès à internet dans un cybercafé pour un mineur de moins de dix-huit ans est un accès limité, qui exclut les sites web à caractère pornographique, violent, raciste ou dégradant et de manière générale tous les sites web portant atteinte à la dignité humaine ou incitant à l'incivisme.

Art. 44. — Les personnes dont l'activité est d'offrir un accès à des services de communication en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

Art. 45. — Est puni d'une peine d'amende de 1.000.000 à 10.000.000 de francs CFA, quiconque ne respecte pas l'obligation d'information et de mise à disposition de moyens techniques de filtrage.

Le fournisseur de services offrant un accès à des services de communication ou assurant à titre gratuit ou onéreux le stockage direct et permanent pour mise à disposition de contenus, est tenu, sur décision du juge compétent, de suspendre immédiatement l'accès auxdits services ou contenus.

Art. 46. — Les personnes physiques ou morales qui offrent un accès à des services de communication en ligne ou qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent voir leur responsabilité civile ou pénale engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services :

— si elles n'avaient effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;

— si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ;

— si le retrait de ces données n'a pas été ordonné par un tribunal.

Art. 47. — La connaissance des faits litigieux est présumée acquise par les personnes mentionnées à l'article précédent, lorsqu'il leur est notifié par la victime ou par une personne intéressée, les activités illicites ou les faits et circonstances faisant apparaître ce caractère. Pour être prise en compte la notification doit comporter les éléments suivants :

— si l'auteur de la notification est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance.

— si l'auteur de la notification est une personne morale : sa dénomination et son siège social ;

— les nom, prénoms et domicile du destinataire du service en cause ou s'il s'agit d'une personne morale, sa dénomination et son siège social ;

— la description des faits litigieux et leur localisation précise sur le réseau ;

— les droits et les motifs pour lesquels le retrait du contenu litigieux est demandé ;

— la copie de la correspondance adressée à l'auteur ou à défaut à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

Art. 48. — La procédure de notification des faits ou d'activités illicites prévue à l'article précédent n'a pas pour effet d'engager la responsabilité d'une des personnes concernées par les exceptions prévues à l'article 47 de la présente loi.

Art. 49. — Est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 5.000.000 de francs CFA, le fait, pour toute personne de présenter de mauvaise foi aux personnes mentionnées à l'article 47 de la présente loi, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion.

Art. 50. — Les personnes mentionnées à l'article 47 de la présente loi ne sont pas soumises à une obligation de surveillance des informations qu'elles transmettent ou stockent, ni à une obligation de recherche des faits ou des circonstances révélant des activités illicites.

Toutefois, l'autorité judiciaire peut requérir de ces personnes une surveillance ciblée et temporaire des activités exercées par le biais de leurs services.

Art. 51. — Les fournisseurs d'accès internet sont tenus de mettre en place un dispositif facilement accessible et visible sur leur site internet permettant à toute personne de porter à leur connaissance ce type d'activités illicites et sont tenus de rendre publics les moyens consacrés à cette lutte.

Les fournisseurs d'accès internet sont tenus également d'informer promptement les autorités publiques compétentes de toutes activités illicites qui leur sont signalées et qu'exercent les destinataires de leurs services.

Tout manquement aux obligations définies ci-dessus est puni d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 5.000.000 de francs CFA.

Art. 52. — L'autorité judiciaire peut prescrire, à toute personne mentionnée à l'article 47 de la présente loi, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Tout manquement aux prescriptions judiciaires définies ci-dessus est puni d'une peine d'emprisonnement d'un an à cinq ans et d'une amende de 1.000.000 à 5.000.000 de francs CFA.

Art. 53. — Les personnes mentionnées à l'article 47 de la présente loi sont tenues de détenir et de conserver sur une période de trois ans les données informatiques de nature à permettre l'identification de quiconque a contribué à la création d'un contenu ou de l'un des contenus des services dont elles sont prestataires conformément aux dispositions légales ou réglementaires relatives à la protection des données à caractère personnel.

L'autorité judiciaire peut requérir auprès de ces personnes la communication des données d'identification des destinataires des services dont elles sont prestataires.

Art. 54. — Les personnes mentionnées à l'article 47 de la présente loi sont tenues de mettre à la disposition du public en ligne leurs propres données permettant de les identifier lorsque leurs services sont offerts à partir du territoire national ou sont accessibles à partir de ce territoire et destinés aux utilisateurs des réseaux de communication en ligne dudit territoire.

Ces données d'identification doivent comporter les éléments suivants :

s'il s'agit de personnes physiques: leurs nom, prénoms, domicile, date et lieu de naissance, numéro de téléphone, adresse postale, adresse électronique et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier ou au répertoire des métiers, le numéro de leur inscription.

s'il s'agit de personnes morales, leur dénomination sociale et l'adresse de leur siège social, leur numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier ou au répertoire des métiers, le numéro de leur inscription, leur capital social et leur adresse électronique.

Toutefois, les personnes éditant à titre non professionnel un service de communication électronique peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination sociale et l'adresse de la personne mentionnée à l'article 47 de la présente loi, sous réserve d'avoir satisfait auprès de cette dernière à son obligation d'identification telle que prévue ci-dessus.

Art. 55. — Est puni d'une peine d'emprisonnement de un an à cinq ans et d'une amende de 1.000.000 à 5.000.000 de francs CFA le fait pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités mentionnées à l'article 47 de la présente loi, de ne pas satisfaire aux obligations définies aux articles 53 et 54 ci-dessus.

Art. 56. — Toute personne assurant une activité de transmission de contenus sur un réseau de télécommunications ou de fourniture d'accès à un réseau de télécommunications ne peut voir sa responsabilité civile ou pénale engagée en raison de ces contenus que dans l'un des cas suivants :

— lorsqu'elle est à l'origine de la demande de transmission litigieuse ;

— lorsqu'elle sélectionne le destinataire de la transmission ;

— lorsqu'elle sélectionne ou modifie les contenus faisant l'objet de la transmission.

Art. 57. — Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que si :

— elle a modifié ces contenus et ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour ou a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données ;

— elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible.

CHAPITRE 7

Adaptation des infractions classiques aux technologies de l'information et de la communication

Art. 58. — Est puni de dix à vingt ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, le fait pour toute personne de créer, de diffuser ou de mettre à disposition sous quelque forme, que ce soient des écrits, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système d'information.

L'infraction ci-dessus définie est un délit.

Art. 59. — Est puni de deux à cinq ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs CFA d'amende, le fait pour toute personne de menacer autrui de mort ou de violence par le biais d'un système d'information.

Lorsque la menace a un caractère raciste, xénophobe, ethnique, religieux ou fait référence à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, la peine d'emprisonnement est de dix à vingt ans et l'amende est de 20.000.000 à 40.000.000 de francs CFA.

L'infraction ci-dessus définie est un délit.

Art. 60. — Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, le fait pour toute personne de proférer ou d'émettre toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un système d'information.

Art. 61. — Est puni de trois à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, le fait pour toute personne de nier, d'approuver ou de justifier, intentionnellement, des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système d'information.

Art. 62. — Est puni de un mois à cinq ans d'emprisonnement et de 1.000.000 à 20.000.000 de francs CFA d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information.

Art. 63. — Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs CFA d'amende, le fait pour toute personne de diffuser ou de mettre à disposition d'autrui par le biais d'un système d'information, sauf à destination des personnes autorisées, un mode d'emploi ou un procédé permettant la fabrication de moyens de destruction de nature à porter atteinte à la vie, aux biens ou à l'environnement.

Art. 64. — Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs CFA d'amende, le fait pour toute personne de diffuser ou de mettre à disposition d'autrui, par le biais d'un système d'information, des procédés ou des informations d'incitation au suicide.

Art. 65. — Est puni de six mois à deux ans d'emprisonnement et de 1.000.000 à 5.000.000 de francs CFA d'amende, le fait pour toute personne de communiquer ou de divulguer par le biais d'un système d'information, une fausse information tendant à faire croire qu'une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes a été commise ou va être commise.

Est puni des mêmes peines, le fait de communiquer ou de divulguer par le biais d'un système d'information, une fausse information faisant croire à un sinistre ou à toute autre situation d'urgence.

Art. 66. — Est puni de cinq à dix ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs CFA d'amende, le fait pour toute personne de menacer de commettre par le biais d'un système d'information, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'elle est matérialisée par un écrit, une image, un son, une vidéo ou toute autre donnée.

Art. 67. — Est coupable de trahison et puni de l'emprisonnement à vie, le fait pour un Ivoirien :

— de livrer ou de s'assurer de la possession en vue de la livraison à un pays étranger ou à une personne physique ou morale étrangère par le biais d'un système d'information, un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu *(e)* secret dans l'intérêt de la Défense nationale ;

de détruire ou de laisser détruire un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu *(e)* secret dans l'intérêt de la Défense nationale, en vue de favoriser un pays étranger ou une personne physique ou morale étrangère.

Art. 68. — Est coupable d'espionnage et puni de l'emprisonnement à vie, le fait pour un étranger :

— de livrer ou de s'assurer de la possession en vue de la livraison à un pays étranger ou à une personne physique ou morale étrangère par le biais d'un système d'information, un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu *(e)* secret dans l'intérêt de la Défense nationale,

— de détruire ou de laisser détruire un tel renseignement, un document, un procédé ou une donnée informatique qui doit être tenu *(e)* secret dans l'intérêt de la Défense nationale, en vue de favoriser un pays étranger ou une personne physique ou morale étrangère.

Art. 69. — Toute personne morale, à l'exception de l'Etat est pénalement responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par ses représentants.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

La peine encourue par les personnes morales responsables est le double de l'amende prévue pour la personne physique ayant commis l'infraction.

Art. 70. — En cas de condamnation au titre de la présente loi, outre la publicité de la condamnation ordonnée et exécutée, conformément à l'article 75 du Code pénal, le juge peut prononcer à titre complémentaire, la confiscation spéciale la privation des droits et l'interdiction de séjour prévues respectivement aux articles 63, 66 et 80 du Code pénal.

CHAPITRE 8

Procédure pénale en matière de cybercriminalité

Art. 71. — Les officiers de police judiciaire définis à l'article 16 nouveau du Code de Procédure pénale, les experts agréés auprès des tribunaux et toute autre personne dont les compétences sont requises, serment préalablement prêté, peuvent procéder aux opérations prévues par la présente loi.

Les autorités compétentes visées ci-dessus n'ayant pas la qualité d'officier de Police judiciaire ne peuvent procéder à une perquisition qu'en présence de ces officiers.

Art. 72. — Les données relatives aux abonnés doivent être conservées par les fournisseurs de services. Cette obligation impose aux fournisseurs de services de conserver et de protéger l'intégrité desdites données pendant une durée de dix ans.

Lorsqu'il est impossible de retrouver l'auteur diune communication électronique pour défaut de conservation des données relatives aux abonnés, le fournisseur de services encourt une peine d'amende de 10.000.000 à 50.000.000 de francs CFA.

Art. 73. — Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données.

La personne physique ou morale à qui injonction est faite, conserve et protège l'intégrité desdites données pendant une durée aussi longue que nécessaire pour les besoins de l'enquête ou l'instruction.

Art. 74. — L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, peut requérir :

de toute personne physique ou morale, l'obligation de communiquer des données spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique;

d'un fournisseur de services, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle.

Art. 75. — L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le Code de Procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition.

L'autorité compétente peut également accéder à des données intéressant l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé hors du territoire national, elles sont recueillies par l'autorité compétente, sous réserve du respect des engagements internationaux.

Art. 76. — L'autorité compétente peut, dans les conditions prévues par le Code de Procédure pénale, procéder à la saisie des systèmes informatiques, des supports de stockage informatique ou procéder à la copie des données informatiques nécessaires à la manifestation de la vérité.

Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur décision du juge, à l'effacement définitif sur le support physique qui n'a pas été placé sous-main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Lorsque les systèmes informatiques ou les supports de stockage informatique sont mis sous scellés, ils ne peuvent être ouverts que selon les modalités prévues par le Code de Procédure pénale.

Art. 77. — L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, est habilitée :

— à collecter ou enregistrer par tout moyen technique les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information ;

— à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer en temps réel, les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information.

Les surcoûts identifiables et spécifiques éventuellement exposés par les fournisseurs de services pour répondre à ces demandes font l'objet d'une compensation financière de l'Etat.

Art. 78. — Est puni d'une peine d'emprisonnement de trois à six mois et de 1.000.000 à 5.000.000 de francs CFA d'amende, quiconque refuse de déférer à la demande du procureur ou du juge d'instruction.

Lorsqu'il s'agit d'une personne morale, elle encourt une peine d'amende de 10.000.000 à 100.000.000 de francs CFA.

Art. 79. — La présente loi sera publiée au *Journal officiel* de la République de Côte d'Ivoire et exécutée comme loi de l'Etat.

Fait à Abidjan, le 19 juin 2013.

Alassane OUATTARA.

DECRET n° 2013-352 du 22 mai 2013 portant nomination des membres de la Commission centrale de la Commission nationale des Droits de l'Homme de Côte d'Ivoire, en abrégé CNDHCI.

LE PRESIDENT DE LA REPUBLIQUE,

Sur rapport conjoint du garde des Sceaux, ministre de la Justice, des Droits de l'Homme et des Libertés publiques,

Vu la Constitution,

Vu la loi n° 2012-1132 du 13 décembre 2012 portant création, attributions, organisation et fonctionnement de la commission nationale des Droits de l'Homme de Côte d'Ivoire ;

Vu le décret n° 2012-1118 du 21 novembre 2012 portant nomination du Premier Ministre ;

Vu le décret n° 2012-1119 du 22 novembre 2012 portant nomination des membres du Gouvernement ;

Le Conseil des ministres entendu,

DECRETE :

Article premier. —Sont nommées membres de la Commission centrale de la Commission nationale des Droits de l'Homme de Côte d'Ivoire, en abrégé CNDHCI, avec voix délibérative, les personnalités dont la liste suit :

Annexe 8 : Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (Article 1 à 41)

Journal Officiel de la République de Côte-d'Ivoire du 08 août 2013

PARTIE OFFICIELLE

ACTES PRESIDENTIELS

PRESIDENCE DE LA REPUBLIQUE

LOI n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

L'ASSEMBLEE NATIONALE a adopté,

le Président de la République promulgue la loi dont la teneur suit :

CHAPITRE I

Définitions

Article premier. — Les définitions des instruments juridiques de la CEDEAO, de l'Union africaine ou de l'Union internationale des Télécommunications prévalent pour les termes non définis par la présente loi.

Au sens de la présente loi, on entend par :

— *activité de cryptologie*, toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;

— *agrément*, la reconnaissance formelle par un organisme agréé que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié ;

— *archivage électronique sécurisé*, l'ensemble des modalités de conservation et de gestion des archives électroniques destinées à garantir leur valeur juridique pendant toute la durée nécessaire ;

— *atteinte à la dignité humaine*, toute atteinte, hors les cas d'attentat à la vie, à l'intégrité ou à la liberté, qui a pour effet essentiel de traiter la personne comme une chose, comme un animal ou comme un être auquel serait dénié tout droit ;

— *autorité de protection*, l'autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi ;

— *chiffrement*, toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;

— *code de conduite*, la charte d'utilisation élaborée par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologuée par l'Autorité de protection ;

— *commerce électronique*, l'activité économique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture de biens et la prestation de services ;

entrent également dans le champ du commerce électronique, les activités de fourniture de services telles que celles consistant à fournir des informations en ligne, des communications commerciales, des outils de recherches, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, même s'ils ne sont pas rémunérés par ceux qui les reçoivent ;

— *communication électronique*, toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen ;

— *consentement de la personne concernée*, toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique ;

— *conventions secrètes*, toutes clés non publiées, nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;

— *courrier électronique*, tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

— *cryptologie*, la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non-répudiation ;

— *cybercriminalité*, toute infraction pénale qui se commet au moyen ou sur un réseau de communications électroniques ou un système informatique ;

— *destinataire d'un traitement des données à caractère personnel*, toute personne habilitée à recevoir une communication de ces données, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter les données ;

— *document*, le résultat d'une série de lettres, de caractères, de chiffres, de figures ou de tous autres signes ou symboles qui a une signification intelligible, quels que soient leur média et leurs modalités de transmission ;

— *données à caractère personnel*, toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identifié physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

— *données informatiques ou données*, toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information ;

— *données relatives aux abonnés*, toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir sur la base d'un contrat ou d'un arrangement de services ;

— *le type de service de communication*, les dispositions techniques prises à cet égard et la période de service ;

— *l'identité*, l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de communication ;

— *données relatives au trafic*, toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

— *données sensibles*, toutes données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

— *échange de données informatisées (EDI)*, tout transfert électronique d'une information d'un système électronique à un autre mettant en œuvre une norme convenue pour structurer l'information ;

— *écrit*, toute suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles qui a une signification intelligible, quels que soient leur support et leurs modalités de transmission ;

— *fichier de données à caractère personnel*, tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique permettant d'identifier une personne déterminée ;

— *fournisseur de services*, toute personne morale qui fournit au public des services de communications électroniques ou des prestations informatiques ;

— *information*, tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc. ;

— *infrastructures critiques*, les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique et social des citoyens ou encore le fonctionnement continu des services de l'Etat ;

— *interconnexion des données à caractère personnel*, tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ;

— *message électronique*, toute information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie.

— *mineur*, toute personne âgée de moins de dix-huit ans, conformément au code pénal ;

— *moyens de cryptologie*, l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ; on entend, également, par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'écrits ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète ;

— *pays tiers*, tout Etat non membre de la CEDEAO ;

— *personne concernée*, toute personne physique qui fait l'objet d'un traitement de données à caractère personnel ;

— *prestation de cryptologie*, toute opération visant à la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;

— *prestataire de services de cryptologie*, toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

— *pornographie infantile*, toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un enfant de moins de 18 ans se livrant à un agissement sexuellement explicite ou des images représentant un enfant de moins de 15 ans se livrant à un comportement sexuellement explicite ;

— *prospection directe*, tout envoi de message, quel qu'en soit le support ou la nature notamment commercial, politique ou caritative, destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;

— *racisme et xénophobie en matière des TIC*, 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 où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ;

— *responsable du traitement*, la personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités ;

— *signature électronique*, toute donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ;

— *SMS*, le sigle anglo-saxon signifiant « short message service » (en français : service de message court) ;

— *sous-traitant*, toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;

— *surveillance*, toute activité faisant appel à des moyens techniques ou électroniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ;

— *système d'information ou 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 ;

— *tiers*, toute personne physique ou morale, publique ou privée, tout autre organisme ou association autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données ;

— *traitement des données à caractère personnel*, toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel.

CHAPITRE 2

Objet et champ d'application du secrétaire permanent de la Commission nationale du Fonds pour l'Environnement mondial.

Art. 2. — La présente loi a pour objet de régir la protection des données à caractère personnel.

Art. 3. — Sont soumis aux dispositions de la présente loi :

— toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;

— tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier ;

— tout traitement de données mis en œuvre sur le territoire national ;

— tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Art. 4. — sont exclus du champ d'application de la présente loi :

— les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;

— les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

CHAPITRE 3

Formalités nécessaires au traitement des données à caractère personnel

Art. 5. — Le traitement des données à caractère personnel est soumis à une déclaration préalable auprès de l'Autorité de protection des données à caractère personnel.

La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

L'Autorité de protection délivre un récépissé en réponse à la déclaration, le cas échéant, par voie électronique. Le demandeur peut mettre en oeuvre le traitement dès réception de son récépissé ; il n'est exonéré d'aucune de ses responsabilités.

Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Les informations requises au titre de la déclaration ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Art. 6. — Sont dispensés des formalités de déclaration préalable :

— le traitement de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles, domestiques ou familiales ;

— le traitement de données concernant une personne physique dont la publication est prescrite par une disposition légale ou réglementaire ;

— le traitement de données ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;

— le traitement pour lequel le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi, sauf lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers est envisagé.

Art. 7. — Sont soumis à autorisation préalable de l'Autorité de protection avant toute mise en oeuvre :

— le traitement des données à caractère personnel portant sur des données génétiques, médicales et sur la recherche scientifique dans ces domaines ;

— le traitement des données à caractère personnel portant sur des données relatives aux infractions, aux condamnations ou aux mesures de sûreté prononcées par les juridictions ;

— le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphones ;

— le traitement des données à caractère personnel comportant des données biométriques ;

— le traitement des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;

— le transfert de données à caractère personnel envisagé à destination d'un pays tiers.

La demande d'autorisation est présentée par le responsable du traitement ou son représentant légal.

L'autorisation n'exonère pas de la responsabilité à l'égard des tiers.

Art. 8. — Pour les catégories les plus courantes de traitement des données à caractère personnel notamment celles dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'Autorité de protection établit et publie des normes et procédures destinées à simplifier ou à exonérer le responsable du traitement de l'obligation de déclaration préalable.

Art. 9. — La demande d'avis, la déclaration et la demande d'autorisation sont adressés à l'Autorité de protection et contiennent au minimum les mentions suivantes :

— l'identité, le domicile, l'adresse postale ou géographique du responsable du traitement ou si celui-ci n'est pas établi sur le territoire national, celles de son représentant dûment mandaté, et s'il s'agit d'une personne morale, sa dénomination sociale, son siège social, l'identité de son représentant légal, son numéro d'immatriculation au registre du commerce et du crédit mobilier, son numéro de déclaration fiscale ;

— la ou les finalité(s) du traitement ainsi que la description générale de ses fonctions ;

— les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

— les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

— la durée de conservation des données traitées ;

— le ou les service(s) chargé(s) de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données collectées ;

— les destinataires habilités à recevoir communication des données traitées ;

— la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

— les dispositions prises pour assurer la sécurité des traitements, la protection et la confidentialité des données traitées ;

— l'indication du recours à un sous-traitant ou du transfert des données à caractère personnel à destination d'un pays tiers.

En cas de changement intervenu dans les mentions énumérées ci-dessus, le responsable du traitement en informe, sans délai, l'Autorité nationale de protection des données à caractère personnel.

Les conditions de la présentation de la demande d'autorisation et les procédures d'octroi des autorisations sont fixées par décret pris en Conseil des ministres.

L'Autorité de protection peut, par décision, exiger des conditions complémentaires de présentation de la demande d'autorisation ou de déclaration et aux procédures d'octroi des autorisations.

Art. 10. — La déclaration ou la demande d'autorisation peut être adressée à l'Autorité de protection par voie électronique, postale ou par tout autre moyen contre remise d'un accusé de réception.

Art. 11. — L'Autorité de protection se prononce dans un délai d'un mois à compter de la réception de la déclaration ou de la demande d'autorisation. Toutefois, ce délai peut être prorogé d'un mois supplémentaire sur décision motivée de l'Autorité de protection.

L'absence de réponse de l'Autorité de protection dans le délai imparti équivaut à un rejet de la déclaration ou de la demande d'autorisation. Dans ce cas, le responsable du traitement peut exercer un recours devant la juridiction compétente.

Les modalités de dépôt des déclarations ou d'octroi des autorisations pour le traitement des données à caractère personnel conformément aux dispositions de la présente loi sont fixées par décret.

Art. 12. — Le correspondant à la protection des données à caractère personnel est une personne bénéficiant de qualifications requises pour exercer de telles missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur, du fait de l'accomplissement de ses missions. Il peut saisir l'Autorité de protection des difficultés qu'il rencontre dans l'exercice de ses missions.

La désignation du correspondant par le responsable du traitement est notifiée à l'Autorité de protection. Elle est, également, portée, le cas échéant, à la connaissance des instances représentatives du personnel.

Le profil et les conditions de rémunération du correspondant à la protection des données à caractère personnel font l'objet d'un arrêté du ministre chargé des Technologies de l'Information et de la Communication, sur proposition de l'Autorité de protection.

En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de l'Autorité de protection.

Art. 13. — Les traitements des données à caractère personnel opérés pour le compte de l'Etat, d'une personne morale de droit public ou de droit privé gérant un service public sont autorisés par décret, après avis motivé de l'Autorité de protection.

Ces traitements portent sur :

— la sûreté de l'Etat, la défense nationale ou la sécurité publique ;

— la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

— le recensement de la population ;

— le traitement de salaires, pensions, impôts, taxes et autres liquidations.

CHAPITRE 4

Principes-directeurs du traitement des données à caractère personnel

Art. 14. — Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable.

Toutefois, il peut être dérogé à cette exigence du consentement préalable lorsque le responsable du traitement est dûment autorisé et que le traitement est nécessaire :

— soit au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

— soit à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

— soit à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

— soit à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée ;

Art. 15. — La collecte, l'enregistrement, le traitement, le stockage, la transmission et l'interconnexion de fichiers des données à caractère personnel doivent se faire de manière licite et loyale.

Art. 16. — Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Art. 17. — Les données collectées doivent être exactes et, si nécessaire, mises à jour.

Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Art. 18. — Le principe de transparence implique une information obligatoire et claire de la part du responsable du traitement portant sur les données à caractère personnel.

Art. 19. — Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement de ces données comporte des transmissions de données dans un réseau.

Art. 20. — Lorsque le traitement des données à caractère personnel est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes pour la protection et la confidentialité de ces données.

Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect des dispositions de la présente loi.

Art. 21. — Est interdit et puni d'une peine d'emprisonnement de dix à vingt ans et d'une amende de 20.000.000 à 40.000.000 de francs CFA, le fait de procéder à la collecte et à tout traitement de données qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Cette interdiction ne s'applique pas :

— lorsque le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;

— lorsque le traitement des données génétiques ou relatives à l'état de santé est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

— lorsque le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice de la personne concernée :

— lorsqu'une procédure judiciaire ou une enquête pénale est ouverte. Dans ce cas, le traitement des données à caractère personnel n'est poursuivi que pour la constatation des faits ou pour la manifestation de la vérité ;

— lorsque le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls membres de cet organisme ou aux personnes entretenant avec celui-ci des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Tous ces cas de traitement de données à caractère personnel sont autorisés et contrôlés dans leur conception et leur mise en œuvre par l'Autorité de protection.

Art. 22. — Est interdite et punie d'une peine d'emprisonnement de un à cinq ans et d'une amende de 1.000.000 à 10.000.000 de francs CFA, la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Art. 23. —Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche, d'expression artistique ou littéraire est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou de chercheur, dans le respect des règles déontologiques de ces professions.

Art. 24. — Les dispositions de la présente loi ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

Art. 25. — Aucune décision de justice impliquant une appréciation sur le comportement d'une personne physique ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé des données à caractère personnel donnant une définition du profil ou de la personnalité de l'intéressé.

Art. 26. — Le responsable d'un traitement ne peut être autorisé à transférer des données à caractère personnel vers un pays tiers que si cet Etat assure un niveau de protection supérieur ou équivalent de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Avant tout transfert effectif des données à caractère personnel vers ce pays tiers, le responsable du traitement doit préalablement obtenir l'autorisation de l'Autorité de protection.

Le transfert de données à caractère personnel vers les pays tiers fait l'objet d'un contrôle régulier de l'Autorité de protection au regard de leur finalité.

Art. 27. — L'interconnexion des fichiers n'est autorisée que si elle permet d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements.

Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité inappropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

CHAPITRE 5

Droits et exceptions aux droits de la personne concernée

Art. 28. — Le responsable du traitement est tenu de fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

— son identité et, le cas échéant, celle de son représentant dûment mandaté ;

— la ou les finalité(s) déterminée(s) du traitement auquel les données sont destinées ;

— les catégories de données concernées ;

— le ou les destinataire(s) auxquels les données sont susceptibles d'être communiquées ;

— la possibilité de refuser de figurer sur le fichier en cause ;

— l'existence d'un droit d'accès aux données concernant la personne et d'un droit de rectification de ces données ;

— la durée de conservation des données ;

— l'éventualité de tout transfert de données à destination de pays tiers.

Art. 29. — Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander sous forme de questions et obtenir du responsable de ce traitement :

— les informations permettant de connaître et de contester le traitement ;

— la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

— la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

— des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées.

En cas d'impossibilité d'accès de la personne concernée, le droit d'accès peut être exercé par l'Autorité de protection des données qui dispose d'un pouvoir d'investigation en la matière et qui peut ordonner la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi.

L'Autorité de protection des données communique à la personne concernée le résultat de ses investigations.

Le responsable du traitement peut s'opposer aux demandes manifestement abusives de la même personne, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

Art. 30. — Toute personne physique concernée a le droit :

— de s'opposer, pour des motifs légitimes tenant à sa situation particulière, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition légitime, le traitement mis en œuvre par le responsable du traitement ne peut porter sur les données en cause ;

— de s'opposer, sur sa demande et gratuitement, au traitement de données la concernant à des fins de prospection ;

— d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément accorder le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Art. 31. — Toute personne physique, justifiant de son identité, peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Art. 32. —ration du secrétaire permanent de la Commission nationale du Fonds pour l'Environnement mondial.

Les ayants droit d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les ayants droit en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Art. 33. — La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était mineur, ou pour l'un des motifs suivants :

— les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;

— la personne concernée a retiré le consentement sur lequel est fondé le traitement ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données ;

— la personne concernée s'oppose au traitement des données à caractère personnel la concernant lorsqu'il n'existe pas de motif légal audit traitement ;

— le traitement des données n'est pas conforme aux dispositions de la présente loi ;

— pour tout autre motif légitime.

Art. 34. — Lorsque le responsable du traitement a rendu publiques les données à caractère personnel de la personne concernée, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.

Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel de la personne concernée, il est réputé responsable de cette publication et prend toutes les mesures appropriées pour mettre en œuvre le droit à l'oubli numérique et à l'effacement des données à caractère personnel.

Art. 35. — Le responsable du traitement procède à l'effacement sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire :

— soit à l'exercice du droit à la liberté d'expression ;

— soit pour des motifs d'intérêt général dans le domaine de la santé publique, conformément à la loi ;

— soit au respect d'une obligation légale de conserver les données à caractère personnel prévue par la législation en vigueur à laquelle le responsable du traitement est soumis.

Art. 36. — Le responsable du traitement met en place des mécanismes appropriés assurant la mise en œuvre du respect du droit à l'oubli numérique et à l'effacement des données à caractère personnel ou examine périodiquement la nécessité de conserver ces données, conformément aux dispositions de la présente loi.

Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données à caractère personnel.

Art. 37. — L'Autorité de protection des données adopte des mesures et des lignes directrices aux fins de préciser :

— les conditions de la suppression des liens vers ces données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;

— les conditions et critères applicables à la limitation du traitement des données à caractère personnel.

Art. 38. — Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée.

Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle.

L'Autorité de protection des données peut préciser le format électronique, ainsi que les normes techniques, les modalités et les procédures pour la transmission de données à caractère personnel.

CHAPITRE 6

Obligations des responsables et de leurs subordonnés

Art. 39. — Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Art. 40. — Le responsable du traitement est tenu de prendre toute précaution au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisi un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

Art. 41. — Le responsable du traitement est tenu :

— d'empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données ;

— d'empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ;

— d'empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;

— d'empêcher que des systèmes de traitement de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données ;

— d'empêcher que des systèmes de traitement de données soient utilisés à des fins de blanchiment de capitaux et de financement du terrorisme ;

— de garantir que, lors de l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur autorisation ;

— de garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;

— de garantir que puisse être vérifiée et constatée a posteriori l'identité des personnes ayant eu accès au système d'information contenant des données à caractère personnel, la nature des données qui ont été introduites, modifiées, altérées, copiées, effacées ou lues dans le système, le moment auquel ces données ont été manipulées ;

INDEX SELECTIF

A

B

C

D

E

F

H

I

L

M

O

P

R

S

T

U

Table des matières