

UNIVERSITE ASSANE SECK DE ZIGUINCHOR



UFR DES SCIENCES ÉCONOMIQUES ET SOCIALES

DEPARTEMENT DE DROIT DES AFFAIRES

MEMOIRE DE MASTER

Spécialité : Droit de l'Entreprise

Sujet : LA RESPONSABILITE DES PRESTATAIRES TECHNIQUES

Présenté par

Monsieur Boubacar DIASSY

Sous la direction de

Monsieur le Professeur Abdoul Aziz DIOUF

Agrégé des Facultés de Droit à l'Université Cheikh Anta DIOP de Dakar

Soutenu publiquement le 19 janvier 2017 devant le jury composé de :

Président : Pr Jean-Louis CORREA, Agrégé des Facultés de Droit, UASZ

Membres :

Dr Diélya Y. W. BA, Enseignante au département de Droit des Affaires, UASZ

Dr Philippe BASSENE, Enseignant au département de Droit des Affaires, UASZ

ANNEE UNIVERSITAIRE 2014 -2015

DELIBERATION DU JURY

Note : 17 / 20

Mention : Très Bien

UNIVERSITE ASSANE SECK DE ZIGUINCHOR



UFR DES SCIENCES ÉCONOMIQUES ET SOCIALES

DEPARTEMENT DE DROIT DES AFFAIRES

MEMOIRE DE MASTER

Spécialité : Droit de l'Entreprise

Sujet : LA RESPONSABILITE DES PRESTATAIRES TECHNIQUES

Présenté par
Monsieur Boubacar DIASSY

Sous la direction de
Monsieur le Professeur Abdoul Aziz DIOUF
Agrégé des Facultés de Droit à l'Université Cheikh Anta DIOP de Dakar

Soutenu publiquement le 19 janvier 2017 devant le jury composé de :

Président : Pr Jean-Louis CORREA, Agrégé des Facultés de Droit, UASZ

Membres :

Dr Diélya Y. W. BA, Enseignante au département de Droit des Affaires, UASZ

Dr Philippe BASSENE, Enseignant au département de Droit des Affaires, UASZ

ANNEE UNIVERSITAIRE 2014 -2015

L'Université n'entend donner aucune approbation ni improbation aux opinions émises dans les mémoires ; ces opinions doivent être considérées comme propres à leur auteur.

*L'évolution des mœurs et des techniques
donne naissance à de nouvelles formes de délinquances¹.*

¹ Doyen Jean CARBONNIER, « Sociologie juridique », Paris, PUF, 1978, p.401.

A

*Dr Babacar SARR, pour le Régime Particulier,
Pr Jean-Louis CORREA, qui m'a fait aimer le Droit,
et
Dr Mandickou NGOM et Dr Diélya Yaya WANE BA,
mes professeurs de Droit de l'Informatique.*

REMERCIEMENTS

Je tiens à remercier chaleureusement le Professeur Abdoul Aziz DIOUF, agrégé des Facultés de Droit, non seulement pour avoir accepté la direction de mes recherches mais aussi pour sa confiance, sa générosité, ses conseils et sa disponibilité inestimables qui ont contribué à constituer un excellent environnement de travail afin de concrétiser le présent mémoire.

Merci aux formidables enseignants-chercheurs du département de Droit des Affaires de l'UASZ pour l'assurance, la vigueur et la rigueur avec lesquelles ils ont guidé mes frères pas pendant toutes les années que sanctionne ce mémoire.

Je souhaite remercier Monsieur Marc-Pascal BASSENE, fonctionnaire en service à la Cour suprême, pour l'aide inconditionnelle qu'il m'a apportée et qui m'a permis d'accéder à divers documents y compris inédits et dont l'exploitation m'a été d'un grand apport dans le traitement de mon sujet.

Merci à ma douce épouse Mme Safiétou J. DIEME et à mes adorables enfants qui ont accepté mes longues absences pendant tout le temps qu'ont duré mes recherches et la rédaction de ce mémoire. Mes parents ne sauraient être en reste.

Merci aux agents de la Sonatel Ziguinchor, de Tigo Ziguinchor, d'Expresso Ziguinchor, de l'ARTP, de la CDP et de l'ADIE qui n'ont ménagé aucun effort pour une meilleure rédaction de ce mémoire.

Je souhaite associer aux remerciements les agents de la Mutuelle Générale de l'Éducation du Sénégal, antenne de Ziguinchor, ainsi que les affables informaticiens notamment les webmasters, les techniciens en informatique de Ziguinchor et d'ailleurs pour la plénitude de leur soutien.

A

ADIE : Agence De l'Informatique de l'Etat

ARJEL : Autorité de Régulation des Jeux en Ligne

I

IDI : Indice de Développement des Technologies de l'Information et de la Communication

J

JOCE ou J.O.C.E. : Journal Officiel des Communautés Européennes

JORF ou J.O.R.F : Journal Officiel de la République Française

JORS ou J.O.R.S. : Journal Officiel de la République du Sénégal

L

LCEN : Loi pour la Confiance de l'Economie Numérique

LOSI : Loi d'Orientation de la Société de l'Information

P

PHAROS : Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements.

PUF : Presses Universitaires de France

S

SABAM : Société d'Auteurs Belge – Belgische Auteurs Maatschappij

SAS : Société par Actions Simplifiée

SENTEL : SENégal TELéphonie

SONATEL : SOciété NAtionale des TELécommunications du Sénégal

SUDATEL: *The SUDAn TELecommunication Group*

T

Télécom : Télécommunications

TIC : Technologies de l'Information et de la Communication

TOR: *The Onion Router*

U

UCAD : Université Cheikh Anta Diop de la Dakar

UMOA : Union Monétaire Ouest Africaine

A

AAARGH : Association des Anciens Amateurs de Récits de Guerre et d'Holocauste
ADSL: *Asymmetric Digital Subscriber Line*
AFA: Association des Fournisseurs d'Accès
AIPJ: Action Internationale Pour la Justice
ANSD: Agence Nationale de Statistique et de la Démographie
ARTP: Autorité de Régulation des Télécommunications et de la Poste

B

BCEAO: Banque Centrale des Etats de l'Afrique de l'Ouest
BSD (Licence): *Berkeley Software Distribution License*

C

CA OU C.A.: Cour d'Appel
CD: *Compact Disc*
CDMA: *Code Division Multiple Access*
CDP : Commission de protection des Données Personnelles
CE : Conseil de l'Union Européen
CFA : Communauté Financière Africaine
CGV : Conditions Générales de Vente
CIOMag : *Chief Information Officer Magazine*
CJUE : Cour de Justice de l'Union Européenne
COCC : Code des Obligations Civiles et Commerciales

D

DNS : *Domain Name System*
DTAI : Direction du Traitement Automatique de l'Information

F

FAI : Fournisseur d'Accès à Internet
FMI : Fonds Monétaire International
FSJP: Faculté des Sciences Juridiques et Politiques

G

GMT: *Greenwich Mean Time*
GSM: *Global System for Mobile Communications*

H

HTML: *HyperText Markup Language*
HTTP: *HyperText Transfer Protocol*

I

IP: *Internet Protocol*

ISP: *Internet Service Provider*

ITU: *International Telecommunication Union*

J

JDN: Journal Du Net

L

LBC: Le Bon Coin

LGDJ: Librairie Générale de Droit et de Jurisprudence

O

OCLCTIC: Criminalité liée aux Technologies de l'Information et de la Communication

ONDRP: Observatoire National de la Délinquance et des Réponses Pénales

R

RGD: Revue Générale de Droit

RLDI : Revue Lamy Droit de l'Immatériel

S

SA ou S.A. : Société Anonyme

SARL: Société à Responsabilité Limitée

SFR: Société Française de Radiotéléphone

SMS: *Short Message Service*

SMSI : Sommet Mondial de la Société de l'Information

T

TCP : *Transmission Control Protocol*

TD ou T.D. : Travaux Dirigés

TF1 : Télévision Française 1

TGI ou T.G.I. : Tribunal de Grande Instance

TRHC : Tribunal Régional Hors Classe

U

UCL : Université Catholique de Louvain

UEJF : Union des Etudiants Juifs de France

UIT : Union Internationale des Télécommunications

UMTS: *Universal Mobile Telecommunications System*

URL: *Uniform Resource Locator*

USA: *United States of America*

W

WPAN: *Wireless Personal Area Network*

WWW: World Wide Web

ABBREVIATIONS

A

a.: autres
Act. Com.: *Active communication Ltd*
al.: alinéa
Ass.: Assemblée
avr.: avril

B

Bull.: Bulletin

C

c/: contre
Cass. : Cassation
Cf.: Confer
Ch.: Chambre
Civ.: Civile
Coll.: Collection
Com.: Commercial
Comm. : Communication
Cons.: Conseil
Coord.: Coordinateur
Crim. ou *Cri.*: Criminel

D

D.: (Recueil) Dalloz
Dir. : Directive
Dr ou *Dr.*: Docteur

E

E.D.: Ecole Doctorale
éd.: Edition
Electr.: Electronique

G

Gde.: Grande

J

janv. : janvier
juill.: juillet

N

N° ou *n°* : numéro
nov. : novembre

O

obs. : observation

Op. cit. : *Opere citato*

Ord.: Ordonnance

P

p. : page

Plén. : Plénière

pp. : page...à...page ou pages

Pr ou Pr. : Professeur

R

Réf. : Référé

S

Svts ou s. : suivants

Sect. : Section

Sté : Société

T

t. : tome

V

V. : Voir

vol. : volume

W

WEB : Word Wide Web

Wi-fi ou Wifi : *Wireless Fidelity*

AVERTISSEMENT

EPIGRAPHE

DEDICACE

REMERCIEMENTS

ACRONYMES

SIGLES

ABREVIATIONS

SOMMAIRE

INTRODUCTION

***1^{ERE} PARTIE : LA RESPONSABILITE DEROGATOIRE DES FOURNISSEURS
D'ACCES A INTERNET***

Chapitre 1^{er} : L'irresponsabilité principielle

Section 1^{ère} : L'absence a priori de la responsabilité civile et pénale

Section 2 : L'engagement de la responsabilité du fait personnel

***Chapitre 2 : Les obligations d'information, de moyens, de surveillance, de contrôle et de
résultat***

Section 1^{ère} : Les obligations d'information et de moyens

Section 2 : L'obligation minimale de surveillance et les obligations de contrôle et de
résultat

2^{DE} PARTIE : LA RESPONSABILITE AMENAGEE DES HEBERGEURS

Chapitre 1^{er} : L'exonération limitée de responsabilité

Section 1^{ère} : L'exonération de la responsabilité civile et pénale

Section 2 : Les limites à l'exonération de la responsabilité civile et pénale

Chapitre 2 : L'exonération des obligations générales de surveillance et de recherche

Section 1^{ère} : L'exonération de l'obligation générale de surveillance

Section 2 : L'exonération de l'obligation générale de recherche

CONCLUSION

ANNEXES

BIBLIOGRAPHIE

WEBOGRAPHIE

TABLE DES MATIERES

INTRODUCTION

Dans le rapport quinquennal 2015¹ de l'UIT², intitulé « *Mesurer la Société de l'Information* », l'Indice de Développement des Technologies de l'Information et de la Communication (IDI) du Sénégal est de 2,68 contre 1,80 en 2010 soit une croissance de 0,88. Cela classe le Sénégal au rang de 11^{ème} africain contre celui de 16^{ème}, cinq ans plus tôt. Ce rapport rend compte du dynamisme de la société sénégalaise de l'information.

Ce dynamisme témoigne de l'entrain global des 167 pays pris en compte par l'UIT dans le calcul de l'IDI, et qui affichent des chiffres en nette progression entre 2010 et 2015³. Concernant le Sénégal, il est celui d'un pays ayant choisi de fournir des efforts dans le secteur des télécommunications tout en se dotant d'un dispositif juridique à la mesure de ses ambitions. En effet, de 2003⁴ et 2008, les investissements des opérateurs des télécommunications, que sont la *Sonatel*⁵, *Sentel*⁶ GSM⁷ et *Sudatel*⁸, avaient atteint quelque quatre cent cinquante milliards⁹ de francs CFA¹⁰. Ces investissements se sont poursuivis, permettant en 2016, la disponibilité de l'Internet¹¹ sans-fil ou *Wi-fi*¹² et surtout de la 4G¹³. Et, avec un parc d'abonnés

¹ Il s'agit du dernier rapport quinquennal en vigueur. Toutefois, un rapport annuel, celui de 2016, disponible en version anglaise à partir de ce 5 avril 2016, est intitulé « *Mesures d'incitation réglementaires visant à concrétiser le potentiel du numérique* ». Il est consultable sur le site officiel de l'UIT en modèle *epub*, suivant le lien http://wftp3.itu.int/pub/epub_shared/BDT/2016/2016-Trends/flipviewerexpress.html.

² UIT : en anglais « *International Telecommunication Union* » (ITU) est fondée en 1865. Elle est la principale institution des Nations Unies pour les Technologies de l'Information et de la Communication (TIC). Elle encourage l'innovation dans le secteur des TIC, aux côtés des 193 États Membres et plus de 700 entités du secteur privé et institutions universitaires qui la composent. Source : Site officiel de l'UIT, www.itu.int visité le 5 février 2016.

³ In « *Rapport Mesurer la société de l'information 2015 : résumé analytique* », 2015, ITU, Genève, p. 5.

⁴ C'est l'année du lancement, par Sonatel, de l'ADSL au Sénégal ; précisément en mars 2003. Source : Sonatel, février 2016.

⁵ Acronyme pour « *Société Nationale des Télécommunications du Sénégal* ». Source : Sonatel Ziguinchor, Idem

⁶ « *Sentel GSM* » est le deuxième opérateur de téléphonie du Sénégal. Contrôlé à 75% par MILICOM INTERNATIONAL CELLULAR, « *Sentel GSM* » a obtenu la seconde licence de téléphonie mobile en juillet 1998 pour une durée de 20 ans et a lancé son service en avril 1999. In « *Histoire de l'Internet au Sénégal : 1989 – 2004* » par S. Olivier, B. Christophe et H. Steven, 2013, *University of Oregon Libraries*, USA, p. 30.

⁷ Sentel : Acronyme pour « *Sénégal Téléphonie* » et GSM est le sigle pour « *Global System for Mobile Communications* » qui signifie historiquement « *Groupe Spécial Mobile* » et est une norme numérique de seconde génération pour la téléphonie mobile. Fondée en 1999, Sentel GSM ou Sentel GSM S.A. est un opérateur de télécommunications, filiale au Sénégal de l'Américain *Millicom International Cellular SA*. Il exerce actuellement sous la marque Tigo. Sources : www.agencececofin.com, www.wikipedia.org et www.bloomberg.com, tous visités le 16 février 2016.

⁸ Acronyme pour : « *The Sudan Telecommunications Group* ». Source : Expresso Ziguinchor, février 2016.

⁹ Source : Artp, février et Août 2016 ou www.artpsenegal.sn, site visité le 27 août 2016.

¹⁰ Le Franc CFA est né le 26 décembre 1945, jour où la France ratifie les accords de Bretton Woods et procède à sa première déclaration de parité au Fonds Monétaire International (FMI). Il signifie alors "*Franc des Colonies Françaises d'Afrique*". Il prendra par la suite la dénomination de "*Franc de la Communauté Financière Africaine*" pour les États membres de l'Union Monétaire Ouest Africaine (UMOA). Source : site officiel de la Banque Centrale des États de l'Afrique de l'Ouest (BCEAO), www.bceao.int, visité le 7 février 2016.

¹¹ « *Internet* » est l'acronyme de l'expression anglaise « *Internetworking of networks* » devenu par contraction « *Internet* ». « *Internet* » est plus qu'un réseau, il est un ensemble de réseaux (ou d'interconnexion de réseaux, « *Interconnection of networks* ») qui, par le biais d'un langage informatique commun, parvient à faire communiquer tous les outils de la technologie numérique ; d'où la majuscule au début du mot. Voir également dans « *Le droit et Internet. Les enjeux présents et futurs de la société de l'information* », par Philippe Bouré, L'Hermès, 2002, pp.7-8. Et puis, le philosophe Jacques Dufresne, disait ceci d'Internet in « *Histoire de l'Internet* », 1996 : « *L'expression "internet" sert à désigner un ensemble de réseaux connectés entre eux, et "Internet" l'ensemble des réseaux utilisant les protocoles d'échanges TCP/IP* ».

¹² Le terme « *Wi-Fi* » ou « *Wifi* » suggère la contraction de « *Wireless Fidelity* », il est un ensemble de protocoles de communication sans fil. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, appareil photo, etc.), dits connectés, au sein d'un réseau informatique afin de permettre la transmission de données entre eux. Source : www.futura-science.com, site visité le 6 mars 2016.

¹³ La 4 G désigne la quatrième génération de normes de téléphonie mobile. Elle est représentée principalement par les normes *Universal Mobile Telecommunications System* (UMTS) et CDMA2000. Elle est beaucoup plus rapide que toutes les générations précédentes et permet, sur Internet, le visionnage de vidéos, d'émissions de télévision et la visiophonie. Source : Sonatel, juillet 2016.

estimé, courant décembre 2015, à 7.396.940, le taux de pénétration¹⁴ de l'ensemble des services Internet au Sénégal a augmenté, passant de 2,29%¹⁵ au 31 décembre 2003 à 54,76%¹⁶ au 31 décembre 2015. A titre comparatif, en France, ce taux est passé de moins de 15 % en 2000 à plus de 85 % en 2014 ; celui de l'Internet mobile étant en 2003 à 3% a plafonné en 2015 à 52%¹⁷.

Si, concernant le Sénégal, les efforts fournis ou encouragés par les décideurs en matière d'investissements semblent alors évidents, ils résultent toutefois de la mise en place d'un dispositif juridique s'inscrivant dans la droite ligne de ses objectifs en termes de normes¹⁸ à adopter. L'adoption de la loi n° 2008-10 du 25 janvier 2008 portant Loi d'Orientation sur la Société de l'Information¹⁹ (LOSI), qui est cependant dépourvue de dimension contraignante²⁰, et surtout de la loi n° 2008-08 du 25 janvier 2008 relative aux transactions électroniques²¹, dite « *loi sur les transactions électroniques* », en est un exemple.

A travers cette dernière, le législateur vise globalement²² à favoriser l'essor du commerce électronique pour ainsi respecter les engagements du Sénégal en rapport avec les conclusions du Sommet Mondial de la Société de l'Information (SMSI) de 2003, et à réaliser son ambition d'apporter des réponses juridiques aux questions posées par la sécurité des échanges électroniques et la protection du cyberconsommateur²³. Mieux, s'il n'est pas inutile de soutenir que l'esprit premier d'une loi, sa *ratio legis*²⁴, est la prévision et l'avant-gardisme, il ne semble pas non plus improbable que la loi sur les transactions électroniques soit pour ainsi dire futuriste ; pas plus d'ailleurs que celle française dont elle est inspirée, à savoir la Loi n° 2004-575 du 21 juin 2004 pour la Confiance dans l'Economie Numérique²⁵ (LCEN).

¹⁴ Le taux de pénétration est obtenu en divisant le nombre total de clients par la population totale du Sénégal, est estimée à 13.508.715 habitants lors du dernier recensement général (source : rapport définitif recensement 2013 ANSD, www.ansd.sn, site visité le 12 janvier 2016.)

¹⁵ S. Olivier, B. Christophe et H. Steven, « *Histoire de l'Internet au Sénégal : 1989 – 2004* », University of Oregon Libraries, USA, 2013, p. 15 : « *au 31 décembre 2003, il y avait 229 000 lignes fixes soit un taux de pénétration global de 2,29%* ».

¹⁶ *Ibidem*.

¹⁷ In www.statista.com, le portail français des statistiques. Visité le 30 mars 2016.

¹⁸ Définition de Norme, Normatif, Normative : « *La "Norme" est une règle qui, du fait de son origine (Constitution, Lois, règlements administratifs, Traités ou Accords internationaux.) et de son caractère général et impersonnel, constitue une source de droits et d'obligations juridiques* ». Source : www.dictionnaire-juridique.com, site visité le 26 mars 2016.

¹⁹ Loi n° 2008-10 du 25 janvier 2008 portant Loi d'Orientation sur la Société de l'Information (LOSI), p. 1, JORS n° 6406 du Samedi 3 mai 2008, voir sur www.jo.gouv.sn, site visité le 12 janvier 2016.

²⁰ Ch. Jacques, « *L'État postmoderne* », LGDJ, 2004, 2e éd., p. 123, cité par Bertrand MATHIEU in « *La normativité de la loi : une exigence démocratique* » article publié dans « *Cahiers du Conseil constitutionnel* », n° 21, janvier 2007, p. 1 ; article publié aussi sur le site www.conseil-constitutionnel.fr, visité le 31 mars 2016.

²¹ Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS n° 6439 du Samedi 22 novembre 2008, voir sur www.jo.gouv.sn, site visité le 12 janvier 2016

²² In exposé des motifs. *Ibidem*.

²³ *Ibidem*.

²⁴ S. Alain, B. Marc, « *Le commentaire de textes juridiques : lois et règlements* », 2^{ème} éd., Ellipses, Paris, 2007, p. 10 : « *dans le jargon juridique, l'esprit est la "ratio legis" de la loi : la raison d'être de la loi. La "ratio legis" commande l'emploi des mots et des phrases par l'auteur de la loi (ou du règlement)* ».

²⁵ JORF n° 143 du 22 juin 2004 texte n° 2/108 page 11168, voir sur www.legifrance.gouv.fr, ou www.journal-officiel.gouv.fr, sites visités le 12 janvier 2016.

La LCEN est une transposition en droit français du régime juridique mis en place par la Directive 2000/31/CE du 8 juin 2000²⁶ du Parlement européen et du Conseil sur le commerce électronique ayant pour objectif d'uniformiser les règles relatives à la responsabilité des prestataires de services Internet agissant en qualité d'intermédiaires, lesquels ont toujours été parmi les acteurs du développement de l'Internet. Ce régime juridique met en exergue, entre autres, l'encadrement de la responsabilité de ces acteurs. Le législateur sénégalais, à l'instar de son homologue français, a en conséquence prévu et encadré les activités de ces prestataires techniques, qu'il est nécessaire de déterminer à ce stade de cette réflexion.

Sans doute, serait-ce fondamental d'appréhender d'abord les contours sémantiques et juridiques de la notion de « *responsabilité* ». Dès lors, considérant que la faute est un manquement à une obligation préexistante de quelque nature qu'elle soit²⁷, et que l'obligation lie un débiteur à son créancier en donnant à celui-ci le droit d'exiger une prestation ou une abstention²⁸, le droit commun sénégalais de la responsabilité retient qu'est responsable celui qui, par sa faute, cause un dommage à autrui²⁹. Le législateur sénégalais de prescrire que c'est le dommage, pouvant être matériel ou moral³⁰, actuel ou futur³¹ et devant toujours³² être certain³³ ou direct³⁴, qui est générateur de responsabilité s'il porte atteinte à un droit³⁵. Il a également consacré la responsabilité du fait d'autrui³⁶, des animaux et des choses³⁷.

En droit français, la combinaison de plusieurs articles du Code civil permet de retenir qu'on est responsable non seulement du dommage que l'on cause par son propre fait³⁸, par sa négligence ou par son imprudence³⁹, mais aussi de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses dont on est propriétaire⁴⁰ ou que l'on a sous sa garde⁴¹. Par ailleurs, le propriétaire d'un animal, ou celui qui s'en sert, pendant qu'il est à son usage, est responsable du dommage que l'animal a causé, soit que l'animal fût sous sa garde, soit qu'il fût égaré ou échappé⁴². C'est dire, en conséquence, que tout fait

²⁶ Directive n° 2000/31/CE 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 dite « *directive sur le commerce électronique* », JOCE 17 juillet 2000, n° L 178, pp. 1-16, (voir aussi sur www.legifrance.gouv.fr, site visité le 15 janvier 2016).

²⁷ Article 119 du Code des Obligations Civiles et Commerciales (COCC).

²⁸ Article 1^{er} du COCC.

²⁹ Article 118 COCC.

³⁰ Article 124 COCC.

³¹ Article 125 COCC.

³² *Ibidem*.

³³ Article 126 COCC

³⁴ Article 127 COCC

³⁵ Article 124 COCC

³⁶ Article 142 COCC

³⁷ Article 137 COCC

³⁸ Article 1384 Code civil

³⁹ Article 1383 Code civil

⁴⁰ Article 1386 Code civil

⁴¹ Article 1384 Code civil

⁴² Article 1385 Code civil

quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer⁴³.

Quant au « *prestataire technique* », il s'agit, au sens de l'article 2-3 de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, de « *tout prestataire utilisant les protocoles de l'Internet qui met à la disposition des personnes physiques ou morales, publiques ou privées, des biens et services* ». En clair, aux termes de l'article 3-1 et 2 de la même loi, les prestataires techniques sont composés aussi bien des « *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, [que 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* ». Ces mêmes précisions définitionnelles⁴⁴, au relent descriptif, ont été retenues par le législateur français⁴⁵ aux points 1 et 2 de l'article 6-I de la LCEN.

Aussi, sont-ils appelés « *les prestataires de service Internet ou intermédiaires techniques* »⁴⁶ comparativement aux acteurs d'Internet, dont ils font d'ailleurs partie. Le fonctionnement d'Internet repose alors sur ces personnes physiques et morales que sont d'une part l'opérateur de télécommunication - exemples : *Bouygues Telecom, Numéricâble, Free, Orange, Expresso, Tigo* - assurant la fourniture d'accès à Internet par l'entremise d'une prestation de transport des données au moyen d'infrastructures techniques, et offrant aux utilisateurs d'Internet la possibilité de se connecter au réseau, généralement en contrepartie d'un prix déterminé, d'autre part le fournisseur d'hébergement ou l'hébergeur - exemples : *Google Inc., YouTube, Dailymotion, Facebook, Twitter* - qui met à la disposition des utilisateurs l'espace nécessaire, sur ses serveurs, au stockage de leurs données. Au Sénégal, l'Agence De l'Informatique de l'Etat (ADIE) est le fournisseur d'accès à Internet pour l'administration et ses usagers⁴⁷. Elle assure la fourniture du⁴⁸ « *large bande* »⁴⁹ aux bâtiments administratifs ainsi que les services à ses usagers.

⁴³ Article 1382 Code civil

⁴⁴ T. Patrick, « *Evolutionnisme et linguistique* », Vrin, Paris, 1980, p. 27.

⁴⁵ Avant son homologue sénégalais, puisque la LCEN - JORF n° 143 du 22 juin 2004 texte n° 2/108 page 11168- précède de 4 ans la loi sénégalaise sur les transactions électroniques.

⁴⁶ C. Christine, « *La responsabilité des intermédiaires techniques* », La Documentation Française. Paris, 2004, p. 108 ; R. Jean-Michel, P. Geneviève, P. Emmanuèle, « *La mémoire de la société de l'information* », Jouve, Paris, 2003, p. 36 ; N. Cécile, « *La protection du mineur dans le cyberspace* » Thèse, Université de Picardie Jules Verne, Amiens, 2007, p. 6.

⁴⁷ Dans une interview accordée au bimestriel africain spécialisé dans le domaine des technologies de l'information et de la communication, le Directeur général de l'ADIE, M. Cheikh BAKHOUM, a déclaré : « *l'ADIE est le fournisseur du large bande pour l'administration et ses usagers. Et gère les infrastructures télécoms et l'accès Internet des bâtiments administratifs ainsi que les services aux usagers (téléphone fixe, Internet filaire, 3G).* » In CIOMag n° 39, décembre 2015 – janvier 2016, p. 34 ; interview publiée aussi sur le site officiel de l'ADIE à l'adresse suivante : www.adie.sn/fr/le-directeur-général-de-l-adie-dans-cio-mag, site visité le 23 septembre 2016.

⁴⁸ L'expression « *large bande* » est une expression consacrée, elle est bien masculine.

⁴⁹ Les services « *large bande* » (ou accès à Internet à large bande, par traduction littérale du terme anglais *broadband*) établissent des connexions Internet au moins cinq fois plus rapides que l'accès téléphonique, par modem ; ce qui permet à l'utilisateur d'accéder aux informations beaucoup plus efficacement qu'auparavant. Source : www.itu.int ou <https://www.itu.int/osg/spu/spunews/2003/oct-dec/broadband-fr.html>, site visité le 23 septembre 2016.

En tous les cas, tant la doctrine, les législateurs français et sénégalais que les techniciens⁵⁰ en informatique et les informaticiens⁵¹ subdivisent les prestataires techniques en deux familles : les « fournisseurs d'hébergement » ou « hébergeurs » et « les fournisseurs⁵² d'accès à Internet » ou FAI⁵³.

La réflexion que voici s'efforcera, tant bien que mal et sous réserve des imperfections juridiques et cognitives qu'elle comporterait, de s'articuler autour de la responsabilité de ces prestataires techniques, non sans l'éclairage des droits positifs sénégalais et français. A ce titre, depuis plusieurs années, une préoccupation est au cœur des débats juridiques en rapport avec les transactions électroniques. En effet, si la responsabilité de l'éditeur d'un contenu souffre de doute, celle des prestataires techniques l'est moins. Le droit sénégalais et celui français semblent esquisser un début de réponse à travers respectivement la loi n° 2008-08 du 25 janvier 2008 et la LCEN. Mais à vrai dire, le nœud ne semble toujours pas entièrement défait.

Alors, irréfutablement, l'on est en droit de se demander : quel est le degré d'engagement de la responsabilité des prestataires techniques en cas de fautes commises sur Internet ?

L'évolution actuelle d'Internet est à un niveau tel que les prestataires techniques sont omniprésents et incontournables dans la transmission et l'hébergement des contenus. A partir du moment où ce sont eux qui assurent l'accès des tiers au *Web* et le transport de leurs contenus qu'ils stockent aussi, penser les détails de leurs actes juridiques⁵⁴, à l'aune du degré d'engagement de leur responsabilité, contribuerait au rétablissement d'un certain ordre sur la Toile⁵⁵, possiblement au Sénégal et en France.

Cela est d'autant plus probable que, pour le moment, les conditions juridiques semblent réunies, en tout cas en France et davantage au Sénégal. Ces pays ont un régime de responsabilité plutôt aménagé et *a priori* favorable aux prestataires techniques. Mais cela semble insuffisant, et l'expérience du *Deep Web*⁵⁶ est assez éloquente pour faire bouger les lignes juridiques sur Internet, notamment au sujet de la

⁵⁰ Un technicien en informatique ou en maintenance informatique est un professionnel qui s'occupe du parc informatique, de l'entretien des ordinateurs et des éléments liés à l'univers ou au côté « *hard* » de l'informatique. Source : Enquêtes menées en février 2016 à Ziguinchor.

⁵¹ Un informaticien est un professionnel de l'étude, la conception, la programmation, la production, la gestion et/ou la maintenance des systèmes de traitement de l'information. Il s'occupe du côté « *soft* » de l'informatique. Source : *Ibidem*.

⁵² Ce concept sera rencontré plusieurs fois dans cette réflexion. En mettant tout court, au singulier, « le (au) fournisseur d'accès à Internet », nous entendrons utiliser la même expression, sous sa forme générique.

⁵³ On l'appelle aussi « *Provider* » (*Fournisseur*) ou encore « *ISP* », sigle pour « *Internet Service Provider* (en Français, « *Fournisseur de Services Internet* »). C'est un service, généralement payant, permettant de se connecter à Internet. Source : Orange, Tigo et Expresso /Ziguinchor

⁵⁴ M. Benoît, « *De l'acte et du fait juridique ou d'un critère de distinction incertain* », Article publié dans la revue juridique *Thémis*, Montréal, 1997, p. 6 : « *l'acte juridique est la réalisation matérielle du pouvoir de la volonté sur le droit. Il se présente dans tous les domaines juridiques.* »

⁵⁵ D. Abdoul Aziz, « *Essai sur le régime juridique des noms de domaine* », Thèse, Université d'Orléans, 2010, p. 9 : « *la Toile est une forme d'analogie de l'Internet imaginé comme une toile d'araignée mondiale, un World Wide Web.* »

⁵⁶ Le *Deep Web* ou Internet Profond est la face cachée d'Internet où rien n'est référencé. Il regorge d'informations illégales qui ne sont pas publiables sur le *Web* grand public sous peine de poursuites pénales et de prison. On peut y trouver très facilement toutes sortes de marchés noirs, de la drogue, des armes de guerre et le trafic d'organes ; les achats s'y font avec la monnaie virtuelle Bitcoin. Source : [www.hitek.fr](http://hitek.fr) ou suivre le lien <http://hitek.fr/actualite/deep-web-face-cachee-internet> 259, site visité le 15 mars 2016.

responsabilité des prestataires techniques. Ce Web profond fonctionne principalement à l'aide de logiciels⁵⁷ cryptés dont le plus connu est TOR⁵⁸. Il constitue une sorte de zone de non-droit et, par conséquent, une zone de prédilection des cybercriminels agissant au plan international ; ce qui fait que sur Internet, les enjeux sont divers, les défis multiples, complexes et pour le moins trop longs à relever. L'espace numérisé que constitue le cyberspace en général, Internet en particulier, est actuellement un lieu non négligeable pour la commission d'agissements répréhensibles de toutes sortes, attentatoires tant aux intérêts des particuliers qu'à ceux de la chose publique⁵⁹.

Et puis, le caractère volatile de la Toile et l'anonymat qui y est presque devenu une norme contribuent non seulement à brouiller les pistes et repères du système pénal dont les réponses traditionnelles et permanentes, conçues et élaborées pour un environnement matérialisé et national, se sont vite révélées quelque peu inappropriées et inadaptées pour une meilleure préhension de cette nouvelle réalité⁶⁰. Pis, l'audit de la législation sénégalaise, avant l'adoption de la loi portant sur la cybercriminalité, a révélé des situations juridiques dans lesquelles les systèmes informatiques⁶¹, les données informatisées⁶² et les réseaux informatiques⁶³ ont été la cible d'agissements cybercriminels⁶⁴. Actuellement, cela va sans doute *crecendo*⁶⁵. D'ailleurs, on assiste d'autant plus à une recrudescence de la cyberdélinquance⁶⁶, que l'expansion du cyberspace, favorisant par là-même l'explosion des transactions électroniques⁶⁷, passe par des supports informatiques chaque jour plus nombreux, divers, mobiles, mais aussi plus interactifs⁶⁸ avec les réseaux sociaux ; une bonne partie étant utilisée à mauvais escient⁶⁹.

⁵⁷ Un logiciel est un ensemble de programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données. Source : www.biz-en-or.com ou <http://www.biz-en-or.com/les-outils-indispensables/logiciel-application-plugin-script-quelle-est-la-difference/>, site visité le 3 mars 2016.

⁵⁸ TOR : acronyme pour « *The Onion Router* » (Le Router Oignon), est un logiciel libre sous licence BSD révisée. Comme un oignon, il est un réseau informatique superposé mondial et décentralisé. Il se compose d'un certain nombre de serveurs, appelés nœuds du réseau. Ce réseau permet d'anonymiser l'origine de connexions Internet. Source : www.wikipedia.org, site visité le 22 mars 2016

⁵⁹ In exposé des motifs de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité, JORS n° 6406 du Samedi 3 mai 2008.

⁶⁰ *Ibidem*.

⁶¹ Article 431-7, point 6 de la loi sur la cybercriminalité : « *Un système informatique est 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* ».

⁶² Article 431-7, point 2 de la loi sur la cybercriminalité : « *les données informatisées consistent en toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique* »

⁶³ Un réseau informatique permet de relier, physiquement ou via les ondes radio, un ensemble de serveurs et de postes de travail dans le but d'échanger des données et des informations de façon sécurisée.

Source : www.reseau-informatique.prestataires.com, site visité le 20 septembre 2016.

⁶⁴ *Op. cit.* note 59.

⁶⁵ C. Nicolas, M. Pierre-Alain, « *La société de l'information* », La Documentation française, Paris, 2004, p. 110.

⁶⁶ Selon le "JURIDICTIONNAIRE" (ou recueil des difficultés et des ressources du français juridique), réalisé pour le compte du Centre de Traduction et de Terminologie Juridiques de l'Université de Moncton, par Jacques PICOTTE, actualisé au 13 juillet 2015, page 1315 : « *la cyberdélinquance englobe toute action illicite visant les systèmes informatiques soit comme formant l'objet du délit, soit comme constituant le moyen de commettre l'infraction. Le cyberdélinquant pourra ainsi utiliser l'ordinateur pour diffuser des contenus illicites, procéder à des extorsions de fonds, commettre des actes de fraude commerciale, proférer des menaces ou se livrer à la cyberdélinquance.* »

⁶⁷ A titre illustratif, 29 transactions d'achat sont enregistrées en France chaque seconde par les sites d'e-commerce, contre 19 en 2013 et 10 en 2010. Cela représente plus de 850 millions de transactions en 2015. Il y a environ 150 000 sites marchands d'e-commerce actifs en France. Source : www.planetoscope.com, site visité le 26 mars 2016.

⁶⁸ Cf. *Supra* Web 3.0 et IoT.

⁶⁹ L'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP) évalue le préjudice subi par la France à cause de la cybercriminalité à 1,7 milliards d'euros. Cet observatoire a recensé 33 905 infractions qualifiées de « *délinquance astucieuse* » sur Internet dont

Pour ces raisons, le besoin s'est fait ressentir de trouver à côté de l'auteur proprement dit de l'acte fautif, de nouveaux responsables plus facilement localisables, plus solvables, et dans certains cas, géographiquement plus proches⁷⁰. Ce sont, en l'espèce, ceux-là qui, justement, jouissent de prérogatives monopolistiques consistant pour les uns à mettre à disposition et héberger des sites Internet dont ils stockent les contenus, pour les autres à permettre l'accès du public à ces sites afin d'y poster des contenus⁷¹. Etant donné l'importance de ces prestataires techniques, c'est tout naturellement de leur côté que les regards des législateurs pourraient et devraient se tourner ; ceci, d'autant plus qu'ils peuvent directement intervenir pour remédier à la commission d'un acte illicite sur le réseau.

Ainsi, afin de mener à bien cette réflexion, semble-t-il important d'étudier d'abord la responsabilité dérogatoire des fournisseurs d'accès à Internet (Première partie), puis la responsabilité aménagée des hébergeurs (Seconde partie).

80 % étant des escroqueries ou des abus de confiance, les 20% restant correspondant à des falsifications ou usages de cartes de crédit. Source : 7^{ème} Rapport, 2011.

⁷⁰ C. Nicolas, M. Pierre-Alain, « *La société de l'information* », La Documentation française, Paris, 2004, p. 108.

⁷¹ Nous entendons par ce vocable, tous types et formats de documents numériques. S'il est utilisé au singulier, il l'est alors génériquement.

Première partie

La responsabilité dérogatoire des fournisseurs d'accès à Internet

A une nuance près, en France et au Sénégal, les fournisseurs d'accès à Internet appartiennent à la famille des transmetteurs⁷² ou encore des transporteurs de messages, d'informations, en somme, de contenus. La consécration de cette fonction au fournisseur d'accès est d'ailleurs d'origine prétorienne. Elle sera reprise par une directive du Parlement européen et du Conseil sur le commerce électronique transposée par la LCEN. En effet, alors qu'Internet était à ses débuts en France, la Cour de cassation a rendu un arrêt de principe dans lequel il considérait, en matière télématique, que *France Télécom*⁷³ n'était qu'« un simple transporteur de messages »⁷⁴.

La conséquence de ce principe a été qu'en rendant une telle décision, la jurisprudence a jugé que *France Télécom* était alors exonérée de toute responsabilité en cas de commission d'une faute sur son réseau. Les juges ont considéré qu'il n'était pas établi que l'opérateur, en sa qualité de « simple transporteur de messages », avait eu « connaissance de la violation d'engagements conventionnels avant ou au moment de la commission des infractions »⁷⁵. En clair, ces transporteurs de contenus sont les personnes dont l'activité est d'offrir un accès à des services de communication au public⁷⁶ en ligne. Or, sur le fondement de l'article 1^{er} de la LCEN⁷⁷ et de l'article 2 de la loi sur les transactions électroniques⁷⁸, la communication au public en ligne est définie comme étant « toute transmission de données numériques, sur demande individuelle, n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique, permettant un échange réciproque ou non d'informations entre l'émetteur et le récepteur ».

Même s'ils ne sont pas des hébergeurs à proprement parler de sites Internet, dont l'activité est de stocker dans des installations techniques conçues, dédiées et habilitées à cela, les fournisseurs d'accès effectuent, en outre, des opérations dites de « caching »⁷⁹, consistant à enregistrer temporairement les données disponibles sur le réseau, auxquelles leurs abonnés accèdent fréquemment dans le seul but de préserver et d'améliorer la fluidité de leurs opérations de transmission.

⁷² Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS n° 6439 du Samedi 22 novembre 2008, notamment en son article 6.

⁷³ France Télécom : 'Orange' depuis le 1er juillet 2013, était une société française de télécommunications. Source : www.wikipedia.org, site visité le 26 mars 2016

⁷⁴ *Cass. crim.*, 17 novembre 1992, n° 91-84.848, *Légipresse* 1993, n° 98, III, p. 1 et s., TGI de Draguignan, 15 mai 1992, *Petites affiches* 23 nov. 1992, p. 12, obs. Huet J.

⁷⁵ *Ibidem.*

⁷⁶ Articles 6-I-1 de la LCEN et 3-1 de la loi sur les transactions électroniques.

⁷⁷ Article 1^{er}-IV-4 LCEN : « On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur ».

⁷⁸ Article 2-5 de la loi n° 2008-8 du 25 janvier 2008 portant sur les transactions électroniques : « service de communication au public en ligne : toute transmission de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique utilisant le réseau Internet permettant un échange réciproque ou non d'informations entre l'émetteur et le récepteur. »

⁷⁹ En informatique, le 'caching' est un enregistrement temporaire des copies de données provenant d'une source, afin de diminuer le temps d'un accès ultérieur pour lecture par un matériel informatique en particulier, en général un processeur à ces données. Source : Enquêtes réalisées auprès d'informaticiens en mars 2016. En droit de l'informatique, voir l'article 13 de la directive sur le commerce électronique : *Dir. Cons.* CE n° 2000/31, 8 juin 2000, *JOCE* 17 juillet 2000, n° L 178, pp. 1-16.

En France, les fournisseurs d'accès rentrent ainsi dans le champ d'une autre définition légale. C'est celle prévue par l'article L 32-3-4 du Code des postes et des communications électroniques⁸⁰, introduit par l'article 9 de la LCEN. En effet, le législateur français⁸¹ prévoit que les fournisseurs d'accès préoccupés par un souci de rapidité, de pragmatisme ou d'efficacité quant à la transmission ultérieure des contenus, peuvent bel et bien s'autoriser à assurer une activité de stockage automatique, intermédiaire et temporaire de ces contenus. Ce faisant, et se limitant à ce seul but, les fournisseurs d'accès ne peuvent en principe et *a priori* voir leur responsabilité civile ou pénale engagée.

Ce qui amène à constater que ce régime, pour le moins dérogatoire, consacre ainsi l'irresponsabilité principale (Chapitre 1^{er}) de ces prestataires techniques, mais qui est atténuée par une série d'obligations d'information, de moyens, de contrôle, de surveillance et de résultat (Chapitre 2).

⁸⁰ Loi n° 2004-575 du 21 juin 2004 art. 9-I Journal Officiel du 22 juin 2004, <http://www.arcep.fr/fileadmin/reprise/textes/lois/cpce-legis.pdf>, site visité le 22 septembre 2016.

⁸¹ En fait, cette disposition n'est que la transposition dans le droit national français, de l'article 13 de la directive n° 2000/31 du 8 juin 2000, JOCE 17 juillet. 2000, n° L 178, pp. 1-16, qui vise les prestataires réalisant un « *stockage automatique, intermédiaire et temporaire [d'une] information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service* ».

CHAPITRE 1^{er} : L'irresponsabilité principale

Le législateur sénégalais a prévu un principe général selon lequel le fournisseur d'accès à Internet, en d'autres termes celui qui assure la mise à disposition au public des biens et services par le biais des technologies de l'information et de la communication⁸², peu importe qu'il ait la qualité de personne physique ou morale, agissant à titre professionnel ou à titre simplement gratuit, ne saurait être responsable⁸³ des activités menées par son client ou par un tiers sur Internet, du simple fait qu'il lui y aurait rendu possible l'accès.

Il s'agirait là d'une absence *a priori* de la responsabilité civile et pénale (Section 1^{ère}) au sens où il est bien possible que le fournisseur d'accès à Internet puisse engager sa responsabilité du fait personnel (Section 2).

Section 1^{ère} : L'absence *a priori* de la responsabilité civile et pénale

Il est évident que, de prime abord, la responsabilité civile et celle pénale présentent des différences considérables, car non seulement le délit pénal ne peut résulter que d'une infraction⁸⁴ à une loi qui interdit un acte ou une omission sous la sanction d'une peine⁸⁵ tandis que le délit civil existe toutes les fois qu'il y a une faute⁸⁶, sans qu'on ait besoin d'en préciser les éléments constitutifs⁸⁷, mais aussi le délit pénal existe même s'il n'a pas été suivi de dommage, la loi visant alors l'action coupable sans que l'on ait à en rechercher les conséquences⁸⁸. Par contre, le délit civil n'est pris en considération que s'il a entraîné un préjudice à une autre personne. Ainsi, existe-t-il, d'une part, des délits pénaux n'entraînant pas de responsabilité civile, notamment en cas de tentative ou d'infractions ne portant atteinte ni aux personnes ni

⁸² Article 3-2 de la loi n° 2008-8 du 25 janvier 2008 portant sur les transactions électroniques.

⁸³ *Ibidem*.

⁸⁴ L. Jean, « Droit pénal général » : « l'infraction est un acte ou une omission interdit par la loi sous menace d'une peine. » et Émile Auguste GARÇON (26 septembre 1851 - 12 juillet 1922), in « Code pénal annoté » : « on appelle infraction pénale tout fait prévu et puni par la loi d'une peine proprement dite. » Source : Le dictionnaire de droit criminel, ou sur

http://ledroitcriminel.fr/dictionnaire/lettre_i/lettre_i_infraction.htm, site visité le 3 mars 2016

⁸⁵ *Ibidem*.

⁸⁶ Cf. *Supra* in « Introduction » pour la définition de « la faute ».

⁸⁷ P. Marcel, « Traité élémentaire de droit civil », 4^e éd., 1952, n° 907 ; Marcel PLANIOL définit la « faute civile » comme étant « le manquement à une obligation préexistante », n° 91, cité par P. Jean-Denis in « Le principe de l'unité des fautes civile et pénale à l'épreuve de la loi du 10 juillet 2000 », Université Paul Cézanne – Aix-Marseille III, 2005, p. 7

⁸⁸ P. Jean-Denis, « Le principe de l'unité des fautes civile et pénale à l'épreuve de la loi du 10 juillet 2000 », Université Paul Cézanne – Aix-Marseille III, 2005, p. 7

aux biens⁸⁹, et d'autre part des hypothèses encore plus variées de délits civils non réprimés par la loi pénale⁹⁰.

Il ne serait pas anodin de faire remarquer qu'en plus de ces différences techniques, il existe une dualité fonctionnelle entre la responsabilité civile et celle pénale. En effet, le premier objectif de la responsabilité pénale est la neutralisation des individus nuisibles à la société. Enrico FERRI⁹¹ expliquait que pour ce faire, en réagissant contre un acte antisocial⁹², la société n'avait plus besoin de prendre en considération les conditions psychologiques du délinquant. Son second objectif est une meilleure réinsertion du délinquant puni, alors que la responsabilité civile est plutôt tournée vers la réparation du préjudice causé. Toutefois, François TERRE⁹³ considère que dans une certaine mesure, la sanction pénale et la sanction civile répondent à un double désir de punition et de dissuasion⁹⁴.

Et puis, dans le domaine non-intentionnel, les deux responsabilités ont les mêmes éléments constitutifs : une faute d'imprudence ou de négligence dont découle un préjudice matériel ou corporel en droit civil, tandis que le droit pénal ne réprime, à une exception près en droit pénal français⁹⁵ et même sénégalais⁹⁶, que les atteintes à l'intégrité physique d'une personne lorsqu'elles résultent d'une telle faute⁹⁷. D'autre part, il n'y a pas de responsabilité pénale pour faute d'imprudence s'il n'en est pas résulté un dommage corporel, excepté, en droit français, les cas de risques causés à autrui, qui constituent une hypothèse quelque peu particulière⁹⁸.

A la lumière de ce court rappel, qui semble utile à ce stade de cette réflexion, force est de constater que les législateurs sénégalais et français ont préféré faire abstraction de ce droit commun lorsqu'il a fallu

⁸⁹ C'est le cas des infractions prévues au Livre IV du Code pénal français, contre la Nation, l'Etat et la paix publique ; et celles prévues au Livre III, Titre 1^{er} du Code pénal sénégalais contre la chose publique, voir sur www.justice.gouv.sn ou www.juricaf.org, sites visités le 02 février 2016.

⁹⁰ C'est, à titre illustratif, le cas du stellionat, délit civil consistant à vendre ou hypothéquer à une personne, au moyen d'affirmations mensongères ou de réticences un bien immeuble qu'on savait déjà vendu ou hypothéqué à une autre personne.

⁹¹ Enrico FERRI (1856-1929) fut Professeur à l'Université de Rome et à l'Université nouvelle de Bruxelles.

⁹² F. Enrico, « *La sociologie criminelle, Chapitres III et IV* », Édition complétée, mars 2005, Chicoutimi, p.110

⁹³ François TERRE, né le 23 juillet 1930 à Paris, est Professeur Emérite de l'Université de Droit Paris II Panthéon-Assas. Depuis 1995, il est membre de l'Institut de France - Académie des Sciences Morales et Politiques, section "Législation, Droit public et Jurisprudence" -. Source : www.asmp.fr ou suivre le lien http://www.asmp.fr/fiches_academiciens/TERRE.HTM, site visité le 15 septembre 2016.

⁹⁴ V. A. Tunc, « *Responsabilité civile et dissuasion des comportements antisociaux, Aspects nouveaux de la pensée juridique* », Mélanges Ancel, 1975, t. I, p. 407 et s. cité in « *Droit civil, Les obligations* », 2^{ème} éd. DALLOZ, 2002, p. 657, François TERRE, Philippe SIMLER et Yves LEQUETTE.

⁹⁵ Art. 322-5 al. 1^{er} du Code pénal français : « *la destruction, la dégradation ou la détérioration involontaire d'un bien appartenant à autrui par l'effet d'une explosion ou d'un incendie provoqués par manquement à une obligation de sécurité ou de prudence imposée par la loi ou le règlement est punie...* »

⁹⁶ Article 307, al. 1^{er} du Code pénal sénégalais : « *quiconque, par maladresse, imprudence, inattention, négligence ou inobservation des règlements, aura commis involontairement un homicide ou des blessures, ou en aura été involontairement la cause, sera puni...* »

⁹⁷ Cf. *Supra* in « *Introduction* » pour la définition de « *la faute* ».

⁹⁸ Cf. Code pénal : Titre II (Des atteintes à la personne humaine), Chapitre III (De la mise en danger de la personne), Section 1 (Des risques causés à autrui), art. 223-1 « *le fait d'exposer directement autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente par la violation manifestement délibérée d'une obligation particulière de prudence ou de sécurité imposée par la loi ou le règlement est puni d'un an d'emprisonnement et de 15 000 euros d'amende.* »

déterminer le régime juridique⁹⁹ des prestataires techniques. Ils leur ont *ipso facto* concédé un régime spécial de responsabilité ; à commencer, pour les fournisseurs d'accès à Internet, par les exigences, d'une part de neutralité et d'exclusivité fonctionnelles (Paragraphe 1^{ère}) dans la transmission¹⁰⁰ de contenus, d'autre part d'exécution d'une décision judiciaire ou administrative (Paragraphe 2).

Paragraphe 1^{er} : L'exigence de neutralité et d'exclusivité fonctionnelles

Le fournisseur d'accès à Internet doit non seulement se conformer à l'exigence de neutralité (A) prévue dans le cadre de l'exercice de sa fonction, mais aussi s'attacher à l'objet exclusif de celle-ci (B).

A : La neutralité fonctionnelle

Le législateur sénégalais et son homologue français estiment que pour ne pas engager sa responsabilité pénale ou civile, le fournisseur d'accès à Internet, professionnel ou non, est tenu à l'obligation de neutralité quant au contenu qu'il transporte. En d'autres termes, dans l'exercice de sa fonction, il doit se garder d'influencer aussi bien le contenu et ceux qui ont contribué à sa création, que sa destination et son destinataire.

En France, la consécration de cette obligation ne date pas d'aujourd'hui. En effet, avant l'avènement de la LCEN, le législateur l'avait déjà prévue dans l'ancien Code des postes et télécommunications - et bien avant même¹⁰¹ - devenu l'actuel Code des postes et des communications électroniques, notamment en son article L 32-1-II-6° qui impose aux opérateurs de communications électroniques le respect du principe de neutralité vis-à-vis du contenu des messages qu'ils transmettent.

Quant à la LCEN, transposition de la directive du 8 juin 2000¹⁰² du Parlement européen et du Conseil, même si elle n'a pas expressément évoqué l'obligation de neutralité des fournisseurs d'accès à Internet, elle a en revanche rétabli les articles L 32-3-2 et L 32-3-3 du code ci-devant cité, avant d'insérer en guise de complément, l'article L 32-3-4 qui prévoit toute une cascade¹⁰³ de responsabilités conditionnelles. C'est dire que le principe de neutralité prévaut pour l'exercice de l'activité de ce prestataire technique. Le professeur Tim WU¹⁰⁴ considère que ce principe est la condition *sine qua non*¹⁰⁵ de son

⁹⁹ Article 2-3 de la loi sur les transactions électroniques et articles 6 -2 et 3 de la LCEN.

¹⁰⁰ Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, notamment en son article 6.

¹⁰¹ En 1986 déjà, l'ancêtre de ce code, à savoir la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), JORF du 1 octobre 1986 page 11755 (voir https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000512205 , site visité le 20 juillet 2016) consacrait le « principe de neutralité technologique » aux termes des articles 3-1 et 99.

¹⁰² Directive n° 2000/31/CE 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 dite «directive sur le commerce électronique», JOCE 17 juillet 2000, n° L 178, pp. 1-16.

¹⁰³ Article 3-I de la LCEN

¹⁰⁴ Tim WU est Professeur de Droit à la New-York Columbia University. Il est connu pour avoir nommé et popularisé le concept de « Neutralité sur Internet » dans son article « Network Neutrality, Broadband Discrimination », contribuant à l'adoption d'une loi fédérale américaine à ce sujet en 2010.

¹⁰⁵ W. Timothy dit Tim. « Network Neutrality, Broadband Discrimination », article, "Journal of Telecommunications and High Technology Law", n° 2, New York, 2003. p. 141-179 : « la neutralité doit être comprise comme un principe d'architecture de réseau. L'idée est qu'un

immunité. La neutralité est, de ce fait, l'une des premières¹⁰⁶ d'une série d'obligations atténuant le caractère dérogatoire de la responsabilité du fournisseur d'accès à Internet.

Au Sénégal, c'est en 2001 que le législateur a imposé le principe de neutralité aux exploitants des réseaux de télécommunications ouverts au public et aux fournisseurs de services ainsi qu'à leurs personnels. En effet, l'ancien Code des télécommunications¹⁰⁷ du Sénégal avait prévu l'obligation, pour ces derniers, d'assurer à leurs clients¹⁰⁸ et aux tiers des « *conditions optimales de confidentialité et de neutralité du service au regard des messages transmis* »¹⁰⁹. L'article 7 du Code des télécommunications de 2011 reconduira les mêmes dispositions.

En France, le législateur a créé un certain nombre de relations dynamiques¹¹⁰ entre la LCEN et le Code des postes et des communications électroniques qu'il a mis à jour, à la différence de son homologue sénégalais qui n'a pas procédé ainsi, pas plus qu'il n'a explicitement prévu le principe en question dans la loi sur les transactions électroniques. Sans doute, le choix du législateur sénégalais est-il davantage une invite à s'intéresser à la *ratio legis*¹¹¹ pour entrevoir ce principe, plutôt qu'à se limiter à la lettre des dispositions légales. Peut-être même qu'à l'instar de la considération qu'a le Doyen CARBONNIER¹¹² de l'équité, il serait admissible de retenir du principe de la neutralité qu'« *elle se sent, elle ne se définit pas* »¹¹³.

Quoi qu'il en soit, il est prévu, aussi bien dans la loi sur les transactions électroniques que dans l'un de ses décrets¹¹⁴ d'application, des dispositions exigeant en filigrane le respect du principe de neutralité par les prestataires techniques, en l'espèce les fournisseurs d'accès à Internet. L'article 6 de ce décret conditionne, par exemple, l'exonération de la responsabilité de ces prestataires techniques au fait qu'ils se

réseau d'information publique est d'autant plus efficace qu'il aspire à traiter tous les contenus, sites et plateformes de la même manière », traduit de l'Anglais par Stéphane COUTURE, in « *Neutralité d'Internet. Ou Internet comme bien commun* » 2014, p. 4

¹⁰⁶ En effet, il a été prévu depuis le Code des postes et télécommunications qui encadrait déjà les balbutiements de l'Internet en France et même bien avant.

¹⁰⁷ Avec l'avènement de la loi n° 2001-15 du 27 décembre 2001 portant Code des télécommunications, JORS N° 6030 du samedi 16 février 2002, voir aussi sur www.gouv.sn, site visité le 15 juin 2016.

¹⁰⁸ Le législateur vise, dans le Code de 2001, les « *consommateurs* » sans pour autant les définir. C'est seulement dans le Code de 2011 (loi n° 2011-01 du 04 février 2011 portant Code des télécommunications, JORS, N° 6576 du lundi 4 mars 2011, page 273, voir aussi sur www.gouv.sn, site visité le 15 juin 2016) qu'il les définit comme étant : « *toute personne physique qui utilise ou demande un service de télécommunications accessible au public à des fins autres que professionnelles* ».

¹⁰⁹ Articles 7 et 22 du Code des télécommunications de 2001.

¹¹⁰ A titre illustratif, le législateur français a procédé au rétablissement des articles L 32-3-2 et L 32-3-3 du Code des postes et des communications électroniques tout en y insérant l'article L 32-3-4.

¹¹¹ S. Alain, B. Marc, « *Le commentaire de textes juridiques : lois et règlements* », 2^{ème} éd., Ellipses, Paris, 2007, p. 10.

¹¹² Jean CARBONNIER (1908-2003), ses études juridiques et l'agrégation des facultés de droit l'ont conduit, entre 1937 et 1955, à être Professeur à l'Université de Poitiers, dont il fut doyen. De cette époque lui est resté ce titre inséparable de son nom dans les milieux juridiques : « *le Doyen Carbonnier* ». Source : Encyclopædia Universalis ou suivre le lien <http://www.universalis.fr/encyclopedie/jean-carbonnier/>, site visité le 1er octobre 2016.

¹¹³ C. Jean, « *Les notions à contenu variable dans le droit français de la famille* », in « *Centre national de recherches de logique* », travaux publiés par Chaïm PERELMAN et R. VANDER ELST, « *Les notions à contenu variable en droit* », Bruxelles, Bruylant, 1984, pp. 99-112, p. 106, cité par Lydie DUTHEIL-WAROLIN in « *La notion de vulnérabilité de la personne physique en droit privé* », Thèse, Université de Limoges, 2004, p. 26.

¹¹⁴ Il s'agit du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

contentent « du stockage automatique ou temporaire de l'information ou de jouer un rôle d'intermédiation dans la transmission » de celle-ci.

A côté de la neutralité, dont doit faire preuve le fournisseur d'accès à Internet pour ne pas engager sa responsabilité civile ou pénale dans l'exercice de sa fonction, il convient de retenir l'exigence de se consacrer exclusivement à l'objet de celle-ci.

B : L'exclusivité fonctionnelle

Cette exclusivité consiste en une conduite que le fournisseur d'accès à Internet doit tenir tant qu'il agit dans le cadre de sa fonction ou qu'il joue son rôle. En effet, s'il est exonéré de sa responsabilité pour avoir été neutre¹¹⁵, il est surtout tenu de ne se limiter qu'aux activités visant exclusivement l'exécution de la transmission ou de la fourniture d'accès¹¹⁶.

En l'espèce, même si, ni la loi sur les transactions électroniques ni la LCEN ne prévoient formellement que le fournisseur d'accès à Internet est, à ce niveau, considéré comme étant le débiteur d'une obligation de ne pas faire, cela semble toutefois le cas, puisqu'il doit s'abstenir de faire autre chose que ce qui rentre dans le cadre de sa fonction, sous peine d'engager sa responsabilité, notamment civile. Pour rappel, en droit commun¹¹⁷ le débiteur de l'obligation de ne pas faire a un devoir d'abstention, sans quoi il est tenu à réparation¹¹⁸. D'ailleurs, au cas où l'obligation ne serait que de se consacrer exclusivement aux activités liées à sa fonction de fournisseur d'accès à Internet, le fait de l'enfreindre devrait l'amener au paiement de dommages et intérêts¹¹⁹.

En outre, si le fournisseur d'accès à Internet, en tant que personne physique, ne se limite pas exclusivement aux activités liées à l'exécution de la transmission ou de la fourniture d'accès, il engage sa responsabilité pénale. Au Sénégal, cela découle des dispositions de l'article 431-45 de la loi sur la cybercriminalité¹²⁰ qui fait état de « toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale » dont l'activité est la fourniture d'accès à Internet. Le législateur sénégalais a prévu, à cet effet, des sanctions allant d'un emprisonnement de 6 mois à 1 an, à une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines, pour non respect des prescriptions de l'article 3 de la loi sur les transactions électroniques, qui encadre les activités des fournisseurs d'accès à Internet.

¹¹⁵ Cf. *supra*. (A), Paragraphe 1^{er}.

¹¹⁶ Article 6-4, *Op. cit.* note 114.

¹¹⁷ En droit sénégalais (voir l'article 6 COCC) comme en droit français (voir les articles 1142 à 1145 du Code civil).

¹¹⁸ Article 6 COCC.

¹¹⁹ Art. 1145 du Code civil : « si l'obligation est de ne pas faire, celui qui y contrevient doit des dommages et intérêts par le seul fait de la contravention. »

¹²⁰ Loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité, JORS n° 6406, du 3 mai 2008, p. 419.

En France, est également punie¹²¹ d'un an d'emprisonnement et de 75 000 euros d'amende la personne physique, ou le dirigeant de droit ou de fait d'une personne morale, qui ne satisfait pas aux obligations strictement liées à l'exercice des activités relatives à la fourniture d'accès à Internet. Certaines personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2¹²² du Code pénal. Elles encourent ainsi une peine d'amende, suivant les modalités prévues par le Code pénal, notamment en ses articles 131-38 et 131-39¹²³. Sous l'empire de ces dispositions, une sanction administrative, telle que l'interdiction d'exercer son activité professionnelle pour une durée de cinq ans au plus, peut même être prononcée contre un fournisseur d'accès à Internet.

Le respect du principe de neutralité ainsi que le fait de se consacrer exclusivement aux activités liées à sa fonction ne suffisent pas comme causes d'irresponsabilité du fournisseur d'accès à Internet. L'exécution d'une décision judiciaire ou administrative peut aussi en être la cause.

Paragraphe 2 : L'exécution d'une décision de l'autorité judiciaire ou administrative

La responsabilité civile ou pénale du fournisseur d'accès à Internet peut être neutralisée par le fait, pour lui, d'exécuter une décision de l'autorité judiciaire (A) ou de celle de l'autorité administrative (B).

A : L'exécution d'une décision de l'autorité judiciaire

Il s'agit, pour le fournisseur d'accès à Internet, de se plier à la décision de l'autorité judiciaire en posant des actes qu'il lui serait illégal d'exécuter sans l'injonction de ladite autorité, ou qu'il aurait dû légalement poser avant ladite injonction s'il avait fait preuve de vigilance et de diligence.

Au Sénégal, par exemple, même en se consacrant exclusivement aux activités liées à sa profession, le fournisseur d'accès à Internet n'a pas la latitude de poser certains actes de communication par voie électronique. En effet, sous peine d'engager sa responsabilité, il ne saurait ignorer ni le respect de la dignité de la personne humaine, de la liberté d'expression et d'opinion, de la propriété d'autrui, ni la sauvegarde de l'ordre public, les besoins de la défense nationale, les exigences de service public et les contraintes techniques inhérentes au moyen de communication¹²⁴.

¹²¹ Article 6 - VI. – 1 al. 1 de la LCEN : « est puni d'un an d'emprisonnement et de 75 000Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies au quatrième alinéa du 7 du I, de ne pas avoir conservé les éléments d'information visés au II ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments. »

¹²² Article 6 - VI. – 1 al. 2 : « les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du Code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce code. L'interdiction mentionnée au 2°de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise. »

¹²³ Ibidem.

¹²⁴ Article 1^{er} de la loi sur les transactions électroniques.

Toutefois, une autorité judiciaire qui vise à faire retirer des données informatiques ou à en interdire l'accès¹²⁵, peut requérir auprès de lui¹²⁶ la communication¹²⁷ d'informations en rapport avec celles-ci. Elle peut également lui demander de procéder, à partir de ses installations, à une activité de surveillance ciblée et temporaire¹²⁸, sans qu'il engage sa responsabilité ; ceci, en dépit de l'exonération légale de l'obligation, faite à ce dernier, quant à la surveillance générale¹²⁹ du caractère illicite des contenus qu'il transporte. Cette même mesure est prévue par le législateur français dans la LCEN¹³⁰.

D'ailleurs, le législateur sénégalais a prévu de tenir pour pénalement responsable un fournisseur d'accès à Internet qui n'aurait pas répondu favorablement à l'injonction d'une autorité judiciaire d'obtenir communication d'éléments qu'elle aurait requis auprès de lui en vue de la bonne marche des investigations judiciaires¹³¹. Ainsi, est-t-il prévu qu'il soit puni, s'il est reconnu coupable d'une telle infraction, d'« *un emprisonnement de six mois à un an et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement* »¹³².

Le législateur français a aussi prévu les mêmes sanctions pénales, à savoir l'emprisonnement et l'amende, à l'encontre d'un fournisseur d'accès à Internet, personne physique, qui aurait refusé de déférer à la demande d'une autorité judiciaire d'obtenir communication¹³³ d'éléments d'informations pouvant faire avancer des investigations judiciaires. Les personnes morales, elles, encourent des sanctions¹³⁴ plutôt administratives ou civiles.

Et puis, si les nécessités de l'information l'exigent, le juge d'instruction¹³⁵ sénégalais peut faire abstraction de l'obligation de neutralité ou encore du secret professionnel du fournisseur d'accès à Internet

¹²⁵ Article 6 – 5 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

¹²⁶ Et même auprès de l'hébergeur, car le législateur parle de prestataires mentionnés aux 1 et 2 de l'article 3 de la loi sur les transactions électroniques.

¹²⁷ Article 4 al. 3 de la loi sur les transactions électroniques.

¹²⁸ Article 3 – 5 de la loi sur les transactions électroniques.

¹²⁹ *Ibidem*.

¹³⁰ Article 6-7 al. 2 de la LCEN.

¹³¹ Articles 677-35 et 677-39 de la loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité

¹³² Article 431-44 de la loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité : « *Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux points 1 et 2 de l'article 3 de la loi sur les transactions électroniques, qui n'aura pas satisfait aux obligations définies au quatrième alinéa du point 5 de l'article 3 de la loi sur les transactions électroniques, n'aura pas conservé les éléments d'information visés à l'article 4 alinéa 1 de la loi susvisée ou n'aura pas déféré à la demande d'une autorité judiciaire d'obtenir communication desdits éléments sera puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement.* »

¹³³ Article 6 – VI – 1 de la LCEN : « *est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies au quatrième alinéa du 7 du I, de ne pas avoir conservé les éléments d'information visés au II ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments. Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du Code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même Code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce Code. L'interdiction mentionnée au 2° de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.*»

¹³⁴ *Ibidem*.

¹³⁵ Article 677-38 de la loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité.

et l'enjoindre, dans le cadre de ses capacités et surtout des moyens techniques existants, d'intercepter en vue d'une saisie informatique, de collecter et d'enregistrer des données informatiques voire de prêter son concours et son assistance aux autorités compétentes pour collecter ou enregistrer lesdites données.

A côté de l'exécution d'une décision de l'autorité judiciaire, qui constitue une cause d'irresponsabilité du fournisseur d'accès à Internet, il convient de retenir celle d'une décision de l'autorité administrative.

B : L'exécution d'une décision de l'autorité administrative

L'exécution, par le fournisseur d'accès à Internet, d'une décision de l'autorité administrative consiste à poser des actes visant principalement à retirer ou faire retirer un contenu litigieux, ou encore à le rendre inaccessible. Ce postulat rend compte de la possibilité, prévue tant en France qu'au Sénégal, pour l'autorité administrative, d'intervenir dans des affaires relevant du numérique en général, des transactions électroniques en particulier, non sans produire des effets.

C'est ainsi que la directive sur le commerce électronique¹³⁶, qui a été transposée dans le droit national français, a précisé qu'une autorité administrative pouvait, conformément aux systèmes juridiques des Etats membres, exiger¹³⁷ d'un prestataire technique qu'il mît un terme à une violation ou qu'il la prévînt. Mieux, cette directive a prévu que les limitations de responsabilité des prestataires de services intermédiaires, parmi lesquels les fournisseurs d'accès à Internet, étaient sans préjudice de la possibilité d'actions en cessation de différents types. Elle a surtout précisé que ces actions pouvaient revêtir la forme de décisions, entre autres, d'autorités administratives exigeant, en plus de la cessation et de la prévision de toute violation, le retrait pur et simple des informations illicites ou rendant l'accès à ces dernières impossible¹³⁸.

Une injonction de l'autorité administrative pourrait ainsi obliger le fournisseur d'accès à Internet à sortir de sa neutralité pour faire en sorte, par exemple, de bloquer l'accès à un site ou à une information litigieuse. Ce qui revient à retenir que ces prestataires techniques pourraient être contraints d'opérer ponctuellement des mesures de filtrage.

Un arrêt rendu le 21 janvier 2014 par la chambre commerciale de la cour de cassation française a combiné l'injonction d'une autorité administrative et celle d'une autorité judiciaire pour contraindre le fournisseur d'accès à Internet, *Darty télécom*, de bloquer des sites costaricains de jeux en ligne illégaux en France. Dans cette espèce, le juge a retenu le fait qu'en cas d'inexécution, par un opérateur, de l'injonction de cesser son activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée, le président

¹³⁶ *Dir. Cons.* CE n° 2000/31, 8 juin 2000, JOCE 17 juillet 2000, n° L 178, pp. 1-16.

¹³⁷ Article 12 – 3 de la directive sur le commerce électronique.

¹³⁸ *Op. cit.* note 136, Considérant 45.

de l'Autorité de Régulation des Jeux en Ligne (ARJEL) pouvait saisir le président du Tribunal de Grande Instance (TGI) de Paris aux fins d'ordonner à son fournisseur d'accès, « visé au 1 du 1 de l'article 6 de la loi n° 2004-575 du 21 juin 2004¹³⁹, l'arrêt de l'accès à ce service »¹⁴⁰.

Selon le juge, il est précisé à l'article 1^{er} du décret n° 2011-2122 du 30 décembre 2011¹⁴¹ que, lorsque l'arrêt de l'accès à une telle offre a été ordonné dans les conditions définies à « l'article 61 de la loi du 12 mai 2010 »¹⁴², les fournisseurs d'accès « procèdent à cet arrêt en utilisant le protocole de blocage par nom de domaine¹⁴³ »¹⁴⁴. Néanmoins, on se demande si leur responsabilité aurait pu être engagée en cas d'inertie de leur part alors même qu'ils avaient eu effectivement connaissance des contenus illicites, sans avoir été saisis par une autorité administrative¹⁴⁵. Deux positions se dégagent. La première est celle des auteurs qui s'y opposent¹⁴⁶ alors que la seconde retient que l'ampleur de l'exonération de responsabilité est si floue¹⁴⁷ qu'elle ne permet pas d'être catégorique. Ce qui est en revanche certain, c'est que les fournisseurs d'accès à Internet ne pourront pas bénéficier d'exonération s'ils ont délibérément participé¹⁴⁸ à la commission d'une faute sur le Web.

Comme en France, au Sénégal, le pouvoir de l'autorité administrative, consistant à décider de faire retirer une information litigieuse ou interdire d'accès sur les réseaux, est prévu par des dispositions légales et réglementaires¹⁴⁹.

Dès lors, tant que les fournisseurs d'accès à Internet s'en seront tenus à leur neutralité, tout en n'exécutant que les activités liées exclusivement à leur profession, dans le respect des décisions des autorités judiciaires ou administratives, le bénéfice de l'exonération de leur responsabilité devra être intact. Seulement, il n'est pas exclu que ces prestataires techniques posent ou s'abstiennent de poser des actes, engageant *ipso facto* leur responsabilité du fait personnel.

¹³⁹ Il s'agit de la LCEN.

¹⁴⁰ Cass. Com. 21 janvier 2014, *Darty Télécom c/ Arjel*, www.legalis.net, site visité le 2 Août 2016

¹⁴¹ Il s'agit du décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée. JORF n°0001 du 1 janvier 2012, texte n° 25, page 41 ; voir aussi sur le site www.legifrance.gouv.fr, site visité le 1^{er} août 2016.

¹⁴² Il s'agit de la 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, JORF n° 0110 du 13 mai 2010, voir aussi sur www.legifrance.gouv.fr, site visité le 25 août 2016.

¹⁴³ Pour la définition du nom de domaine, voir Abdoul Aziz DIOUF in « *Essai sur le régime juridique des noms de domaine* », Thèse, Université d'Orléans, 2010, p. 9 : « du nom patronymique désignant les personnes physiques au nom commercial comme identifiant des entreprises, dans la Toile ou sur Internet, les acteurs parcourant l'univers numérique se distingueront à travers l'outil suivant : le nom de domaine, le nom donné à la plateforme informatique hébergeant son utilisateur. Porte d'accès au cyberspace, le nom de domaine est composé d'un préfixe technique (www), d'un radical (dénomination) et d'un suffixe ou extension (.fr, .com). Au sens strict, le nom de domaine est le radical qui sera choisi par le déposant. »

¹⁴⁴ *Op. cit.* note 140.

¹⁴⁵ Voir judiciaire, tel que prévu par la directive sur le commerce électronique en son Considérant 45 et son article 12-3.

¹⁴⁶ M. Etienne, « *La responsabilité des prestataires intermédiaires de l'Internet* », Ubiquité, juin 2000, n° 5, p. 106, cité par Lionel THOUMYRE in « *La responsabilité pénale et extracontractuelle des acteurs de l'Internet* », Lamy Droit des Médias et de la Communication, Etude 464, 2009, p.37

¹⁴⁷ TH. Verbiest et W. Etienne, « *Le droit de l'Internet et de la société de l'information* », Larcier, 2001, p. 220, *ibidem*

¹⁴⁸ *Op. cit.* note 136. Considérant 44.

¹⁴⁹ Article 6 – 5 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

Section 2 : L'engagement de la responsabilité du fait personnel

La responsabilité du fait personnel trouve son siège, au Sénégal, à l'article 118 du COCC qui dispose qu'« *est responsable celui qui par sa faute cause un dommage à autrui* ».

En France, cette responsabilité se décline, aux termes des articles 1382 et 1383 du Code civil, ainsi qu'il suit : « *tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer. Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».

Toute faute est donc de nature à engager la responsabilité de son auteur, aucun degré de gravité n'est exigé et il n'est pas nécessaire que celui-ci soit animé d'une intention de nuire puisque la faute de négligence et celle d'imprudence sont également sanctionnées.

Transposée par analogie sur Internet et appliquée aux activités des fournisseurs d'accès, cette responsabilité sera alors fondée sur la faute de ceux-ci. Concrètement, ici, le fournisseur d'accès à Internet cause un dommage à autrui en jouant un rôle actif dans le transport du contenu préjudiciable. Le fait générateur de la responsabilité est la faute qui peut résulter de la création, la sollicitation, la sélection, la modification ou de la transmission illégale des contenus. La responsabilité de ce prestataire technique est de nature extracontractuelle car elle trouve son fondement dans un fait, celui d'agir sur le contenu litigieux en amont, au cours du transport ou en aval.

C'est dire que le fournisseur d'accès à Internet engage sa responsabilité d'une part, en étant à l'origine de la transmission du contenu ou en sélectionnant son destinataire (Paragraphe 1^{er}), d'autre part, en procédant à la sélection ou à la modification dudit contenu (Paragraphe 2).

Paragraphe 1^{er} : Le fournisseur d'accès à Internet à l'origine de la transmission du contenu et la sélection du destinataire

Pour garder intact l'exonération de responsabilité dont il bénéficie, le fournisseur d'accès à Internet ne doit ni être à l'origine de la transmission du contenu (A) ni en sélectionner le destinataire. (B).

A : Le fournisseur d'accès à Internet à l'origine de la transmission du contenu

Le fournisseur d'accès à Internet a l'obligation de ne pas créer les contenus qu'il transmet ni d'en solliciter la transmission encore moins d'être la personne qui prend la décision d'effectuer cette transmission.

Cela suppose qu'en assurant le rôle de « *simple transport* (« *Mère conduit* »)¹⁵⁰ qui est le sien, ce prestataire technique, qu'il soit une personne physique ou un dirigeant de droit ou de fait d'une personne morale, ou une personne morale tout court, ne doit nullement être à l'origine de la création du contenu litigieux. Il ne doit pas non plus en solliciter la transmission auprès d'un tiers.

Au Sénégal, l'article 6-2 du décret n° 2008-719 du 30 juin 2008 prévoit qu'en jouant son rôle d'intermédiation, ce prestataire technique doit se garder d'être à « *l'origine de la transmission* »¹⁵¹ des contenus.

En France, le législateur prévoit que pour voir sa responsabilité civile ou pénale engagée à raison de ces contenus, le fournisseur d'accès à Internet devra, entre autres, être « *à l'origine de la demande de transmission litigieuse* »¹⁵². Cette condition semble écarter, en droit français de l'économie numérique¹⁵³, la prohibition de la création du contenu par le fournisseur d'accès à Internet. Mais la considération des principes de neutralité et d'exclusivité analysés plus haut dans cette réflexion, et auxquels ce dernier est assujéti, neutralise déjà cette lecture.

En tous les cas, les législateurs européen¹⁵⁴ et sénégalais¹⁵⁵ considèrent que le simple fait, pour le fournisseur d'accès à Internet, d'être à l'origine de la transmission, engage sa responsabilité. Cela semble logique car la création et la demande de transmission d'un contenu transcendent les principes de neutralité et d'exclusivité imposés au fournisseur d'accès à Internet. Elles procèdent de l'activité éditoriale¹⁵⁶, qui englobe selon la doctrine celles de production et de diffusion¹⁵⁷. Mieux, la jurisprudence considère qu'est éditeur, la personne qui détermine ou est à l'origine des contenus diffusés. En France, le juge a retenu cela dans plusieurs affaires¹⁵⁸.

Le 15 avril 2008, lorsqu'il s'est agi d'apprécier la qualité d'éditeur d'un prestataire technique, en rapport avec des actes posés par la société *Dailymotion*, assignée par deux comédiens, Omar et Fred, pour

¹⁵⁰ Article 12 de la directive sur le commerce électronique.

¹⁵¹ Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques. J.O.R.S. N° 6439 du Samedi 22 novembre 2008

¹⁵² Article 9 de la LCEN.

¹⁵³ En référence à la loi n° 2004 -575 du 21 juin 2004 pour la confiance dans l'économie numérique.

¹⁵⁴ Article 12 de la directive sur le commerce électronique.

¹⁵⁵ Article 6-2 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

¹⁵⁶ L'activité éditoriale n'est définie ni en droit sénégalais ni en droit français. Dans les décisions françaises, par exemple, les juges font référence généralement à la loi pour la confiance dans l'économie numérique qui prévoit la « *personne qui édite* ». Cette loi ne définit pas la notion d'éditeur, tout comme celle sénégalaise sur les transactions électroniques.

¹⁵⁷ B. Van Besien, « *La responsabilité des gestionnaires de forums de discussion 'non commerciaux'* », A. & M., 2010, n° 2010/5, p. 566, cité par Julie ANGENOT in « *L'exonération de responsabilité au profit des hébergeurs s'étend-elle aux gestionnaires de sites participatifs et aux exploitants de forums de discussion ?* » UCL, Louvain, 2015, p. 33 : « *l'activité éditoriale est une intervention dont le caractère va au-delà d'une manipulation purement technique de l'information, notamment en ce qu'elle comporte un jugement sur la valeur ou l'intérêt du contenu et la volonté de la diffuser auprès du public* »

¹⁵⁸ T.G.I. Paris, 19 octobre 2007, *Zadig Production c/ Google vidéo*, confirmé par C.A. Paris (2^{ème} ch.), 03 décembre 2010 ; Cass. Com. 27 avril 2009, *Davis films c/ Dailymotion* ; T.G.I. Paris (réf.), 15 décembre 2008, *Claire L. c/ Mehdi K.* ; T.G.I. Paris, 14 novembre 2008, *Jean-Yves Lafesse et autres c/ Youtube et autres*, www.legalis.net, site visité le 02 mai 2016.

la diffusion et l'offre de téléchargement, sans autorisation, de quelques uns de leurs sketches, le TGI de Paris a estimé que « *l'éditeur est la personne qui détermine les contenus qui doivent être mis à la disposition du public sur le service qu'elle a créé ou dont elle a la charge.* »¹⁵⁹

Ainsi, sans préjudice des dommages et intérêts résultant de l'engagement de sa responsabilité civile, le fournisseur d'accès à Internet, pourrait-il être pénalement poursuivi, par exemple au Sénégal, pour cause d'atteintes se rapportant aux contenus illicites, réprimées par les articles 431-38 à 431-42 de la loi sur la cybercriminalité. Par exemple, l'article 431-38 de cette loi réprime, entre autres, la création et la diffusion 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* ».

Quant aux personnes morales, autres que l'Etat, les collectivités locales et les établissements publics, si elles sont reconnues pénalement responsables des mêmes fautes, commises pour leur compte par leurs organes ou représentants, et, prévient la jurisprudence, que¹⁶⁰ par eux seulement, alors les sanctions à leur encontre sont prévues notamment par l'article 431-62 de la loi sur la cybercriminalité¹⁶¹.

Certes, parmi les conditions d'effectivité de la dérogation de responsabilité, accordée au fournisseur d'accès à Internet, figure le fait qu'il ne soit pas à l'origine de la transmission du contenu ; mais encore faudrait-il qu'il ne sélectionnât pas le destinataire dudit contenu.

B : La sélection du destinataire du contenu

La sélection du destinataire de la transmission, par le fournisseur d'accès à Internet, suppose que ce prestataire technique agisse directement ou indirectement sur la trajectoire des contenus, pendant l'opération de transport dont il a le monopole, afin de les faire parvenir aux personnes physiques ou morales de son choix.

Ce faisant, le fournisseur d'accès à Internet procède, sans l'autorisation des expéditeurs ou des fournisseurs de contenus, ni de celle de la loi, à un tri des destinataires des documents numériques transportés. Par exemple, pour l'action directe, avant d'effectuer la transmission desdits documents à leurs destinataires initiaux, il trie en cochant ou en décochant ceux de son choix ou il en rajoute d'autres sur les listes préétablies par des expéditeurs. Quant à l'action indirecte, le fournisseur d'accès à Internet a la

¹⁵⁹ T.G.I. Paris (3^{ème} ch.), 15 avril 2008, *Omar et Fred et autres c/ Dailymotion*, confirmé par C.A Paris, 14 février 2010, *Omar et Fred et autres c/ Dailymotion*, www.legalis.net, site visité le 02 mai 2016.

¹⁶⁰ Encore que la faute ne doit être commise « *que* » par les organes ou représentants de la personne morale : Cass. Crim., 20 juin 2006, *Bull. Crim.* n° 188 ; *Dr. Pén.* 2006, comm. n° 128 ; *Cass. Crim.* 15 janv. 2008 : *Dr. Pén.* 2008, comm. n° 71 ; JCP 2008, II, 10082, note J.-Y. MARECHAL, cité par Clément MARGAINE in « *La capacité pénale* », Thèse, Université Montesquieu, Bordeaux IV, E.D. 41, 2011, p. 125.

¹⁶¹ Article 431-62 de la loi sur la cybercriminalité : « *les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits...* »

possibilité de programmer ses systèmes de veille, d'exploration, de ciblage et de tri, communément appelés "générateurs de mots-clés" ou encore "robots", de telle manière que la sélection des destinataires, à qui il affecte des métadonnées, se fait automatiquement et sans interruption. D'ailleurs, en se comportant ainsi, il jouerait plus le rôle de fournisseur de moteurs de recherches que celui d'accès à Internet au sens de l'article 3-1 de la loi sur les transactions électroniques et de l'article 6-I-1 de la LCEN.

Cette intervention est techniquement différente du fonctionnement, par exemple de *Google Suggest*¹⁶² tel que retenu par un arrêt de la cour de cassation française datant du 12 juillet 2012¹⁶³. Car ce moteur de recherches fonctionne, sans intervention humaine et, du seul résultat d'algorithmes¹⁶⁴ appliqués à une base de données recensant les requêtes les plus fréquentes.

Cela étant, c'est la LCEN¹⁶⁵, la directive sur le commerce électronique¹⁶⁶ et la loi sur les transactions électroniques avec son décret d'application n° 2008-719 du 30 juin 2008¹⁶⁷ qui énoncent l'irresponsabilité pénale et civile des fournisseurs d'accès à Internet à condition qu'ils ne sélectionnent pas le destinataire de la transmission. La jurisprudence française abonde dans le même sens, car dans un arrêt du 18 février 2010, la cour de cassation a estimé que la société « *Active communication Ltd (Act Com)* », condamnée au fond à verser à la ville de Marseille une provision, avait engagé sa responsabilité en sa qualité de fournisseur d'accès à Internet, pour avoir opéré une sélection du destinataire de la transmission¹⁶⁸.

Cependant, cette exigence faite au fournisseur d'accès ne couvre pas la sélection des destinataires effectuée par d'un fournisseur de contenus, pour qu'un courrier électronique soit envoyé à tous les membres d'un groupe¹⁶⁹.

Si, engage sa responsabilité civile ou pénale le fournisseur d'accès à Internet qui est à l'origine de la transmission du contenu ou en sélectionne le destinataire, son irresponsabilité n'est pas non plus assurée s'il sélectionne ledit contenu ou le modifie.

¹⁶² « *Google Suggest* » est un moteur de recherches qui permet de trouver des informations plus rapidement en consultant les prédictions de recherche. Il s'agit de termes de recherche possibles suggérés à l'internaute. Ceux-ci correspondent aux mots ou expressions que celui-ci saisit et aux recherches d'autres utilisateurs. Les prédictions de recherche sont générées automatiquement par le biais d'un algorithme, sans aucune intervention humaine. Cet algorithme est basé sur un certain nombre de facteurs objectifs, tels que la fréquence de recherche d'un terme par les autres internautes. Sources : www.support.google.com et www.webrankinfo.com, sites visités le 04 mars 2016.

¹⁶³ Cass. Civ. 1ère, 12 juill. 2012, Gaz. Pal. 25-26 juill. 2012, n° 208, p. 9, in Communication de Caroline LE GOFFIC, Revue Lamy droit de l'immatériel (RLDI) 2012/85, n° 2851, obs. L. Costes.

¹⁶⁴ *Algorithme* : Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. Source : www.larousse.fr, site visité le 4 mai 2016.

¹⁶⁵ Article 9 – 1 de la LCEN.

¹⁶⁶ Article 12-1-b 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.

¹⁶⁷ Article 6-1 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

¹⁶⁸ Cass. Civ. (2^{ème} Ch.), 18 février 2010, *Active communication Ltd (Act Com) c/ Ville de Marseille*. www.legalis.net, site visité le 4 mai 2016

¹⁶⁹ TH. Verbiest, TH. Lionel in « *Responsabilités sur Internet : Le mannequin et l'hébergeur, Cour d'appel de Paris, Arrêt rendu en 10 février 1999, Estelle H. c/ Valentin L.* » Source : www.juriscom.net ou sur <http://lthoumyre.chez.com/pro/1/resp19990225.htm>, site visité le 1^{er} février 2016.

Paragraphe 2 : La sélection et la modification du contenu

La sélection (A) et la modification (B) du contenu transmis constituent, pour le fournisseur d'accès à Internet, des actes qui limitent son irresponsabilité légale.

A : La sélection du contenu

La sélection du contenu par le fournisseur d'accès à Internet suppose qu'il choisisse, ou fasse choisir, ceux qui l'agrément parmi un certain nombre de documents numériques, possiblement dans le but de les modifier, de les retarder, d'en rendre impossible ou difficile l'accès, de les détourner, de les voler ou de les supprimer.

L'engagement de la responsabilité du fournisseur d'accès, du fait de la sélection en tant que telle du contenu qu'il transmet, n'est pas prévu par le législateur sénégalais. Cependant, son homologue français en a fait une cause de restriction de l'irresponsabilité de ce prestataire technique. En effet, aux termes de l'article 9-1 de la LCEN qui rétablit l'article L. 32-3-3 du Code des postes et télécommunications, le fournisseur d'accès ne peut voir sa responsabilité civile ou pénale engagée, à raison des contenus qu'il transmet, que s'il sélectionne les contenus faisant l'objet de la transmission¹⁷⁰.

À ce niveau, c'est la neutralité pleine et entière du fournisseur d'accès, à l'égard des contenus, que prévoit le législateur. Au sens où, même s'il n'en est formellement pas question à ce stade de cette réflexion, il semble clair que la disposition ci-devant convoquée pose la sélection des contenus par le fournisseur d'accès à Internet comme étant une condition suffisante pour faire sauter le verrou de son irresponsabilité, à la différence de la Directive européenne qui prévoit que la sélection ne suffit pas, il faut qu'elle soit suivie de la modification¹⁷¹ afin de neutraliser l'irresponsabilité du fournisseur d'accès à Internet.

En droit sénégalais, si les nécessités de l'information l'exigent, le juge d'instruction peut obliger le fournisseur d'accès, selon ses capacités techniques, à collecter ou à enregistrer en temps réel des données spécifiques relatives aux contenus transmis¹⁷². Le législateur n'a pas fait expressément cas de la sélection des contenus à transmettre, mais force est de comprendre que les opérations ordonnées ne sauraient techniquement se réaliser qu'en procédant à la sélection manuelle ou automatique programmée desdits contenus.

¹⁷⁰ Article L. 32-3-3 : « 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 à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission. »

¹⁷¹ Article 12 – 1 – c) de la Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000, « ... à condition que le prestataire...ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission. »

¹⁷² Article 677-38 de la loi n° 2008 -11 du 25 janvier 2008 portant sur la Cybercriminalité

N'empêche, en droit sénégalais comme en droit français, la modification des contenus à transmettre est prévue et sanctionnée par la loi.

B : La modification du contenu

La modification du contenu, transporté ou stocké automatiquement ou temporairement par le fournisseur d'accès à Internet, consiste à en rajouter ou en soustraire des données de telle sorte que l'original ne comporte plus toutes ses caractéristiques indispensables. Le fournisseur d'accès pourrait de ce fait transformer un contenu licite en un nouveau plutôt litigieux ou, pis encore, illicite.

Au Sénégal, en posant un tel acte, le fournisseur d'accès engage sa responsabilité sur le fondement de l'article 6-4 du décret relatif aux communications électroniques¹⁷³ qui énonce l'exonération de la responsabilité des prestataires techniques à partir du moment où ils se « *contentent de faire du stockage automatique ou temporaire de l'information ou de jouer un rôle d'intermédiation dans la transmission de celle-ci* » tout en se gardant de « *modifier les informations faisant l'objet de la transmission* ». Ce faisant, il pourrait être poursuivi pour atteinte aux données informatisées, prévue et réprimée par les articles 431-12 et suivants de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité. A ce titre, le législateur a prévu à l'article 431-12, une peine d'emprisonnement « *d'un an à cinq ans et une amende de 5.000.000 à 10.000.000 francs ou l'une de ces deux peines seulement* ». La même peine est prévue à l'encontre de quiconque aura modifié ou tenté de modifier, frauduleusement, des données informatisées¹⁷⁴.

La répression de ces infractions garantit l'intégrité et le secret des contenus lors de leur transmission, conformément au principe constitutionnel de l'inviolabilité du secret des correspondances électroniques¹⁷⁵. Elle assure leur authenticité. L'article 431-14¹⁷⁶ sanctionne en ce sens la falsification et la contrefaçon informatiques débouchant sur de faux contenus. Dans une affaire¹⁷⁷ rendue le 5 septembre 2008, dite « *affaire de la Direction du Traitement Automatique de l'Information (DTAI)* », la 1^{ère} chambre correctionnelle du tribunal régional de Dakar a admis la possibilité d'un faux portant sur des données informatiques.

¹⁷³ Décret n° 2008 - 719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008 - 08 du 25 janvier 2008 sur les transactions électroniques.

¹⁷⁴ Article 431-13 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

¹⁷⁵ Article 13 de la Constitution du Sénégal du 22 janvier 2001 : « *le secret de la correspondance, des communications postales, télégraphiques, téléphoniques et électroniques est inviolable. Il ne peut être ordonné de restriction à cette inviolabilité qu'en application de la loi* », voir aussi <http://www.gouv.sn/-Constitution-du-Senegal-.html>, site visité le 9 septembre 2016.

¹⁷⁶ Article 431-14 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité : « *quiconque aura produit ou fabriqué un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.* »

¹⁷⁷ V. TRHC de Dakar, n° 499/ 2008 du 5 septembre 2008, *affaire de la Direction du Traitement Automatique de l'Information (DTAI)*, jugement inédit ; in « *La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité* », p. 5, in « *Conférence sur la coopération contre la cybercriminalité, Strasbourg, France, 23-25 mars 2010.* » par Papa Assane TOURE.

En France, cette restriction est prévue à l'article 9 de la LCEN aux termes duquel le législateur a retenu que le fournisseur d'accès ne saurait jouir du bénéfice de l'irresponsabilité que s'il s'évertuait à ne pas modifier les contenus faisant l'objet de la transmission. La directive européenne sur le commerce électronique a, elle aussi, institué cette restriction de l'exonération de responsabilité accordée au fournisseur d'accès, notamment en ses articles 12 et 13 où elle s'applique dès que ce prestataire « *modifie les informations faisant l'objet de transmission* », y compris pendant le « *stockage automatique, intermédiaire, temporaire et transitoire* »¹⁷⁸ des informations transmises.

Somme toute, en consacrant l'irresponsabilité principielle du fournisseur d'accès à Internet à l'égard des contenus qu'il transmet, mais qu'il soumet à des conditions, le législateur sénégalais, pas plus que son homologue français, a prévu en même temps des obligations devant être remplies par ce prestataire technique. Il s'agit des obligations d'information, de moyens, de surveillance, de contrôle et de résultat.

¹⁷⁸ Il s'agit de la « *forme de stockage dite "caching"* » selon l'article 13 de la directive sur le commerce électronique.

CHAPITRE 2 : Les obligations d'information, de moyens, de surveillance, de contrôle et de résultat

La mise à disposition, à temps, d'informations exactes et de moyens notamment techniques, et le fait non seulement de leur assurer le minimum de surveillance tout en contrôlant aussi régulièrement que possible les contenus transportés, mais aussi de s'inscrire de manière efficiente dans la dynamique d'atteinte des résultats escomptés en matière de lutte contre les fautes commises dans le cyberspace, sont autant d'obligations que doit remplir le fournisseur d'accès à Internet dans l'exercice de ses activités.

C'est pourquoi il semble important d'étudier ces obligations, pour une meilleure progression de cette réflexion. Ainsi, serait-ce nécessaire de voir d'une part celles d'information et de moyens (Section 1^{ère}), d'autre part l'obligation minimale de surveillance et celles de contrôle et de résultat (Section 2).

Section 1^{ère} : Les obligations d'information et de moyens

En droit sénégalais des transactions électroniques, ainsi qu'en droit français de l'économie numérique, la mise à disposition des informations disponibles, à qui de droit, par le fournisseur d'accès à Internet est érigée en obligation, tout comme celle concernant les moyens notamment techniques. En clair, parmi les obligations qui incombent au fournisseur d'accès à Internet, en tant que personne physique ou morale dont l'activité à titre professionnel ou gratuit est d'offrir un accès à des services au public par le biais des technologies de l'information et de la communication¹⁷⁹, l'on peut retenir, premièrement, l'obligation d'information (Paragraphe 1^{er}) et, deuxièmement, l'obligation de moyens (Paragraphe 2).

Paragraphe 1^{er} : L'obligation d'information

L'obligation d'information qui pèse sur le fournisseur d'accès à Internet devrait légalement profiter d'une part à ses abonnés et aux tiers (A), de l'autre, à l'autorité compétente (B)

A : L'information à l'attention des abonnés et des tiers

L'obligation d'information à l'attention des abonnés et des tiers tient au fait, pour le fournisseur d'accès à Internet, de leur donner des informations indispensables, pour les premiers, dans le cadre du contrat qui les lie et, pour tous les deux, en rapport avec la lutte contre les agissements¹⁸⁰ illicites sur Internet.

Cette obligation est instituée par le législateur sénégalais à travers l'article 3-1 de la loi sur les transactions électroniques où il a prévu que les fournisseurs d'accès à Internet étaient tenus de donner un

¹⁷⁹ Article 3 – 1 et 2 de la loi sur les transactions électroniques.

¹⁸⁰ Article 3 – 5 al. 3 *Idem*.

certain nombre d'informations à leurs abonnés, en mentionnant dans leurs contrats l'existence de moyens techniques permettant une restriction de l'accès à certains services ou, au moins, de les sélectionner.

A l'égard des tiers, même si sa précision semble discutable, le législateur a estimé que le fournisseur d'accès devait « rendre public »¹⁸¹, autrement dit, informer en plus de ses abonnés, l'ensemble des internautes actuels comme futurs¹⁸², de ce qu'étaient ses moyens de lutte contre les activités illicites sur Internet. A ce titre, si les objectifs poursuivis par le législateur sont majoritairement¹⁸³ « la prévention et la dissuasion » de la commission d'actes illicites sur la Toile, il est évident que les cyber-malfaiteurs, qu'ils soient des abonnés ou des tiers, sauront parfaitement mettre cette publicité à profit, à mauvais escient, pour contourner la cybersécurité mise en place et perpétuer leurs méfaits.

Cela est d'autant plus probable que le législateur sénégalais, qui a toutefois érigé en obligations la conservation¹⁸⁴ et la communication¹⁸⁵ des données de connexion, semble tout de même les y encourager en obligeant les fournisseurs d'accès à tenir informés¹⁸⁶ les utilisateurs de toute mise à jour de leurs moyens de lutte contre la cybercriminalité, et que tout manquement à ces obligations, est « puni d'un emprisonnement de six mois à un an et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement »¹⁸⁷.

En France, les mêmes obligations sont à la charge des fournisseurs d'accès. En effet, en vertu des points I-1 et 7-4 *in fine* de l'article 6 de la LCEN, ceux-ci sont tenus non seulement de mettre à la disposition de leurs abonnés des informations relatives à l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, mais aussi de « rendre publics » les mêmes moyens à l'attention des tiers. Tout manquement à ces obligations est pénalement sanctionné.

En plus des informations que les fournisseurs d'accès à Internet ont l'obligation de donner à leurs abonnés et aux tiers, il y en a qu'ils sont tenus de mettre à la disposition des autorités compétentes.

¹⁸¹ Article 3 – 5 al. 4 *Idem*.

¹⁸² Parce que le droit sénégalais de la cybercriminalité considère comme moyens de diffusion publique, aux termes de l'article 431-58 de la loi sur la cybercriminalité : « la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique. »

¹⁸³ Cette conception utilitariste de la loi, théorisée notamment par des auteurs comme C. DEBUYST, F. DIGNEFFE, J.-M. LABADIE et A. P. PIRES, est ici relativisée par le dernier : « la rigueur actuelle de la loi n'exprime plus adéquatement nos valeurs et notre désapprobation, ne dissuade pas assez les gens et ne permet pas de « réadapter les délinquants violents » » in article intitulé « La rationalité pénale moderne, la société du risque et la juridicisation de l'opinion publique », publié dans la revue « sociologie et sociétés » vol. 33, n°1, Université d'Ottawa, Ontario, Canada, 2001, pp. 179-204, ou suivre ce lien <http://id.erudit.org/iderudit/001562ar>, site visité le 14 septembre 2016.

¹⁸⁴ Article 4 al. 1er de la loi sur les transactions électroniques ; et article 431 – 44 de la loi sur la cybercriminalité.

¹⁸⁵ Article 4 al. 3 *Idem* ; et article 431 – 44 *in fine*, *Idem*.

¹⁸⁶ Article 4 du décret n° 2008 - 719 du 30 juin 2008 relatif aux communications électroniques.

¹⁸⁷ Article 431 – 44 de la loi sur la cybercriminalité.

B : L'information à l'attention des autorités compétentes

Informers les autorités compétentes, à leur demande ou non, des agissements illicites des internautes se servant de leurs moyens d'accès à la Toile, que ces derniers soient leurs abonnés ou des tiers, ce sont les obligations mises à la charge des fournisseurs d'accès par le législateur sénégalais et son homologue français. Cependant, si l'une est une obligation d'information, l'autre semble davantage celle de collaboration que d'information.

Au Sénégal, le législateur a prévu que, « *compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie infantile* »¹⁸⁸, les fournisseurs d'accès dussent concourir à la lutte contre de tels agissements¹⁸⁹ et des activités qui y sont liées. A ce titre, ils ont l'obligation « *d'informer promptement les autorités publiques compétentes* »¹⁹⁰ de l'existence desdites activités, qui leur sont signalées et qu'exercent les destinataires de leurs services.

Sans doute faudrait-il entrevoir, à ce niveau, que le législateur privilégie deux exigences complémentaires. Il s'agit premièrement, avec l'utilisation de l'adverbe « *promptement* », de résoudre un souci de célérité dans le fait de mettre de telles informations à la disposition des autorités compétentes ayant à leur tour la charge de lancer la procédure judiciaire ou administrative adéquate, pour faire cesser les activités illicites et sanctionner les cyber-malfaiteurs. Secondement, le législateur, dans un souci d'efficacité adossée au respect des principes de sécurité juridique¹⁹¹, a concédé la latitude aux fournisseurs d'accès de s'y faire non seulement « *directement ou indirectement* »¹⁹², mais également « *dans les meilleurs délais* »¹⁹³ non sans devoir s'assurer préalablement du caractère « *manifestement illicite* »¹⁹⁴ du contenu en cause. Dans le même sillage, le législateur prévoit que les prestataires techniques et les utilisateurs¹⁹⁵ entendent par « *contenus manifestement illicites, des contenus d'une gravité avérée et dont le caractère illicite ne semble pas discutable, notamment les contenus à caractère pornographique ou faisant l'apologie des crimes de guerre ou portant manifestement atteinte à l'ordre public ou aux bonnes mœurs* »¹⁹⁶.

¹⁸⁸ Article 3 -5 al. 3 de la loi sur les transactions électroniques.

¹⁸⁹ *Ibidem*.

¹⁹⁰ Article 3 -5 al. 4, *op.cit.* note 188.

¹⁹¹ P. Cassia, « *La sécurité juridique, un "nouveau" principe général du droit aux multiples facettes* », Dalloz. 2006, p. 1190 : cet auteur estime qu'« *il conviendrait de parler des principes de sécurité juridique car cette notion recouvre une multitude de principes* », cité par Maiwenn TASCHER in « *Les revirements de jurisprudence de la Cour de Cassation* », Thèse, Université de Franche-Comté, Besançon, 2011, p. 182.

¹⁹² Article 9 du décret n° 2008 - 719 du 30 juin 2008 relatif aux communications électroniques.

¹⁹³ *Ibidem*.

¹⁹⁴ *Ibidem*.

¹⁹⁵ Articles 3, 4, 5 et 10, al. 2 du décret n° 2008 - 719 du 30 juin 2008, *Op. cit.* 192.

¹⁹⁶ Article 2 – 2 du décret n° 2008 - 719 du 30 juin 2008. Voir aussi Lionel THOUMYRE in « *Comment les hébergeurs français sont devenus juges du manifestement illicite* », Juriscom, 28 juillet 2004, cité par Ophélie FONDEVILLE et Anne-Sophie JOUANNON in « *Le "manifestement illicite", mystérieux point de rencontre entre la victime et l'hébergeur.* », Juriscom, 7 avril 2008, p. 3. Existe aussi sur www.juriscom.net ou <http://www.juriscom.net/wp-content/documents/resp20080407.pdf>, sites visités le 16 septembre 2016 : au fond,

Dès lors, on peut concevoir l'existence en filigrane d'une obligation de collaboration à la charge des fournisseurs d'accès ; car le législateur, qui les oblige à informer les autorités compétentes, les autorise alors à mettre à contribution les utilisateurs¹⁹⁷ ou à faire en sorte que, comme prévu à l'article 4 alinéa 3 de la loi sur les transactions électroniques, celles-ci puissent accéder facilement, directement et en permanence¹⁹⁸ à l'information signalétique en question. Si bien que la possibilité pour elles d'avoir un accès facile, direct et permanent¹⁹⁹ les affranchit des éventuelles velléités de camouflage ou de soustraction d'informations jugées compromettantes, de la part de certains fournisseurs d'accès. Par exemple, dans sa « délibération n° 2014-016 du 30 avril 2014 mettant en demeure Tigo Sénégal pour non déclaration de fichiers »²⁰⁰, la Commission de Protection des Données Personnelles (CDP), en tant qu'autorité publique compétente, a fait état du refus de ce fournisseur d'accès de déférer à sa demande de communication, « par une lettre datant du 8 avril 2014 », d'un certain nombre d'informations litigieuses signalées en ligne par ses abonnés.

Au plan judiciaire, les fournisseurs d'accès qui manquent à l'obligation d'information à l'attention des autorités publiques compétentes, prévues notamment à l'article 3 de la loi sur les transactions électroniques, encourent une peine d'emprisonnement allant de six mois à un an assortie d'une amende de 200.000 francs à 1.000.000 francs ou l'une de ces deux peines seulement²⁰¹.

En droit français du numérique, le siège de l'obligation d'information à la charge des fournisseurs d'accès et, au profit des autorités compétentes, est l'article 6-I-7 de la LCEN²⁰². En effet, le législateur y prévoit que compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie infantine, les fournisseurs d'accès doivent, en informant promptement les autorités compétentes de toutes activités illicites, concourir à la lutte contre la diffusion de ces infractions entre autres, et de celles visées à l'article 227-23 du Code pénal. Cet article punit sévèrement les infractions contre les mineurs²⁰³.

« l'interprétation de la notion de « manifestement illicite » pourrait se faire "in concreto", c'est-à-dire en fonction des connaissances juridiques que l'on peut raisonnablement attendre d'un hébergeur »

¹⁹⁷ Articles 3, 4, 5 et 10, al. 2 du décret n° 2008 - 719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008 - 08 du 25 janvier 2008 sur les transactions électroniques.

¹⁹⁸ Article 14 du décret n° 2008 - 719 du 30 juin 2008.

¹⁹⁹ *Ibidem*.

²⁰⁰ L'intitulé complet est : Délibération n° 2014-016 du 30 avril 2014 mettant en demeure Tigo Sénégal pour non déclaration de fichiers, bases de données et systèmes contenant des informations nominatives et pratiques de prospection directe non conforme à la législation. Source : www.cdp.sn, site visité le 13 juin 2016

²⁰¹ Article 461-45 *in fine* de la loi portant sur la cybercriminalité.

²⁰² Ainsi que, en ce qui concerne le droit communautaire européen, l'article 5 de la directive sur le commerce électronique.

²⁰³ Article 227-23 du Code pénal français : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation. Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines. Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques. Le

Et, sans préjudice de la punition prévue à cet article, le législateur français prévoit à l'article 6-VI-1 de la LCEN, qu'en cas de manquement à l'obligation d'informer les autorités compétentes, les fournisseurs d'accès, personnes physiques ou dirigeants de droit ou de fait de personnes morales, encourrent une peine d'un an d'emprisonnement assortie d'une amende de 75000 euros.

Le législateur français a actuellement renforcé le dispositif de répression du terrorisme, y compris son apologie sur Internet, en tant que délit indépendant du cyberterrorisme²⁰⁴. C'est ainsi que la loi n° 2014-1353 du 13 novembre 2014²⁰⁵, dite « loi Cazeneuve », a créé et inséré l'article 421-2-5 dans le Code pénal, réprimant les délits de « *provocation directe à la commission d'actes terroristes et d'apologie du terrorisme* » sur Internet, lesquels n'étaient que des délits de presse jusqu'en 2014. Ils sont punis de « *sept ans d'emprisonnement et 100 000 euros d'amende* »²⁰⁶. C'est dire qu'un fournisseur d'accès doit, pour ne pas être poursuivi sur le terrain de la complicité²⁰⁷, porter ces infractions en ligne à la connaissance de l'autorité compétente.

Dans une espèce²⁰⁸ en date du 7 septembre 2016, le fournisseur d'accès *Free* a porté à la connaissance des autorités judiciaires, à leur demande, des informations en relation avec des activités illicites en ligne sur la période allant du 30 septembre 2014 au 11 mai 2015 à Paris, permettant ainsi au TGI de Paris de condamner un prévenu au pénal et au civil.

En tous les cas, au Sénégal comme en France, à côté de l'obligation d'information pesant sur les fournisseurs d'accès, existe celle de moyens.

fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende. Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée. La tentative des délits prévus au présent article est punie des mêmes peines. Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

²⁰⁴ Selon le dictionnaire Larousse, le cyberterrorisme est l'« ensemble des attaques graves (virus, piratage, etc.) et à grande échelle des ordinateurs, des réseaux et des systèmes informatiques d'une entreprise, d'une institution ou d'un État, commises dans le but d'entraîner une désorganisation générale susceptible de créer la panique. »

²⁰⁵ Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. JORF n° 0263 du 14 novembre 2014, voir aussi sur www.legifrance.gouv.fr, site visité le 16 septembre 2016.

²⁰⁶ Article 5 – I, *ibidem*.

²⁰⁷ T. Papa Assane, « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, pp. 415-417.

²⁰⁸ TGI Paris, 17^e ch. correctionnelle, 7 septembre 2016, *Avocats sans frontières, Licra, SOS Racisme c/ M. X.*, www.legalis.net, site visité le 8 septembre 2016.

Paragraphe 2 : L'obligation de moyens

Est qualifiée d'obligation de moyens, l'obligation en vertu de laquelle un débiteur, qui ne promet *a priori* aucun résultat, doit déployer ses meilleurs efforts pour l'atteinte d'un objectif prédéfini. Il s'engage ainsi à garantir au créancier de l'obligation, tous les soins d'un bon père de famille nécessaires à l'exécution de celle-ci. Par suite, sa responsabilité est engagée par l'inexécution, un retard dans l'exécution²⁰⁹ ou l'exécution partielle voire défectueuse de son obligation²¹⁰.

Ramenée²¹¹ à l'échelle du droit sénégalais des transactions électroniques, cette obligation explicite²¹² se résume à la prescription de moyens par le législateur, à la charge des prestataires techniques, dans le but d'assurer une efficacité et une sécurité²¹³ desdites transactions. Ainsi, oblige-t-il les fournisseurs d'accès à les assurer aux éditeurs, aux autorités compétentes et aux tiers (A), sans oublier ceux destinés à la protection des mineurs (B).

A : Les moyens au profit des éditeurs, des autorités compétentes et des tiers

Au Sénégal comme en France, ce sont principalement les moyens techniques que les fournisseurs d'accès à Internet ont l'obligation de mettre à la disposition des utilisateurs.

Cette obligation découle, par exemple, des dispositions de l'article 3 de la loi sur les transactions électroniques qui fait des éditeurs²¹⁴ les acteurs de la Toile attributaires de ces moyens techniques. En effet, les fournisseurs d'accès ont l'obligation de leur fournir des moyens leur permettant « *de satisfaire aux conditions d'identification* » prévues respectivement à l'article 5 de la loi susmentionnée et à l'article 6-III de la LCEN qui obligent les éditeurs, personnes physiques et morales, exerçant leurs activités à titre professionnel ou non, à mettre à la disposition du public, dans un standard ouvert, l'ensemble des informations légales donnant aux internautes la possibilité d'obtenir des éléments d'identification les concernant.

²⁰⁹ Article 1147 du Code civil : « *Le débiteur est condamné, s'il y a lieu, au paiement de dommages et intérêts soit à raison de l'inexécution de l'obligation, soit à raison du retard dans l'exécution, toutes les fois qu'il ne justifie pas que l'inexécution provient d'une cause étrangère qui ne peut lui être imputée, encore qu'il n'y ait aucune mauvaise foi de sa part.* »

²¹⁰ Article 7 du COCC : « *Le débiteur peut garantir au créancier l'exécution d'une obligation précise ou s'engager simplement à apporter tous les soins d'un bon père de famille à l'exécution de son obligation. La responsabilité du débiteur est engagée par l'inexécution ou l'exécution défectueuse de son obligation.* »

²¹¹ Les obligations de moyens et de résultat (qui sera étudiée dans la suite de cette réflexion) ont pour siège, en droit français, l'article 1147 du Code civil et, en droit sénégalais, l'article 7 du COCC. François Dienes, faisant allusion à travers un article juridique à François Génys et René Demogue, préconise ceci, parlant de l'article 1147 : « *le centenaire du Code civil avait inspiré chez certains juristes comme François Génys et René Demogue une vision plus libérale du droit caractérisée par la nécessité d'adapter les textes aux exigences de la vie moderne.* » In D. François, « *Les applications de l'article 1147 du Code civil de 1804 à 2004* » Revue Générale de Droit (RGD), vol. 34, n° 3, 2004, p. 439.

²¹² D. François, « *Les applications de l'article 1147 du Code civil de 1804 à 2004* » RGD, vol. 34, n° 3, 2004, p. 464 : « *tandis que les obligations explicites sont constituées par l'ensemble des engagements expressément consentis par les parties ou définis par la loi, les obligations implicites sont des obligations latentes découlant des suites naturelles de chaque contrat ou du comportement des parties.* »

²¹³ In exposé des motifs de la loi sur les transactions électroniques : « *l'objet de ce présent projet de loi vise donc à assurer la sécurité et le cadre juridique nécessaires à l'émergence d'un commerce électronique fiable au Sénégal. Il prévoit notamment une consécration, dans un double souci d'efficacité et de sécurité...* »

²¹⁴ Article 4 al. 2 de la loi sur les transactions électroniques et article 6 – III – 1 de la LCEN

En ce qui concerne les autorités compétentes, les fournisseurs d'accès à Internet ont l'obligation, en vertu des articles 11 et 14 du décret n° 2008-719 du 30 juin 2008, de leur fournir des moyens techniques devant leur permettre un accès facile, direct et permanent aux informations portant sur les contenus litigieux, les données de connexion²¹⁵ sans oublier celles d'identification des éditeurs et des données à caractère personnel²¹⁶ de l'ensemble des utilisateurs dont l'exploitation est, par contre, encadrée²¹⁷. En l'espèce, le secret professionnel n'est pas opposable à l'autorité judiciaire²¹⁸.

S'agissant des tiers, les fournisseurs d'accès ont l'obligation de mettre à leur disposition un dispositif de signalement des contenus illicites, de préférence un formulaire simple d'utilisation et comportant le maximum de rubriques afin que suffisamment d'informations puissent être portées soit à leur connaissance soit à celle des autorités compétentes²¹⁹.

En tous les cas, au Sénégal comme en France, des sanctions sont prévues à l'encontre de quiconque n'aura pas respecté ces obligations. A titre illustratif, au Sénégal, la combinaison de l'article 15 du décret ci-devant cité et de l'article 431-46 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité, permet de retenir que le défaut de mise à disposition des éditeurs, des autorités compétentes et du public de ces mesures techniques légales, par les fournisseurs d'accès à Internet, est puni d'un d'emprisonnement de six mois à un an et d'une amende de 200 000 francs à 2 000 000 francs ou de l'une de ces deux peines seulement.

Quoi qu'il en soit, en plus de ces moyens techniques devant être appropriés, efficaces et accessibles en vue d'identifier les erreurs commises dans la saisie des données et de les corriger le cas échéant, il en est prévu d'autres destinés à la protection des mineurs non seulement lorsqu'ils utilisent les technologies de l'information et de la communication, mais aussi contre les agissements inconvenants des cyber-malfaiteurs.

B : Les moyens de protection des mineurs

Deux familles de moyens de protection des mineurs²²⁰ sont envisageables à ce niveau : les moyens de protection utilisés au moment de la connexion à Internet et ceux mis en branle pour contrecarrer les

²¹⁵ Article 4 al. 1^{er} de la loi sur les transactions électroniques et article 11, 12 et 13 du décret n° 2008 -719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008 - 08 du 25 janvier 2008 sur les transactions électroniques

²¹⁶ *Ibidem*.

²¹⁷ Article 4 al. 4 de la loi sur les transactions électroniques.

²¹⁸ Article 5 – 2 al. 3 *Idem*.

²¹⁹ Article 10 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les Transactions Electroniques.

²²⁰ Article 431-7-4 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité : « au sens de la présente loi, on entend par « mineur », toute personne âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant. » ; Article 1er de la Convention internationale des droits de l'enfant, Convention des Nations-Unies du 20 novembre 1989 : « au sens de la présente Convention, un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable. »

cyber-malfaiteurs utilisant les réseaux informatiques à des fins pédopornographiques²²¹, terroristes ou de cyberterrorisme.

L'autonomisation²²² des mineurs devant l'ordinateur, la tablette, le Smartphone, la Smartwatch²²³ connectés à Internet et le manque de vigilance des parents finissent par créer un vide autour de ceux-ci. Ce vide est comblé par Internet où les enfants trouvent une occupation, font des rencontres avec des interlocuteurs avec qui ils discutent sans tabous²²⁴, s'exposant *de facto* à des risques. Pour prévenir ces risques et rendre ainsi plus sûre la navigation des mineurs sur Internet, les législateurs imposent aux fournisseurs d'accès de proposer gratuitement au moins un²²⁵ moyen de contrôle parental. Au Sénégal, l'article 3 du décret n° 2008-719 du 30 juin 2008 prescrit même « *des mesures techniques de filtrage* ». Ce sont soit des moyens « *matériels de filtrage mi-mécaniques mi-informatiques fonctionnant, selon les cas, à l'aide de touches physiques ou de codes alphanumériques combinés à un CD²²⁶ d'installation, soit des logiciels* »²²⁷ de contrôle parental à télécharger gratuitement sur les sites des fournisseurs d'accès à Internet. Ils couvrent des aspects différents de la sécurisation de la navigation du mineur sur Internet²²⁸.

Ils peuvent fonctionner aussi avec des clés prohibés rendant l'accès à certains sites, impossible. Les logiciels les plus performants²²⁹, à l'image du « *Logiciel de Contrôle Parental Numéricable* »²³⁰ et du « *Contrôle Parental d'Orange V6* »²³¹, en France, vont jusqu'à analyser les contenus par catégories - violences, drogues, pornographie, racisme, jeux d'argent - et les images de sites *a priori* réputés propres.

²²¹ Ce qualificatif renvoie à la « *pornographie infantile* » prévue et définie par le droit sénégalais du numérique à travers l'article 431-7-5 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité : « *au sens de la présente loi, on entend par « 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.* »

²²² N. Cécile, « *La protection du mineur dans le cyberspace* » Thèse, Université de Picardie Jules Verne, Amiens, 2007, p. 214.

²²³ La Smartwatch, ou la « *montre intelligente* » ou encore la « *montre connectée* » a des fonctions multiples. On peut la décrire comme étant un petit ordinateur ambulant ou comme un Smartphone fixé au poignet. Elle sert ainsi de substitution au Smartphone. La montre connectée permet surtout à la personne qui la porte de : passer ou recevoir des appels, recevoir des alertes pour les SMS, les mails et les réseaux sociaux, avoir accès aux applications, se servir d'Internet, se localiser grâce au GPS, etc. Source : www.info-digitale.com, site visité le 22 septembre 2016.

²²⁴ *Op. cit.* note 222.

²²⁵ Article 6 *in fine* de la LCEN

²²⁶ Le CD (abréviation de « *Compact Disc* » en anglais) est un disque optique de 12 cm de diamètre et de 1,2 mm d'épaisseur (l'épaisseur peut varier de 1.1 à 1.5 mm) permettant de stocker des informations numériques. Source : www.commentcamarche.net ou en suivant le lien <http://www.commentcamarche.net/contents/736-cd-cd-audio-et-cd-rom#la-geometrie-du-cd>, site visité le 6 septembre 2019.

²²⁷ C'est le cas des LiveBox 1, 2 et Pro d'Orange. Source : Orange Ziguinchor

²²⁸ *Op. cit.* note 222.

²²⁹ In « *Tests E-enfance des logiciels de contrôle parental gratuits* » : « *les tests comparatifs d'E-Enfance sont conçus du point de vue des utilisateurs. Ils sont donc menés, avec la Délégation Interministérielle à la Famille / Ministère du Travail et la Délégation aux Usages de l'Internet, en se mettant dans la situation de clients lambda, c'est-à-dire en s'inscrivant auprès de chaque fournisseur d'accès à Internet comme le feraient n'importe quels parents* ». Source : www.e-enfance.org ou http://www.e-enfance.org/assistance-ordinateur_2.html, site visité le 23 septembre 2016.

²³⁰ Source : www.numericable.fr ou suivre le lien <https://client.numericable.fr/securite>, site visité le 23 septembre 2016.

²³¹ Source : www.orange.fr ou suivre le lien https://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/la-securite/controle-parental/controle-parental-d-orange-v6-pc-decouvrir_41733-42540, site visité le 23 septembre 2016.

Au Sénégal, les dispositions légales existantes depuis 2008 ne résolvent pas encore le fait que, dans la pratique²³², aucune mesure ne soit proposée aux utilisateurs ni dans les contrats d'abonnement ni sur les sites commerciaux²³³ des trois fournisseurs privés d'accès à Internet actuellement en activité.

Quoi qu'il en soit, un adolescent qui s'y connaît en informatique serait capable de déprogrammer ces logiciels ou même les désinstaller, accédant du coup à des contenus illicites à partir de n'importe quel moteur de recherches²³⁴. Pis, les mineurs peuvent consulter des sites inconvenants sous le couvert de l'anonymat, en mentant sur leurs âges ou *via* leurs propres²³⁵ tablettes, Smartphones ou Smartwatches en téléchargeant des applications inappropriées voire cryptées.

D'autre part, la manière d'utiliser certains programmes de filtrage n'a pas convaincu la jurisprudence. En France, les éditeurs de trois sites pornographiques ont été condamnés par la Cour d'appel de Paris²³⁶ pour insuffisance quant à la restriction de l'accès des mineurs à ces sites. La cour a estimé que « *la simple apposition d'un disclaimer²³⁷ avertissant de la nature du site était insuffisante* », considérant que les « *mises en garde et informations sur les logiciels de restriction d'accès présentées dans les pages d'accueil* » ne constituaient pas non plus des « *précautions utiles* ». La Cour d'appel a également retenu que c'était « *à juste titre que les premiers juges [avaient] relevé que l'obligation de précaution s'imposait au diffuseur du message et non au receveur* »²³⁸. Le juge français a ainsi rejeté l'approche consistant à faire reposer la responsabilité de la protection des mineurs, contre les contenus illicites, sur les utilisateurs eux-mêmes, non sans conforter l'irresponsabilité légale des fournisseurs d'accès qui, à partir du moment où ils ont doté leurs abonnés des moyens techniques en rapport avec la nature de la prestation, ne répondent pas de la manière dont ceux-ci s'en servent.

Dans le même sillage, en vertu de l'article 431-36 de la loi sur la cybercriminalité, le législateur sénégalais réprime le fait de faciliter à un mineur l'accès à des images, des documents, du son ou à une représentation présentant un caractère de pornographie. Les coupables de tels agissements sont en effet

²³² Informations obtenues lors de nos enquêtes menées, entre mars et septembre 2016 à Tigo Ziguinchor, Expresso Ziguinchor et Orange Ziguinchor.

²³³ Il s'agit des sites : www.orange.sn ou <https://assistance.orange.sn/questions/1189325-controle-parental>, de www.expressotelecom.sn ou <https://www.expressotelecom.sn/fr/termes-conditions> et de www.tigo.sn ou <http://www.tigo.sn/content/abonnements-contr%C3%B4le-parental>, tous visités le 23 septembre 2016.

²³⁴ Les FAI le savent tellement bien que certains n'hésitent pas à prodiguer dans ce sens des conseils pratiques aux parents. C'est le cas de ce conseil publié sur le site officiel d'Orange. « *Les restrictions d'accès sont efficaces et conseillées avec les jeunes enfants. Pour les adolescents, la sensibilisation et la responsabilisation reste la meilleure protection.* » Source : www.orange.fr, site visité le 25 septembre 2016.

²³⁵ Parce que les tablettes, Smartphones, Smartwatches des parents peuvent être équipés des applications de contrôle parental.

²³⁶ Cour d'appel de Paris, 2 avril 2002, repris par S. Valérie, in « *Principes généraux du droit de la responsabilité et responsabilité des acteurs de l'internet* », Article juridique, Légamedia, Paris, 2002, p. 11.

²³⁷ Un « *disclaimer* » est un anglicisme qui signifie « *dégagement de responsabilité* ». C'est un petit texte de droit, une formule qu'on trouve souvent en tête de la documentation d'un logiciel placé dans le domaine public ou libre, où l'auteur du programme décline toute responsabilité face aux dégâts que pourrait causer l'utilisation de sa production. Source : www.jargonf.org (Le Jargon Français : le dictionnaire d'informatique francophone) visité le 23 septembre 2016.

²³⁸ *Ibidem*.

punis de peines d'emprisonnement et d'amende ou de l'une des deux peines²³⁹. La vigilance du législateur en matière de protection des mineurs sur Internet est, ainsi, si grande qu'il a prévu et réprimé la déclinaison numérique des fautes traditionnellement commises sur eux, à commencer par les actes et comportements explicites²⁴⁰ et implicites²⁴¹ entrant dans le cadre de la pornographie infantile²⁴². Au Sénégal, il est puni d'un emprisonnement de cinq à dix ans et d'une amende de 5.000.000 à 15.000.000 francs ou de l'une de ces deux peines seulement, le fait de mener toute activité au profit d'autrui ou de soi « *par le biais d'un système informatique ou d'un moyen quelconque de stockage de données informatisées* » en rapport avec « *une image, un son ou des documents présentant un caractère de pornographie infantile* »²⁴³. Commises en bande organisée²⁴⁴, ces mêmes infractions sont punies du maximum de la peine prévue à l'article 431-23²⁴⁵ de la loi sur la cybercriminalité.

Certes, en droit sénégalais, ces agissements n'engagent en rien ni la responsabilité civile ni celle pénale du fournisseur d'accès à Internet tant qu'il se contente de ne jouer que son rôle passif de transmetteur de contenus. Mais à partir du moment où il y joue un rôle actif, il tombe sous le coup des sanctions sus-évoquées. En France aussi, les mêmes faits sont réprimés, notamment par les articles 225-12-1 à 225-12-4 et l'article 227-23 du Code pénal, sans oublier, selon la nature de la faute commise sur Internet, les sanctions prévues par la « *loi Cazeneuve* »²⁴⁶ et la loi n° 98-468 du 17 juin 1998 dite « *loi Guigou* »²⁴⁷ qui prévoit et réprime les infractions sexuelles contre les mineurs.

Les obligations d'information et de moyens mises à la charge des fournisseurs d'accès à Internet sont au cœur de la lutte contre les agissements illicites dans le cyberspace. A côté de ces obligations, il convient de noter d'une part les obligations de contrôle et de résultat, de l'autre et dans une moindre mesure, celle de surveillance.

²³⁹ Articles 431-34 et 431-35 de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

²⁴⁰ Clairement prévus par les textes juridiques en vigueur au Sénégal et en France.

²⁴¹ Il s'agit de la « *pseudo-pornographie infantile* », théorisée par la doctrine sous la plume d'Etienne WERY, évoquant une partie de l'article 227-23 du Code pénal français, in « *Sexe en ligne : aspects juridiques et protection des mineurs* », éd. Larcier, Bruxelles, 2004, p. 67. « *La pseudo-pornographie infantile englobe deux phénomènes : d'une part, les images virtuelles, les réalisations de synthèse et les dessins représentant des mineurs et, d'autre part, les images impliquant des personnes bien réelles ayant l'aspect de mineurs, mais qui sont en réalité majeurs au sens de la loi au moment où les photos sont prises.* »

²⁴² Article 431-7-5 de la loi sur la cybercriminalité : « *au sens de la présente loi, on entend par « 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.* »

²⁴³ Article 431-34 de la loi sur la cybercriminalité : « *Quiconque aura produit, enregistré, offert, mis à disposition, diffusé, transmis une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'un emprisonnement de cinq (5) à dix (10) ans et d'une amende de 5.000.000 à 15.000.000 francs ou de l'une de ces deux peines seulement.* »

²⁴⁴ Article 431-37 de la loi sur la cybercriminalité.

²⁴⁵ Article 431-23 de la loi sur la cybercriminalité : « *Quiconque aura procédé ou fait procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne conformément aux dispositions de l'article 68 de la loi sur les données à caractère personnel, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.* »

²⁴⁶ Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. JORF n° 0263 du 14 novembre 2014, voir aussi sur www.legifrance.gouv.fr, site visité le 16 septembre 2016.

²⁴⁷ Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. JORF n° 0139 du 18 juin 1998, p. 09255, voir aussi sur www.legifrance.gouv.fr, site visité le 16 septembre 2016.

Section 2 : L'obligation minimale de surveillance et les obligations de contrôle et de résultat

Surveiller tant soit peu ce qui se passe sur Internet est une chose, mais contrôler et surtout réagir en vue d'obtenir un résultat quelconque, lorsque cela s'impose, en sont d'autres. Tous les trois sont érigés en obligations par le législateur sénégalais et son homologue français qui, afin de s'assurer qu'un œil vigilant est gardé sur les faits et gestes sur la Toile, et qu'il y existe une certaine réactivité, ont fait peser sur les fournisseurs d'accès l'obligation minimale de surveillance (Paragraphe 1^{er}) de ceux-ci et les obligations de contrôle et de résultat (Paragraphe 2).

Paragraphe 1^{er} : L'obligation minimale de surveillance

Tandis qu'en France c'est la LCEN et, dans une large mesure, la directive sur le commerce électronique qui font peser l'obligation minimale de surveillance sur les fournisseurs d'accès, en droit sénégalais, c'est la loi sur les transactions électroniques qui l'institue. En effet, cette loi-ci, l'énonçant déjà dans son exposé des motifs²⁴⁸ en la posant comme étant parmi « *les règles relatives à la responsabilité des prestataires techniques* », prévoit l'obligation de surveillance ciblée et temporaire (A) en vue de la prévention et de la cessation du dommage (B).

A : La surveillance ciblée et temporaire

La surveillance ciblée et temporaire se démarque de la surveillance générale en ce qu'en plus d'être légale, elle procède d'une décision judiciaire.

C'est ainsi que conformément à l'article 3-5 alinéas 1 à 3 de la loi sur les transactions électroniques, les fournisseurs d'accès à Internet ne sont, d'emblée, « *pas soumis à une obligation générale de surveillance des contenus qu'ils transmettent* » ni à « *une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* ». Mais, l'autorité judiciaire peut leur imposer une obligation minimale de surveillance ciblée et temporaire, dans le cadre de la répression d'infractions aussi graves que « *l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie infantile, l'incitation à la violence et les atteintes à la dignité humaine* ». A ce titre, le législateur leur fait même l'obligation de dérouler toutes sortes d'activités²⁴⁹ de surveillance ciblée et temporaire, pourvu que celles-ci aient pour but la satisfaction de la demande formulée par l'autorité judiciaire.

²⁴⁸ V. point 5 de l'exposé des motifs de la loi sur les transactions électroniques : « *cette loi prévoit notamment ... des obligations minimales de surveillance et, partant des règles relatives à la responsabilité des prestataires techniques* »

²⁴⁹ Article 8 al. 2 du décret n° 2008 -719 du 30 juin 2008 relatif aux communications électroniques.

En droit français, c'est sur le fondement l'article 6-I-7, alinéas 1 à 3 de la LCEN²⁵⁰ que les fournisseurs d'accès sont exonérés de l'obligation générale de surveillance des contenus transportés - exonération²⁵¹ érigée d'ailleurs en interdiction²⁵² par le législateur communautaire européen - au profit de l'obligation minimale de surveillance ciblée et temporaire, prévue dans les mêmes conditions que celles retenues par le législateur sénégalais.

Par une ordonnance de référé du 10 février 2012, le TGI de Paris a retenu l'exonération de l'obligation générale de surveillance de six fournisseurs d'accès à Internet en déboutant le requérant, le ministre de l'intérieur M. Claude GUEANT, de sa volonté de les faire reconnaître coupables du transport de contenus qu'il estimait diffamatoires à l'encontre de la police française et de les condamner au blocage de trente cinq sites Internet²⁵³.

Si l'obligation minimale de surveillance mise à la charge du fournisseur d'accès à Internet est consacrée par le législateur, c'est pour qu'elle permette la prévention d'un dommage et la cessation d'un dommage actuel en matière de communication au public en ligne.

B : La prévention et la cessation du dommage

Le fait, pour le fournisseur d'accès à Internet, de prévenir et de faire cesser le dommage occasionné par les contenus litigieux, découle, tel que prévu par le législateur, d'une décision judiciaire. Au Sénégal, conformément aux dispositions de l'article 3-6 de la loi sur les transactions électroniques, le juge compétent peut prescrire, en référé ou sur requête, à tout hébergeur²⁵⁴ ou, à défaut, à tout fournisseur d'accès à Internet, « *toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». C'est dans les mêmes termes, au visa de l'article 6-I-8 de la LCEN²⁵⁵, que le législateur français a autorisé le juge à enjoindre aux fournisseurs d'accès à Internet la prévention et la cessation du dommage occasionné par les contenus mis en ligne.

²⁵⁰ Article 6 – 7, al. 1 à 3 de la LCEN : « *les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire. Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie infantile, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et à l'article 227-23 du Code pénal.* »

²⁵¹ Article 15 – 1 de la directive sur le commerce électronique : « *les Etats membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.* »

²⁵² Considérant 47 de la directive sur le commerce électronique : « *l'interdiction pour les Etats membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère général. Elle ne concerne pas les obligations de surveillance applicables à un cas spécifique et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale.* »

²⁵³ TGI Paris, Ord. Réf., « *Claude Guéant c/ Free et autres* », 10 février 2012. www.legalis.net, visité le 16 septembre 2016.

²⁵⁴ Cf. *Infra*, Seconde partie, Chapitre 2, Section 2, Paragraphe 2, (A).

²⁵⁵ Article 6 – I - 8 de la LCEN : « *l'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 [hébergeurs] ou, à défaut, à toute personne mentionnée au 1 [fournisseurs d'accès à internet], toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.* »

Ces dispositions consacrent, au Sénégal comme en France, le principe de subsidiarité dans leurs lois respectives ; en ce sens que les mesures devant amener à la prévention et la cessation desdits dommages devraient être d'abord conduites contre les hébergeurs des sites en cause et, ce n'est qu'après défaillance constatée de la part de ces derniers qu'elles nécessiteraient, au nom de l'intérêt général, d'être soulevées contre les fournisseurs d'accès. La jurisprudence précise que les conditions d'application de ce principe sont remplies dès lors que les demandeurs à l'action visant à obtenir des mesures de blocage démontrent qu'ils ont accompli les diligences nécessaires pour « *rechercher, par priorité, les prestataires d'hébergement sans pour autant devoir les assigner en la cause pour être recevables et que toute possibilité d'agir efficacement à l'encontre de ceux-ci s'avère objectivement vaine et en tout cas incompatible avec les exigences d'une procédure conçue pour la prise rapide de mesures dictées par l'intérêt général.* »²⁵⁶

Mais, le risque d'appliquer ces dispositions est, dans le cas du Sénégal, le fait de prendre le contrepied de l'alinéa 1^{er} de l'article 8 de la Constitution²⁵⁷ qui consacre entre autres la « *liberté d'expression et la liberté de presse* » ; tandis que pour la France, il pourrait s'agir de s'écarter de l'alinéa 1^{er} de l'article 10 de la Convention européenne des droits de l'homme²⁵⁸ qui consacre également la « *liberté d'expression* ». Si au Sénégal, l'alinéa 2⁵⁹ de la même disposition neutralise le risque, ce n'est pas forcément le cas de la France malgré les précautions prévues par l'alinéa 2⁶⁰ de l'article susmentionné.

En effet, en France, dans le cadre d'une affaire opposant des fournisseurs d'accès à Internet à plusieurs associations de lutte contre le racisme et l'antisémitisme²⁶¹, portant sur la circulation sur le site Internet de l'AAARGH²⁶², de propos pris pour racistes et négationnistes, dans deux ordonnances rendues le

²⁵⁶ *Ibidem.*

²⁵⁷ Article 8 al. 1er, Constitution du Sénégal : « *la République du Sénégal garantit à tous les citoyens les libertés individuelles fondamentales, les droits économiques et sociaux ainsi que les droits collectifs. Ces libertés et droits sont notamment : Les libertés civiles et politiques : liberté d'opinion, liberté d'expression, liberté de la presse, liberté d'association, liberté de réunion, liberté de déplacement, liberté de manifestation, les libertés culturelles, les libertés religieuses, les libertés philosophiques, les libertés syndicales, la liberté d'entreprendre, le droit à l'éducation, le droit de savoir lire et écrire, le droit de propriété, le droit au travail, le droit à la santé, le droit à un environnement sain, le droit à l'information plurielle.* »

²⁵⁸ Article 10 – 1, Convention européenne des droits de l'homme : « *toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.* » Trouver cette convention sur [www.echr.coe.int](http://www.echr.coe.int/Document/Library_Bibliotheque_Bulletin_2015_3.pdf) ou sur http://www.echr.coe.int/Documents/Library_Bibliotheque_Bulletin_2015_3.pdf, sites visités le 1^{er} octobre 2016.

²⁵⁹ Article 8 al. 2, Constitution du Sénégal : « *ces libertés et ces droits s'exercent dans les conditions prévues par la loi.* »

²⁶⁰ Article 10 – 2, Convention européenne des droits de l'homme : « *l'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire.* » *Op. cit.* note 258.

²⁶¹ A. Taïeb, « *La liberté d'expression est-elle garantie sur internet ?* », article cité par Thibault VERBIEST et Marie DE BELLEFROID in « *Filtrage et responsabilité des prestataires techniques de l'internet : retour sur l'affaire SABAM C/ Tiscali* », Chroniques et Opinions, Legipresse n°246, Novembre 2007, p. 160.

²⁶² F. Bergeron Aka, O. Masset, « *Affaire Aaargh : première et singulière application du référé LCEN* », article cité par Thibault VERBIEST et Marie DE BELLEFROID in « *Filtrage et responsabilité des prestataires techniques de l'internet : retour sur l'affaire SABAM C/ Tiscali* », Chroniques et Opinions, Legipresse n°246, Novembre 2007, p. 160, et puis, AAARGH signifie : Association des Anciens Amateurs de Récits de Guerre et d'Holocauste.

20 avril et le 13 juin 2005, le TGI de Paris ordonne aux fournisseurs d'accès cités en justice, d'interdire toute mise à disposition sur le territoire français, dudit site internet. La cour d'appel, saisie par les fournisseurs d'accès à Internet, confirmera ces décisions²⁶³. Cela suscite une interrogation sur l'existence d'un possible équilibre procédant de la conciliation des dispositions en matière de responsabilité des prestataires techniques, visée par l'article 6-I-8 de la LCEN et de la protection de la liberté d'expression prévue par l'article 10 de la convention ci-devant citée ; puisque c'est sur la base du premier que le TGI de Paris comme, à sa suite, la cour d'appel, ont ordonné aux fournisseurs d'accès à Internet de prendre toutes mesures propres à interdire l'accès au site en cause.

Un arrêt²⁶⁴ du TGI de Paris y répond par l'affirmatif. Selon cet arrêt, les pouvoirs conférés par l'article 6-I-8 la LCEN à l'autorité judiciaire constituent « *une conciliation qui n'est pas manifestement déséquilibrée* » entre cette liberté d'expression et les objectifs poursuivis.

Sans doute, l'assujettissement des fournisseurs d'accès à l'obligation minimale de surveillance est-il, pour le législateur, un moyen nécessaire de les amener à jouer un rôle actif dans la sécurisation du cyberspace, quitte à rompre légalement la neutralité qui est la clef de voûte de leur irresponsabilité dans cet espace virtuel. Cette obligation semble toutefois insuffisante. C'est l'une des raisons pour lesquelles elle a été renforcée par celles de contrôle, de résultat et de secret.

Paragraphe 2 : Les obligations de contrôle, de résultat et de secret

L'obligation de contrôle (A) et les obligations de résultat et de secret (B), que doivent respecter les fournisseurs d'accès à Internet, sont d'origine légale. Mais, pour assainir et sécuriser²⁶⁵ les transactions électroniques d'une part et, d'autre part installer la confiance numérique, les législateurs sénégalais et français n'ont pas manqué d'encadrer ces obligations.

A : L'obligation de contrôle

Au Sénégal, le législateur entend par obligation de contrôle des prestataires techniques, en l'espèce des fournisseurs d'accès à Internet, l'obligation selon laquelle ceux-ci, sauf disposition contraire²⁶⁶, sont tenus du contrôle spécifique des transactions électroniques afin de détecter d'éventuelles infractions²⁶⁷.

²⁶³ CA Paris, 4 nov. 2006, *SA Tiscali (Telecom Italia), AFA, France Telecom et a. c/UEJF, J'Accuse, SOS Racisme et a.*, cité par Thibault VERBIEST et Marie DE BELLEFROID in « Filtrage et responsabilité des prestataires techniques de l'internet : retour sur l'affaire SABAM C/ Tiscali », *Chroniques et Opinions*, Legipresse n°246, Novembre 2007, p. 160

²⁶⁴ TGI Paris, Ord. Réf., « *Claude Guéant c/ Free et autres* », 10 février 2012. www.legalis.net, visité le 16 septembre 2016.

²⁶⁵ In exposé des motifs de la loi sur les transactions électroniques : « *L'objet de ce présent projet de loi vise donc à assurer la sécurité et le cadre juridique nécessaires à l'émergence d'un commerce électronique fiable au Sénégal.* » Voir aussi l'article 1er du décret n° 2008-719 du 30 juin 2008 : « *Le présent décret a pour objet de fixer les conditions d'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, notamment celles relatives à la sécurité des transactions électroniques.* »

²⁶⁶ Notamment en application du point 5 de l'article 3 de la loi sur les transactions électroniques.

²⁶⁷ Article 8 al. 1^{er} du décret n° 2008 -719 du 30 juin 2008 relatif aux communications électroniques.

Cette obligation de contrôle passe par celle de surveillance ciblée et temporaire, demandée par l'autorité judiciaire aux fournisseurs d'accès dans l'espoir de détecter parmi les contenus qu'elle pointe, lesquels pourraient être illicites et, par conséquent, neutralisés dans le cadre de la prévention et de la cessation d'un dommage.

Les fournisseurs d'accès sont ainsi tenus de faire preuve de diligence pour ne pas laisser leur échapper des agissements dommageables.

C'est dire qu'il est possible d'engager leur responsabilité dès lors qu'un manquement à l'obligation de contrôle est prouvé. Autrement dit, l'engagement de la responsabilité civile ou de celle pénale du fournisseur d'accès à Internet, pour manquement à l'obligation de contrôle, pourrait se jouer sur le terrain de la preuve ; tout comme d'ailleurs les obligations de résultat et de secret qui lui incombent aussi.

B : Les obligations de résultat et de secret

Plutôt contractuelle et ayant pour siège²⁶⁸ en droit sénégalais l'article 7 du COCC et en droit français l'article 1147 du Code civil qui la jumèlent avec l'obligation de moyens²⁶⁹, l'obligation de résultat est l'obligation à travers laquelle le débiteur est tenu de fournir au créancier un résultat bien déterminé. Ce résultat doit être atteint, à défaut de quoi la satisfaction du créancier est incomplète.

En clair, au niveau des obligations de résultat, l'engagement du débiteur consiste à exécuter la promesse faite au créancier de l'obligation, sous peine d'engager sa responsabilité civile envers lui. En ce moment, le créancier doit apporter la preuve que le résultat n'est pas atteint, et c'est au débiteur qu'il appartient de justifier l'inexécution. Seuls un cas de force majeure²⁷⁰ ou une faute de la victime²⁷¹ peuvent exonérer le débiteur de l'obligation de résultat de sa responsabilité²⁷².

²⁶⁸ Son siège et non sa source. En ce sens, V. Marius TCHENDJOU, « *Droit des obligations* », éd. VUIBERT, Coll. Vuibert Droit, Paris, 2015, pp. 11-16 : « *les sources du droit des obligations sont plurielles, à savoir : la Constitution, la loi, la jurisprudence et les usages. Certaines obligations ont des origines jurisprudentielles. Il en est ainsi notamment de l'obligation de sécurité, d'information, de l'obligation de moyens et de l'obligation de résultat. Elles sont retenues par la jurisprudence dans le but d'adapter le droit aux exigences du moment. Cet effort effectué par les juges s'est manifesté tout particulièrement en droit de la responsabilité civile où, pour pallier les carences législatives, les juges ont dû créer un régime général de responsabilité du fait d'autrui ou adopter des solutions audacieuses destinées à provoquer une intervention législative.* »

²⁶⁹ *Op. cit.* notes 209, 210 et 211.

²⁷⁰ E. Julien, « *La responsabilité civile* », Fiche 14, 2000, p. 2 : « *la force majeure ou cas fortuit est un événement imprévisible, irrésistible et extérieur à l'activité du défendeur ou la chose, instrument du dommage. La preuve d'un tel événement entraîne l'exonération totale du défendeur puisqu'il n'a été que l'instrument passif de la force majeure, seule cause du dommage.* » Source : www.lagazettedescommunes.com, site visité le 20 Août 2016

²⁷¹ E. Julien, « *La responsabilité civile* », Fiche 14, 2000, p. 2 : « *la faute de la victime qui a elle-aussi contribué à la production de son propre dommage, pourra constituer une cause d'exonération totale ou partielle de responsabilité. La responsabilité du défendeur sera totalement écartée si la faute de la victime a présenté les caractères de la force majeure. La responsabilité du défendeur sera partiellement écartée si la victime a commis une faute qui a simplement concouru à la production de son dommage. Le juge diminuera le montant des dommages-intérêts octroyés à la victime.* » Source : *ibidem*.

²⁷² *Op. cit.* notes 270 et 271.

Au Sénégal, en matière de transactions électroniques, l'obligation de résultat est plutôt d'origine légale. En effet, sur le fondement de l'article 12 du décret n° 2008-719 du 30 juin 2008²⁷³ et de l'article 4 de la loi sur les transactions électroniques, les fournisseurs d'accès à Internet ont une obligation de résultat se traduisant par « *la détention et la conservation des données de nature à permettre l'identification de quiconque a contribué à la création du contenu en ligne ou de l'un des contenus des services dont ils sont prestataires* ». Il s'agit en principe, d'une part des données à caractère personnel²⁷⁴ y compris, depuis le 19 octobre 2016 - la cour de cassation française le confirme le 3 novembre 2016 - des adresses IP²⁷⁵ dynamiques²⁷⁶, d'autre part des données de connexion à Internet ou données relatives au trafic²⁷⁷. Toutes participent au final, à quelques exceptions près, de l'identification rapide et efficace des acteurs d'Internet ; car elles permettent la traçabilité de ceux-ci. Sauf que la détention et la conservation sont encadrées. Le législateur sénégalais prévient en effet, que ces données conservées portent exclusivement sur les éléments permettant l'identification des utilisateurs des services fournis par les fournisseurs d'accès et, en aucun cas, sur le contenu des correspondances échangées ni sur les informations consultées²⁷⁸. Il s'inscrit ainsi dans la droite ligne du principe constitutionnel de l'inviolabilité du secret de la correspondance²⁷⁹.

Cependant, si les fournisseurs d'accès détiennent des données manifestement fantaisistes, ne permettant pas l'identification envisagée par le législateur, ils engagent alors leur responsabilité par négligence, conformément à l'article 431-44 de la loi sur la cybercriminalité²⁸⁰.

Une fois conservées, les bonnes données de connexion, qui présentent des enjeux de politique criminelle²⁸¹, puisque permettant de remonter jusqu'à l'auteur du contenu²⁸², servent dans le cadre de

²⁷³ Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS n° 6439 du Samedi 22 novembre 2008.

²⁷⁴ Article 4 – 6 de la loi n° 2008 – 12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, J.O.R.S. n° 6406 du Samedi 3 mai 2008 : « *au sens de la présente loi, on entend par 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.* »

²⁷⁵ TGI de Paris, Ord. Réf., 5 mars 2009, *Roland Magdane et autres c/ YouTube* : « *l'adresse IP permet d'identifier une personne en indiquant sans aucun doute possible un ordinateur précis et établit la correspondance entre l'identifiant attribué lors de la connexion et l'identité de l'abonné* », sur www.legalis.net, site visité le 16 octobre 2016 ; confirmé par cet arrêt portant sur une autre affaire : Cass. Civ., 1ère ch., 3 nov. 2016, Arrêt n° 1184, pourvoi n° 15-22.595, *Cabinet Peterson c/ Groupe Logisneuf et autres*. www.courdecassation.fr, site visité le 3 novembre 2016.

²⁷⁶ CJUE, 2ème Ch., 19 octobre 2016, *Patrick Breyer c / Bundesrepublik Deutschland*, Affaire C-582/14, sur www.curia.europa.eu/juris/document/1404507, site visité le 19 octobre 2016.

²⁷⁷ V. « *Rapport explicatif de la Convention sur la cybercriminalité* », Série des traités européens n°185, Budapest, 23 novembre 2001, p. 7. « *Il s'agit de données produites par des ordinateurs appartenant à la chaîne de communication pour acheminer une communication de son origine à sa destination. Elles sont donc des auxiliaires de la communication elle-même et renseignent sur : l'origine de la communication (un numéro de téléphone, une adresse IP ou un moyen similaire d'identifier un dispositif de communication), la destination, l'itinéraire, l'heure (GMT), la date, la taille, la durée et le type du service sous-jacent (type du service utilisé au sein du réseau : transfert de fichiers, courrier électronique ou messagerie instantanée).* »

²⁷⁸ Article 13 du décret n° 2008 -719 du 30 juin 2008.

²⁷⁹ Article 13 de la Constitution du Sénégal du 22 janvier 2001 : « *le secret de la correspondance, des communications postales, télégraphiques, téléphoniques et électroniques est inviolable. Il ne peut être ordonné de restriction à cette inviolabilité qu'en application de la loi* », voir aussi <http://www.gouv.sn/-Constitution-du-Senegal-.html>, site visité le 9 septembre 2016.

²⁸⁰ Article 431-44 de la loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité.

²⁸¹ T. Papa Assane, « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 440.

l'enquête²⁸³. La traçabilité des utilisateurs, véritable fil d'Ariane de la responsabilité²⁸⁴, ne peut alors qu'être utile au législateur pour atteindre et neutraliser les cyber-malfaiteurs. C'est ainsi que l'autorité judiciaire a le pouvoir, sous l'empire de l'article 11, alinéa 2 du décret susmentionné, de demander aux fournisseurs d'accès à obtenir les données portant sur l'identification des personnes utilisatrices de leurs services. Et si, en droit sénégalais, le législateur n'a pas précisé une durée de conservation de ces données, se bornant à prévoir, pour celles à caractère personnel, « *une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées* »²⁸⁵, il a par contre fait état d'un décret à prendre pour définir les données concernées. Pas encore disponible, ce décret devrait déterminer « *la durée et les modalités de conservation* »²⁸⁶ desdites données. Celui qui est disponible, à savoir le décret n° 2008-721 du 30 juin 2008²⁸⁷, n'a pas résolu cela ; mais leur traitement sera soumis²⁸⁸ aux dispositions de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel.

Dans le même temps, en France, l'article 6-II de la LCEN prescrit comme obligation de résultat, la détention et la conservation des données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus²⁸⁹ des services dont les fournisseurs d'accès sont prestataires, tout en donnant à l'autorité judiciaire le pouvoir d'en requérir communication auprès d'eux. Le décret²⁹⁰ d'application de cet article définit les données concernées tout en déterminant la durée et les modalités de leur conservation. Il en est ainsi de la conservation, en vertu de l'article 1^{er} de ce décret, pour chaque connexion des utilisateurs, « *de l'identifiant de la connexion, de l'identifiant attribué à l'abonné, de l'identifiant du terminal utilisé pour la connexion, des dates et heures de début et de fin de la connexion, et des caractéristiques de la ligne de l'abonné* ». Son article 3 prévoit « *une durée d'un an de conservation des données* » avec des différences pratiques quant au début du chronométrage²⁹¹. Le fournisseur d'accès qui manque au respect de ces dispositions engage la responsabilité.

²⁸² R. Pascal, « *Le fournisseur d'accès et la conservation des données engendrées par les communications électroniques.* » Communication Commerce électronique, Juin 2005, n° 6, p. 19, cité par Papa Assane TOURE, *op. cit.* note 281.

²⁸³ *Op. cit.* note 281.

²⁸⁴ P. Philippe, « *De la trace à la traçabilité : des enjeux nouveaux pour des nouveaux risques* », cité par TOURE Papa Assane, *Idem*.

²⁸⁵ Article 35 de la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, JORS n° 6406 du Samedi 3 mai 2008.

²⁸⁶ Article 4 al. 5 de la loi sur les transactions électroniques.

²⁸⁷ Il s'agit du décret n° 2008-721 du 30 juin 2008, portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel ; J.O.R.S. n° 6443 du samedi 20 décembre 2008, pp. 1169-1177.

²⁸⁸ Article 4 al. 4 de la loi sur les transactions électroniques.

²⁸⁹ Article 2 du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne : « *La contribution à une création de contenu comprend les opérations portant sur : a) Des créations initiales de contenus ; b) Des modifications des contenus et de données liées aux contenus ; c) Des suppressions de contenus* ».

²⁹⁰ Il s'agit du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, JORF n° 0050 du 1 mars 2011, texte 32 sur 170.

²⁹¹ Article 3 du décret n° 2011-219 du 25 février 2011 : « *La durée de conservation des données mentionnées à l'article 1er est d'un an : a) S'agissant des données mentionnées aux 1o et 2o, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu telle que définie à l'article 2 ; b) S'agissant des données mentionnées au 3o, à compter du jour de la résiliation du*

A côté de l'obligation légale de résultat à la charge des fournisseurs d'accès, l'on retient l'obligation de secret professionnel. Consacrée en droit sénégalais par l'article 5-2 de la loi sur les transactions électroniques et l'article 16²⁹² du décret n° 2008-719 du 30 juin 2008, cette obligation est mise en œuvre dans les mêmes conditions que celles prévues à l'article 363²⁹³ du Code pénal, quant à la divulgation des éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée.

Le législateur sénégalais prévoit des limites à cette obligation de secret, puisqu'au sens de l'article 17 du même décret et de l'article 5-2 alinéa 3 de la même loi, non seulement elle cesse dès que la révélation des éléments d'identification personnelle est faite par la personne concernée, mais aussi le secret professionnel n'est pas opposable à l'autorité judiciaire.

A l'instar du fournisseur d'accès à Internet, l'hébergeur est bénéficiaire d'un aménagement encadré de responsabilité, dans le cadre de sa fonction remplie en tant que professionnel ou non.

contrat ou de la fermeture du compte ; c) S'agissant des données mentionnées au 4o, à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement ».

²⁹² Article 16 du décret n° 2008-719 du 30 juin 2008 : « l'obligation de secret prévu à l'article 5 de la loi sur les transactions électroniques s'impose à toutes les personnes dont l'activité est d'offrir un accès en ligne à des services au public par le biais des technologies de l'Internet notamment les éléments d'identification personnelle qui leur sont confiés dans le cadre de leur activité professionnelle. »

²⁹³ Article 363 du Code pénal : « Les médecins, chirurgiens, ainsi que les pharmaciens, les sages-femmes et toutes autres personnes dépositaires, par état ou par profession ou par fonctions temporaires ou permanentes, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter dénonciateurs, auront révélé ces secrets, seront punis d'un emprisonnement d'un à six mois et d'une amende de 50.000 à 300.000 francs. Le secret professionnel n'est jamais opposable au juge qui, pour les nécessités des investigations qu'il accomplit ou ordonne, peut en délier ceux qui y sont astreints. Il est également inopposable aux officiers de police judiciaire et aux agents de la Direction générale des Impôts et des Domaines agissant dans le cadre des enquêtes préliminaires diligentes sur instructions écrites du Procureur spécial près la Cour de Répression de l'Enrichissement illicite, pour la recherche et la constatation des infractions prévues par l'article 163 bis. Les alinéas 2 et 3 ci-dessus ont été institués par la loi n° 81 53 du 10 juillet 1981 relative à l'enrichissement illicite. »

Seconde partie

La responsabilité aménagée des hébergeurs

Au Sénégal comme en France, l'aménagement de la responsabilité des hébergeurs procède de la volonté du législateur. Mais sitôt l'exonération de la responsabilité civile et pénale de ces prestataires techniques énoncée qu'elle est soumise à des conditions. En clair, l'exonération de la responsabilité des hébergeurs est limitée (Chapitre 1^{er}), mais maintenue quant aux obligations générales de surveillance et de recherche (Chapitre 2).

CHAPITRE 1^{er} : L'exonération limitée de responsabilité

Il s'agira d'abord d'examiner l'exonération de la responsabilité civile et pénale (Section 1^{ère}) des hébergeurs, puis les limites de cette exonération (Section 2).

Section 1^{ère} : L'exonération de la responsabilité civile et pénale

Tandis qu'au Sénégal, dans les années 1990, on assistait à un vide juridique, la question de la responsabilité de l'hébergeur retenait, pour la première fois en France, l'attention du justiciable dans les affaires « *Estelle Hallyday* » et « *36 15 Renouveau* ».

Dans la première, par arrêt du 10 février 1999²⁹⁴, la cour d'appel de Paris, statuant en référé, a condamné un hébergeur à verser à Estelle Hallyday, une provision en guise de dommages-intérêts et à faire publier un communiqué à ses frais, pour avoir « *créé et hébergé* » le site « *Altern.org* » diffusant sans autorisation de l'intéressée, des photos portant atteinte au droit qu'elle détenait « *sur son image et à l'intimité de sa vie privée* ». Un an plus tôt, l'arrêt « *service 36 15 Renouveau* »²⁹⁵ rendu le 8 décembre 1998 par la cour de cassation avait retenu que le promoteur d'un service de communication audiovisuelle et d'échange d'opinions sur des thèmes prédéfinis, pouvait être poursuivi « *en qualité de producteur* » en application de la responsabilité en cascade prévue par l'article 42 de la loi du 29 juillet 1881²⁹⁶ sur la liberté de la presse. Cette décision semblait déjà discutable²⁹⁷ au sens où la Cour avait assimilé²⁹⁸ un producteur de services à un producteur de contenus, actuellement désigné sous le nom de « *fournisseur de contenus* ».

Pourtant avant ces affaires, l'hébergeur, appelé à l'époque « *centre serveur* »²⁹⁹, avait toujours vu sa responsabilité écartée en matière civile au titre des contenus par exemple « *à caractère pornographique* »³⁰⁰

²⁹⁴ CA Paris, 14^{ème} Ch, Sect. A, 10 février 1999, *Estelle H. c/ Valentin L.*; arrêt disponible à travers le lien <http://altern.org/alternb/defense/jugement.html>, visité le 25 septembre 2016.

²⁹⁵ T. Papa Assane, « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 402.

²⁹⁶ JORF du 30 juillet 1881 page 4201, article 42 (modifié par ordonnance du 26 août 1944, art. 15, JORF 30 août 1944 ; loi 52- 336 du 25 mars 1952, art. 4, JORF 26 mars 1952) : « *seront passibles, comme auteurs principaux des peines qui constituent la répression des crimes et délits commis par la voie de la presse, dans l'ordre ci-après, savoir : 1) les directeurs de publications ou éditeurs, quelles que soient leurs professions ou leurs dénominations, et, dans les cas prévus au deuxième alinéa de l'article 6, de les codirecteurs de la publication ; 2) à leur défaut, les auteurs ; 3) à défaut des auteurs, les imprimeurs ; 4) à défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs. Dans les cas prévus au deuxième alinéa de l'article 6, la responsabilité subsidiaire des personnes visées aux paragraphes 2°, 3° et 4° du présent article joue comme s'il n'y avait pas de directeur de la publication, lorsque, contrairement aux dispositions de la présente loi, un codirecteur de la publication n'a pas été désigné.* » Cette même responsabilité en cascade, qui est en fait un mécanisme de responsabilité éditoriale, est prévue aux : Livre 3 (des crimes, des délits et de leur punition), Titre 1^{er} (crimes et délits contre la chose publique), Chapitre IV (crimes et délits contre la paix publique), Section VI (des infractions commises par tous moyens de diffusion publique), articles 470 à 472 du Code pénal sénégalais.

²⁹⁷ T. Papa Assane, « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 400.

²⁹⁸ A. LEPAGE, « *Liberté d'expression, responsabilité et forums de discussion* », *Comm. Com. Electr.*, janvier 2003, p. 21 ; également A. LUCAS, J. DEVEZE et J. FRAYSSNET, « *Le droit de l'informatique et de l'Internet* », PUF, 2001, p. 117, n° 1006, tous cités par Papa Assane TOURE in « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 402.

²⁹⁹ I. Olivier, « *Peut-on assimiler un hébergeur au directeur de publication d'un magazine de presse ?* » Article, *JDN*, 7 novembre 2000, ou sur www.journaldunet.com, visité le 25 septembre 2016.

³⁰⁰ Cass. Crim. 15 novembre 1990 Bull. Crim. 1990 n°388 ; 17 Novembre 1992 Les Petites Affiches 12 avril 1993, n°44. *Op.cit.*, note 274.

ou au regard d'un arrêt du 8 janvier 1998³⁰¹, voire en matière pénale par le biais de la « *complicité par fourniture de moyens* »³⁰². Mais ce fut en 2000 que la directive³⁰³ sur le commerce électronique stabilisa la responsabilité de l'hébergeur ; laquelle, faudrait-il le rappeler, fut transposée en 2004 en droit français par la LCEN, source d'inspiration du législateur sénégalais à travers la loi sur les transactions électroniques, en 2008.

La stabilisation a consacré une exonération de la responsabilité civile et pénale de l'hébergeur à des conditions alternatives, ponctuées par l'utilisation répétée de la conjonction de coordination « *ou* ». Il doit en effet se plier à l'obligation de prompt réaction dès connaissance du forfait (Paragraphe 2), à défaut de justifier de la méconnaissance (Paragraphe 1^{er}) de celui-ci.

Paragraphe 1^{er} : La méconnaissance, condition de l'exonération

La méconnaissance, comme l'une des conditions d'exonération de la responsabilité de l'hébergeur, suppose qu'elle le soit effectivement en ce qui concerne non seulement l'illicéité du contenu (A), mais également pour des faits, circonstances et activités générateurs dudit contenu (B).

A : La méconnaissance de l'illicéité du contenu

En droit sénégalais et en droit français, en vertu des dispositions législatives en vigueur, la responsabilité civile des hébergeurs ne saurait être engagée à cause des contenus qu'ils stockent sur leurs serveurs s'ils méconnaissent effectivement le caractère illicite desdits contenus. Le législateur sénégalais a prévu cela à l'article 3-2, alinéa 1^{er} de la loi sur les transactions électroniques en précisant que leur responsabilité civile ne pourrait être engagée s'ils « *n'avaient pas effectivement connaissance du caractère illicite* » des contenus stockés. C'est, entre autres, la même condition, avec les mêmes termes, qui est posée par le législateur français à travers l'article 6-I-2, alinéa 1^{er} de la LCEN.

Dans le même temps, les articles 3-3, alinéa 1^{er} de la loi sur les transactions électroniques et 6-I-3, alinéa 1^{er} de la LCEN disposent qu'on ne saurait non plus engager la responsabilité pénale des hébergeurs à raison des informations qu'ils stockent, à partir du moment où ils n'avaient pas « *effectivement connaissance* » de l'illicéité de celles-ci.

La question qui se pose porte sur l'insistance des législateurs sur l'adverbe « *effectivement* » antéposé au vocable « *connaissance* ». Autrement dit, il y a lieu de chercher à stabiliser le sens juridique du fait d'avoir « *effectivement connaissance* ». Si les législateurs n'ont pas explicité cette expression, encore moins défini, un arrêt du TGI de Nanterre a retenu qu'il suffirait de l'« *apprécier au regard des*

³⁰¹ Cass. Crim, 8 janvier 1998, *Affaire Ricard*, inédit, *idem*

³⁰² Cass. Crim, 15 novembre 1990, Bull. Crim, n°388, *idem*.

³⁰³ Directive n° 2000/31/CE 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 dite « *directive sur le commerce électronique* », JOCE 17 juillet 2000, n° L 178, pp. 1-16.

compétences propres du fournisseur d'hébergement. »³⁰⁴ Mieux, un arrêt de la cour de cassation, du 17 février 2011, indiquera qu'« un hébergeur pourra être tenu pour responsable de contenus illicites dès qu'il en aura eu connaissance de façon très précise ».

Il semble par conséquent, à la lumière de ces arrêts, que le fait d'avoir « *effectivement connaissance* » ne consiste pas pour les hébergeurs, à avoir des connaissances complètes et rigoureuses³⁰⁵ voire scientifiques, pour s'assurer de l'illicéité du contenu.

A défaut donc de cette « *effective connaissance* », les hébergeurs pourraient valablement se prévaloir d'une certaine méconnaissance de l'illicéité des contenus qu'ils hébergent. Mais encore, faudrait-il qu'ils justifient de la méconnaissance des faits, des circonstances et des activités générateurs des contenus illicites stockés.

B : La méconnaissance des faits, circonstances et activités générateurs du contenu illicite

Le législateur sénégalais et son homologue français ont prévu, aux termes des articles 3-2, alinéa 1^{er} et 6-I-2, alinéa 1^{er} respectivement de la loi sur les transactions électroniques et de la LCEN, que tant que les fournisseurs d'hébergement n'ont pas « *effectivement connaissance des faits et circonstances faisant apparaître* » le caractère illicite des contenus qu'ils stockent, ils ne peuvent voir leur responsabilité civile engagée.

A ce titre, l'article 14-I-a de la directive sur le commerce électronique³⁰⁶ fait obligation aux Etats membres de « *veiller à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente* ».

L'article 3-3, alinéa 1^{er} de la loi sénégalaise évoquée et l'article 6-I-3, alinéa 1^{er} de la LCEN, prévoient une exonération de la responsabilité pénale de l'hébergeur, en raison des contenus illicites qu'ils stockent, tant qu'il est en situation de méconnaissance effective de l'activité génératrice de ces contenus. C'est dire que la responsabilité de l'hébergeur peut être engagée lorsqu'il ne fait rien pour retirer ou empêcher l'accès au contenu dont le caractère illicite lui est apparu sur des faits et circonstances.

³⁰⁴ TGI de Nanterre, 1ère Ch., Sect. A, 24 mai 2000, *Union des Etudiants Juifs de France (Uejf) / SA Multimania Production*, www.legalis.net, site visité le 30 septembre 2016.

³⁰⁵ P. Sandrine, « *La connaissance pure du droit et ses limites* », éd. Vrin, Paris, 2000, p. 2. Un extrait est publié sur www.droitconstitutionnel.org, ou <http://www.droitconstitutionnel.org/congresmtp/textes4/PINA.4.pdf>, site visité le 5 octobre 2016.

³⁰⁶ Directive n° 2000/31/CE 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 dite « *directive sur le commerce électronique* », JOCE 17 juillet 2000, n° L 178, pp. 1-16.

Cependant, l'expression « *faisant apparaître* », revenue dans les dispositions évoquées ci-dessus, signifie que l'hébergeur n'engagera pas sa responsabilité s'il refuse de retirer le contenu dont il peut raisonnablement douter du caractère illicite. Ce qui voudrait dire, quant à la procédure judiciaire, qu'il appartiendra au demandeur de démontrer, d'une part le caractère illicite des données et informations litigieuses et, de l'autre, que l'hébergeur a eu connaissance d'éléments suffisamment précis et probants³⁰⁷ lui donnant toutes les raisons de croire au caractère illicite de ce contenu.

Seulement, autant les hébergeurs sont légalement exonérés de leur responsabilité civile et pénale en cas de méconnaissance d'une part de l'illicéité des contenus stockés, d'autre part des faits, circonstances et activités les ayant générés, autant ils sont tenus à l'obligation d'une prompte réaction dès qu'ils en ont une connaissance effective.

Paragraphe 2 : L'obligation de prompte réaction dès connaissance du forfait

La prompte réaction dès connaissance du forfait rend compte de la réactivité³⁰⁸ dont doivent faire preuve les hébergeurs dès qu'ils ont effectivement connaissance de l'illicéité des contenus qu'ils stockent. Celle-ci ne doit cependant pas être sans effet, à savoir le fait de rendre inaccessible le contenu illicite (B), à défaut de le retirer (A) tout bonnement des serveurs.

A : Le retrait du contenu illicite

En droit sénégalais, comme en droit français, le fait pour l'hébergeur de retirer promptement de ses serveurs un contenu illicite, dès qu'il en a une connaissance effective, participe de l'exonération légale de responsabilité dont il bénéficie.

Ce régime spécial de responsabilité est prévu, au Sénégal, par l'article 3 - 2 et 3 de la loi sur les transactions électroniques et, en France, par l'article 6 - I - 2 et 3 de la LCEN. Cela change le rapport de l'hébergeur au contenu, passant de la passivité³⁰⁹ à la réactivité³¹⁰ non sans résultat heureusement légal pour le premier, à savoir le retrait pur et simple du second dès l'instant qu'il se convainc de son illicéité. Cette conviction, découlant de la connaissance effective du caractère illicite par l'hébergeur, devrait en fait passer par une étape essentielle, celle de savoir si le contenu est en réalité « *manifestement illicite* », tel que

³⁰⁷ P. Jurgita, « *L'évolution du régime de la responsabilité de l'hébergeur* », Chronique, Paris, Lamy, 2004, p. 14

³⁰⁸ Article 3 - 2, al. 1^{er} *in fine* et 3 - 3, al. 1^{er} *in fine* de la loi sur les transactions électroniques et l'article 9, al. 2 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi sur les transactions électroniques ; voir également l'article 6 - I - 2, al. 1^{er} *in fine* et 6 - I - 3, al. 1^{er} *in fine* de la LCEN ; voir enfin Considérant 46 et article 14 - 1 - b) de la directive sur le commerce électronique

³⁰⁹ CJUE, Gde. Ch., 12 juillet 2011, *L'Oréal c/ EBay International*, Affaire n°C-324/09, <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-324/09>, site visité le 1^{er} octobre 2016, voir aussi CA de Paris, Pôle 5, 1^{ère} Ch., 2 décembre 2014, *TF1 et autres / Dailymotion*. www.legalis.net, site visité le 1^{er} octobre 2016.

³¹⁰ Cass. Civ. 1^{ère} Ch., 17 février 2011, *Nord-Ouest Production et autres c/ Dailymotion*, www.legavox.fr, site visité le 06 août 2016.

prévu en droit sénégalais par l'article 9 du décret n° 2008-719 du 30 juin 2008³¹¹, et précisé dans la définition donnée à son article 2-2, probablement inspiré du Considérant 9 de la décision n° 2004/496 DC du 10 juin 2004 du conseil constitutionnel français³¹². Dans cette décision, le Conseil constitutionnel a émis une réserve quant à l'interprétation des I-2 et I-3 de l'article 6 de la LCEN. Il a estimé que, « *considérant que les 2 et 3 du I de l'article 6 de la loi déférée ont pour seule portée d'écarter la responsabilité civile et pénale des hébergeurs dans les deux hypothèses qu'ils envisagent ; que ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge.* »

Autant retenir, à la lueur de la précision définitionnelle³¹³ du législateur sénégalais dans le décret susmentionné et de la réserve émise par le conseil constitutionnel français dans la décision venant d'être évoquée, que pour retirer promptement le contenu illicite de ses serveurs, l'hébergeur ne saurait en aucun cas être juge³¹⁴ de l'« *illicite* »³¹⁵, il peut tout de même être « *celui du manifestement illicite* »³¹⁶. N'empêche, l'injonction du juge pour le retrait d'un contenu litigieux, préconisée par le Conseil constitutionnel, est inscrite à l'article 8 de la *loi Cazeneuve* qui prévoit et réprime le délit d'apologie du terrorisme sur Internet. En France toujours, au nom du droit à l'oubli³¹⁷ et du droit à l'image³¹⁸, qui étaient déjà protégés en dehors de la Toile, deux décisions de suppression de contenus illicites ont été rendues à l'encontre de l'hébergeur Google, respectivement en 2010 et 2013. Dans la première espèce, le juge a estimé que la question centrale dont il s'agissait, et qui avait motivé la condamnation à supprimer les contenus, était celle « *du droit à l'oubli* »³¹⁹ numérique. Dans la seconde, le TGI de Paris a « *condamné Google Inc. sur le fondement des articles 1382 et 1383 du Code civil* » à verser la somme de 4000 euros à titre de dommages-intérêts avant de lui « *ordonner de supprimer les contenus* »³²⁰ litigieux.

³¹¹ Il s'agit du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

³¹² JORF du 22 juin 2004, p. 11182, texte n° 3, Recueil, p. 101, voir aussi sur www.conseil-constitutionnel.fr, site visité le 24 septembre 2016.

³¹³ *Op. cit.* note 44. Et pour la définition en tant que telle, V. note 196.

³¹⁴ H. Christine, « *La responsabilité des acteurs de l'Internet dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* », Contrats - Concurrence Consommation, n° 11, 2004, p. 8, citée par Jurgita PETRAUSKAITE in « *L'évolution du régime de la responsabilité de l'hébergeur* », Chronique, Paris, Lamy, 2004, p. 14 ; en ce sens voir aussi Papa Assane TOURE in « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 419.

³¹⁵ TGI Paris, réf., 4 avr. 2013, RLDI 2013/94, n° 3129, p. 51 : « *l'hébergeur n'a pas l'obligation de vérifier le caractère illicite d'un contenu diffamatoire* ».

³¹⁶ T. Papa Assane « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal* », éd. L'Harmattan, Paris, 2014, p. 419.

³¹⁷ Cela fait plus d'un quart de siècle déjà que ce droit est débattu au niveau des prétoires. Cass. Civ., 1ère Ch. 20 novembre 1990, pourvoi n°89-12580. La Cour a estimé que « *dès lors qu'une information à caractère privée a été licitement divulguée en leur temps, l'intéressé ne peut invoquer un droit à l'oubli pour empêcher qu'il en soit à nouveau fait état* ».

³¹⁸ CA de Paris, 1re ch. B, 19 juin 1998, D. 1998, IR, p. 204, Voir aussi in « *Droit à l'image des personnes* » article, La SAIF, p. 1, ou en suivant le lien www.saif.fr/IMG/pdf/Droit_a_l_image_des_personnes.pdf, site visité le 15 octobre 2016.

³¹⁹ TGI de Paris 17ème Ch. 5 septembre 2010, commentaire de Jérôme HUET pp. 429-430. Légipresse n°278, pp. 426 à 430. Décembre 2010

³²⁰ TGI de Paris 17ème Ch. Civ., 23 octobre 2013, Bruno L. *Ressources et actualisation c/ Google Inc., Google France*, www.legalis.net, site visité le 26 septembre 2016

Au Sénégal, l'affaire des jeunes filles de Grand-Yoff (Dakar) a donné une occasion au juge de se prononcer sur un contenu illicite dans le système informatique. Dans cette affaire impliquant quatre jeunes filles et jugée par le Tribunal Régional Hors Classe (TRHC) de Dakar le 19 juin 2012³²¹, deux d'entre elles se livraient à des actes contre-nature pendant que les deux autres les filmaient à l'aide de leurs téléphones portables. En possession de la vidéo, de jeunes garçons l'ont partagée avec des tiers via la technologie Bluetooth³²². Ils ont été condamnés pour outrage aux bonnes mœurs à l'aide d'un moyen de communication électronique. Selon les juges, « *les représentations montrant les jeunes filles se livrant à des agissements sexuellement explicites, impliquant des personnes du même sexe, constituent des images contraires aux bonnes mœurs au sens de l'article 431-59³²³ du Code pénal* » et donc de la loi sur la cybercriminalité. Le juge avait d'autre part reproché à ces jeunes garçons le fait de « *stocker et d'envoyer* » la vidéo litigieuse à des tiers par Bluetooth.

Toujours au Sénégal, dans « *l'affaire Palluci* »³²⁴, dont le jugement est rendu le 10 mars 2010³²⁵, le TRHC de Dakar a condamné un homme à une peine d'emprisonnement ferme conformément à l'article 431-59 de la loi sur la cybercriminalité. Cet homme avait ouvert une boîte mail et envoyé à partir d'elle, des photos qu'il avait prises pendant qu'il vivait ensemble et en bons termes avec une femme, lesquelles montraient celle-ci dans des positions obscènes ; ceci, après leur séparation. Dans cette espèce, les juges n'ont pas retenu la qualité de correspondance privée du mail. Mais pour ne pas s'éloigner des textes, alors que les délits reprochés au prévenu étaient entre autres « *la distribution d'images contraires aux bonnes mœurs* » à maintenir dans le lot des infractions commises par tous moyens de diffusion publique, les juges ont mis en œuvre, par analogie, le critère de la communauté d'intérêts. Ainsi, ont-ils finalement retenu ceci : « *les photographies litigieuses ont été envoyées au moyen d'un courrier électronique, c'est-à-dire un moyen de diffusion publique au sens de l'article 431-58 du Code pénal ; qu'en effet, si le courrier électronique au moyen duquel les photos sont diffusées est assimilé à une correspondance privée, il reste*

³²¹ TRHC Dakar, n° 2715 du 19 juin 2012, *affaire des jeunes filles de Grand-Yoff*, inédit, mais repris par Papa Assane TOURE in « *Cinq ans de droit pénal des technologies de l'information et de la communication (2008 – 2013) : chronique de jurisprudence sénégalaise* », Cour Suprême, Dakar, Bull. d'Info., Décembre 2015, n° 7 – 8, pp. 117 – 150.

³²² Bluetooth, littéralement en Anglais « *dent bleue* », est une technologie de réseaux personnels sans fils notée WPAN, pour « *Wireless Personal Area Network* », d'une faible portée (entre 10 et 100 m) et permettant de relier des appareils entre eux sans aucune liaison filaire. Source : www.commencamarche.net ou <http://www.commentcamarche.net/contents/108-bluetooth>, site visité le 27 septembre 2016.

³²³ Article 431-59 du Code pénal : « *Sera puni d'un emprisonnement de 6 mois à 7 ans, d'une amende de 500 000 francs à 10 000 000 francs ou l'une de ces deux peines seulement quiconque aura : 1) fabriqué ou détenu en vue d'en faire commerce, distribution, location, affichage ou exposition ; 2) importé ou fait importer, exporté ou fait exporter, transporté ou fait transporter sciemment aux mêmes fins ; 3) affiché, exposé ou projeté aux regards du public ; 4) vendu, loué, mis en vente ou en location, même non publiquement ; 5) offert, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ; 6) distribué ou remis en vue de leur distribution par un moyen quelconque. Tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs. Le maximum de la peine sera prononcé lorsque les faits ci-dessus visés ont un caractère pornographique. Le condamné pourra en outre faire l'objet, pour une durée ne dépassant pas six mois, d'une interdiction d'exercer, directement ou par personne interposée, en droit ou en fait, des fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publication périodiques. Quiconque contreviendra à l'interdiction visée ci-dessus sera puni des peines prévues au présent article.* »

³²⁴ TRHC Dakar, n° 1159 du 16 mars 2010, *affaire Palluci*, inédit, *Op. cit.* note 321.

³²⁵ Ce jugement a été confirmé par un arrêt de la cour d'appel de Dakar du 25 mars 2011 : C.A. Dakar, n° 356 du 25 mars 2011, *affaire Palluci*, inédit, *Op. cit.* 321.

cependant qu'en l'espèce, la diffusion incriminée revêt un caractère public, les mails contenant en fichiers attachés les photos litigieuses, ayant été envoyés à treize personnes dont il n'est pas établi qu'elles sont liées par une communauté d'intérêts »³²⁶.

S'il est vrai qu'il n'est pas indiqué dans ces espèces l'injonction des juges de faire supprimer les contenus litigieux, il ne semble pas moins vrai que s'ils l'avaient fait, ils auraient certainement eu gain de cause pour les jeunes garçons, au contraire des correspondants de M. PALLUCI, encore moins de l'hébergeur de la plateforme dans laquelle il avait ouvert sa boîte mail. En tous les cas, cette seconde affaire rappelle un phénomène qui se développe sur Internet et auquel les prestataires techniques devraient faire face. Il consiste à propager des photos ou des vidéos sexuelles d'ex-partenaires contre leur gré, avec des conséquences allant jusqu'au suicide³²⁷. L'objectif poursuivi est l'humiliation à la suite d'une rupture, d'un refus sentimental ou d'une infidélité. Il résulte d'une enquête³²⁸ menée en 2016, qu'en Ile-de-France 28% des jeunes dont 17% de filles ont été victimes, au moins une fois, de violences à caractère sexuel sur Internet. Mais l'article 226-2-1 du code pénal français, nouvellement créé par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique³²⁹ en son article 67, érige cette pratique en délit qu'il sanctionne par des peines de « deux ans d'emprisonnement et 60 000 euros d'amende ». Cette disposition sanctionne les fournisseurs de contenus, laissant à l'alinéa 2 de l'article 226-2 du même code, le soin de prévoir que si ce délit est commis en des matières spéciales comme celle de « la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

Le retrait du contenu illicite des serveurs des hébergeurs, fut-il prompt, participe de la mise en œuvre de l'exonération de leur responsabilité. Le législateur qui l'a prévu, lui a joint le fait de rendre inaccessible ce contenu.

B : Le fait de rendre inaccessible le contenu illicite

La promptitude avec laquelle l'hébergeur est tenu de retirer de ses serveurs tout contenu illicite, voire manifestement illicite, dès qu'il en a effectivement connaissance, est valable lorsqu'il s'agit de rendre ledit contenu inaccessible.

En droit sénégalais, le législateur prévoit à l'article 9, alinéa 2 du décret n° 2008-719 du 30 juin 2008, que les hébergeurs, après avoir informé les autorités compétentes de l'existence d'un contenu en

³²⁶ Sur l'ensemble de cette question, voir Papa Assane TOURE, « Cinq ans de droit pénal des technologies de l'information et de la communication (2008 – 2013) : chronique de jurisprudence sénégalaise », Cour Suprême, Dakar, Bull. d'Info., Décembre 2015, n° 7 – 8, pp. 117 – 150.

³²⁷ M. Maïa, « La pornographie comme revanche », Lemonde.fr, 09 octobre 2016, site www.lemonde.fr, visité le 09 octobre 2016.

³²⁸ Enquête menée par le « Centre francilien pour l'égalité femmes-hommes » : « ... 17 % des filles et 11 % des garçons déclarent avoir été confrontés à des cyber-violences à caractère sexuel, à travers la diffusion virale de selfies dénudés ; les garçons gagnent en popularité, et les filles sont jugées de manière négative et insultées. » Source : www.centre-hubertine-auclert.fr, site visité le 09 octobre 2016.

³²⁹ JORF n° 0235 du 8 octobre 2016, p. 7, Texte 1, voir sur www.legifrance.gouv.fr, site visité le 8 octobre 2016.

ligne manifestement illicite, directement ou indirectement et dans les meilleurs délais, doivent agir promptement pour en rendre l'accès impossible conformément aux dispositions légales en vigueur.

En effet, en vertu de l'article 3-2 et 3 de la loi sur les transactions électroniques, pour ne pas voir leur responsabilité engagée, les hébergeurs ont l'obligation, dès qu'ils ont effectivement connaissance du caractère illicite, d'une part des contenus qu'ils stockent à la demande des destinataires de leurs services, d'autre part d'activités, de faits et de circonstances faisant apparaître ce caractère, d'agir promptement afin d'en rendre l'accès impossible. A titre illustratif, après une mise en demeure faite aux opérateurs de jeux d'argent et de hasard ou de paris en ligne, non autorisés, de cesser leurs activités illicites sous huitaine, en cas d'inexécution de l'injonction par l'intéressé à l'issue de ce délai, le président de l'ARJEL peut saisir le président du TGI de Paris aux fins d'ordonner aux hébergeurs, en la forme des référés, de faire usage de toute mesure destinée à arrêter purement et simplement l'accès aux sites litigieux³³⁰. L'initiative de la mise en demeure peut résulter d'un constat fait par l'Arjel-même ou d'une saisine de la part du ministère public ou bien de toute personne physique ou morale ayant intérêt à agir³³¹.

Le décret³³² n° 2011-2122 du 30 décembre 2011 pris pour l'application de l'article 61 de la loi n° 2010-476 du 12 mai 2010 et qui explicite les modalités de blocage des sites de jeux illégaux, prescrit dans sa notice que « *lorsque l'arrêt de l'accès à une offre de paris ou de jeux d'argent et de hasard en ligne a été ordonné par le président du TGI de Paris... les hébergeurs de sites doivent procéder à cet arrêt* ». Ce même décret prévoit à son article 1er, que l'arrêt doit être fait « *en utilisant le protocole de blocage par nom de domaine³³³ (DNS) qui consiste à rendre inopérant le système de noms utilisé pour localiser des ordinateurs et des services en ligne.* »

Dès lors, dans le cadre de la mise en œuvre de la responsabilité aménagée des prestataires techniques, dans plusieurs affaires, le juge français a conforté l'exonération de responsabilité³³⁴ profitant aux hébergeurs tant qu'ils sont restés neutres³³⁵ à l'égard des contenus et ont agi promptement pour en rendre l'accès impossible à défaut de les avoir retirés dès qu'ils ont effectivement eu connaissance ou conscience³³⁶ que ceux-ci étaient soit illicites soit liés à des activités, des faits ou encore des circonstances illicites. Dans une affaire concernant l'hébergeur *Dailymotion*, le juge a retenu qu'« *aucun manquement à l'obligation de promptitude à retirer le contenu illicite ou à en interdire l'accès ne pouvait être reproché à*

³³⁰ Article 61 de la 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, JORF n° 0110 du 13 mai 2010, voir aussi sur www.legifrance.gouv.fr, site visité le 25 août 2016.

³³¹ *Ibidem*.

³³² JORF n°0001 du 1 janvier 2012, texte n° 25, page 41.

³³³ Sur le régime juridique des noms de domaine, voir Abdoul Aziz DIOUF, in « *Essai sur le régime juridique des noms de domaine* », Thèse, Université d'Orléans, 2010, p. 27.

³³⁴ Cass. Civ. 2^{ème} Ch., 18 février 2010, *Active communication Ltd (Act Com) c/ Ville de Marseille*, www.legalis.net, visité le 4 mai 2016.

³³⁵ Cass. Civ. 1^{ère} Ch., 17 février 2011, *Nord-Ouest Production et autres c/ Dailymotion*, www.legavox.fr, site visité le 06 août 2016 ; voir aussi TGI Paris, 17^e ch., 14 nov. 2011, *Olivier M. c/ Sté Prisma Presse et a.*, www.legalis.net, site visité le 19 septembre 2016.

³³⁶ Considérant 46 de la Directive sur le commerce électronique. *Op. cit.* note 72.

la société Dailymotion qui n'avait eu connaissance effective du contenu litigieux qu'avec l'assignation à jour fixe et les pièces annexées »³³⁷.

Au Sénégal et en France, l'exonération de la responsabilité civile et pénale de l'hébergeur a certes été légalement consacrée tout en étant encadrée quant à sa mise en œuvre, mais cela n'en fait pour autant pas attributaire d'une immunité juridique au sens où cette exonération ne prospère ni même ne prévaut dès l'instant où celui-ci change de statut dans son rapport au destinataire de ses services ; d'où l'existence de limites à l'exonération de sa responsabilité civile et pénale.

³³⁷ Cass. Civ. 1ère Ch., 17 février 2011, *Nord-Ouest Production et autres c/ Dailymotion*, www.legavox.fr, site visité le 06 août 2016.

Section 2 : Les limites à l'exonération de la responsabilité civile et pénale

Assurer la sécurité³³⁸ des transactions électroniques et installer la confiance dans l'économie numérique tout en gardant en ligne de mire « *le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression et la sauvegarde de l'ordre public* »³³⁹, c'est la finalité poursuivie par le législateur respectivement au Sénégal et en France, mais pas à n'importe quel prix. En effet, l'exonération de responsabilité, qui est accordée à l'hébergeur, s'analyse davantage en une manière de le mettre à l'aise et de le doter de moyens d'accompagnement juridiques lui permettant de jouer son rôle dans « *la lutte contre l'acceptation, le traitement et la diffusion de contenus illicites* »³⁴⁰, qu'en un privilège ou une immunité juridique au détriment des autres acteurs d'Internet.

C'est dire dès lors, qu'un hébergeur qui, sous le couvert ou pas de cette exonération légale, pose des actes attestant de son autorité ou de son contrôle sur le destinataire (Paragraphe 1^{er}) de ses services, engage sa responsabilité ; encore qu'il est déjà présumé avoir connaissance des faits litigieux sur Internet (Paragraphe 2).

Paragraphe 1^{er} : L'autorité ou le contrôle de l'hébergeur sur le destinataire

L'autorité de l'hébergeur sur le destinataire (A) de ses services ou le contrôle (B) qu'il exerce sur lui, constituent des limites à l'exonération de la responsabilité civile et pénale dont jouit ce prestataire technique.

A : L'autorité de l'hébergeur sur le destinataire

En droit sénégalais, l'omission d'un quelconque exercice de l'autorité de l'hébergeur sur le destinataire de service, de la liste des conditions de désengagement de sa responsabilité civile et pénale, est prévue aux alinéas 2 des points 2 et 3 de l'article 3 de la loi sur les transactions électroniques. Le législateur y prescrit en ce sens que l'exonération « *ne s'applique pas lorsque le destinataire du service agit sous l'autorité* » de l'hébergeur.

Le droit français de l'économie numérique retient la même prescription, les mêmes conditions de mise en œuvre et les mêmes notions utilisées au niveau des alinéas 2 des points 2 et 3 du paragraphe I de l'article 6 de la LCEN. Mais si au Sénégal, comme en France, le législateur s'est borné à énoncer lesdites prescriptions, les ressources du droit commun rendent compte du fait que, par analogie, la relation entretenue par l'hébergeur et le destinataire du service laisse penser à celle qui existe entre le commettant

³³⁸ In exposé des motifs de la loi sur les transactions électroniques : « *l'objet de ce présent projet de loi vise donc à assurer la sécurité et le cadre juridique nécessaires à l'émergence d'un commerce électronique fiable au Sénégal. Il prévoit notamment une consécration, dans un double souci d'efficacité et de sécurité...* »

³³⁹ Article 1^{er} de la LCEN.

³⁴⁰ V. le point 6 de l'exposé des motifs de la loi sur les transactions électroniques, où le législateur énonce « *la participation des hébergeurs et des fournisseurs d'accès à la lutte contre l'acceptation, le traitement et la diffusion de contenus illicites* ».

et le préposé ; et lorsque le premier est une personne morale, ce peut par extension être entre elle et ses organes ou représentants.

Si tels étaient les cas, alors au Sénégal, sous l'empire de l'article 146 du COCC, l'hébergeur, en tant que commettant ou patron, répondrait des dommages causés par la personne du destinataire de service, soumise à son autorité, lorsque celle-ci encourait dans l'exercice de ses fonctions une responsabilité à l'égard d'autrui. D'autre part, agissant pour le compte de l'hébergeur, personne morale, le destinataire engagerait dans les mêmes conditions la responsabilité de celui-ci. Mieux, en vertu de l'article 147 du COCC, l'hébergeur, en tant que commettant, est encore responsable lorsque son préposé, le destinataire, a agi sous son autorité au moins apparemment, dans l'exercice de ses fonctions. Et même en cas d'abus de fonction de la part du destinataire du service, s'il est établi un lien de causalité ou de connexité avec l'exercice de ses fonctions, cela suffirait à rendre l'hébergeur responsable.

Cette déportation de l'engagement de la responsabilité civile de l'hébergeur vers le droit commun peut alors tenir au fait que, même dans l'exercice de sa fonction d'hébergeur qui est protégée, ce dernier ne joue plus que ce rôle. Par conséquent, ce faisant, il sort du champ d'application de l'exonération de responsabilité. Toutefois, le législateur précise à l'article 149 du COCC qui détermine le type de rapport existant entre le commettant et le préposé, que la responsabilité du commettant, l'hébergeur, n'exclut pas celle du préposé, le destinataire du service. C'est ainsi qu'à l'alinéa 2 de cet article, l'on peut retenir qu'en cas de dommage causé, « *tous deux sont solidairement responsables du dommage causé, et le civilement responsable peut exercer un recours contre son préposé.* »

En France, l'article 1384 alinéa 5 du Code civil prévoit à titre analogique, à l'encontre d'un hébergeur ne s'étant pas limité à sa neutralité à l'égard des contenus stockés et exerçant une autorité sur le destinataire de ses services, qu'il est responsable en tant que commettant, du dommage causé par son préposé dans les fonctions auxquelles il l'a employé. Seulement, la responsabilité de l'hébergeur ne saurait être engagée en cas de dommages causés par le destinataire qui aurait agi hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions³⁴¹ ; sauf « *si la victime démontre qu'elle pouvait légitimement croire que le préposé agissait à des fins conformes à son emploi* »³⁴².

Au plan pénal, l'article 461-62 de la loi sur la cybercriminalité, donc du code pénal sénégalais, et l'article 121-2 du code pénal français prévoient que les personnes morales autres que l'Etat, les collectivités locales - ou territoriales et leurs groupements - et les établissements publics « *sont pénalement responsables des infractions commises pour leur compte par leurs organes ou représentants ; la*

³⁴¹ Ass. Plén., 19 mai 1988, D. 1988-513, 2000, p. 4.

³⁴² V. « *Pour une réforme du droit de la responsabilité civile* », Cour de Cassation, Rapport, sous la direction de François TERRE, Paris, 2012, p. 10. Voir sur www.courdecassation.fr ou suivre le lien <https://www.courdecassation.fr/IMG/reforme-droit-RC.pdf>, visité le 1^{er} octobre 2016.

responsabilité des personnes morales n'exclut pas celle des personnes physiques auteures ou complices des mêmes faits ». Les peines encourues sont nombreuses et vont de « l'amende à la fermeture définitive ».

Dans une affaire concernant le moteur de recherches *Google Suggest*, la cour de cassation française, qui a infirmé d'abord la qualité d'hébergeur de cet organe appartenant à l'hébergeur *Google Inc.*, l'a ensuite condamné en tant que « fournisseur de moyens », pour « complicité de contrefaçon de droit d'auteur » constituée par le fait de « mettre à disposition des liens menant vers des contenus illicites. »³⁴³

L'autorité de l'hébergeur sur le destinataire de service est couplée par le législateur au fait, pour ce prestataire technique, d'exercer un contrôle sur cet acteur d'Internet.

B : Le contrôle exercé par l'hébergeur sur le destinataire

A l'instar de l'exercice d'une autorité sur le destinataire de service par l'hébergeur, celui de son contrôle sur ce dernier est prévu, en droit sénégalais, aux alinéas 2 des points 2 et 3 de l'article 3 de la loi sur les transactions électroniques. En droit français, ce sont les alinéas 2 des points 2 et 3 du paragraphe I de l'article 6 de la LCEN qui l'ont énoncé. Les législateurs de ces pays ont prévu que toutes les fois que le destinataire du service d'hébergement a agi sous le contrôle du fournisseur d'hébergement, alors le régime exonératoire de responsabilité accordé à ce dernier ne saurait lui être appliqué en cas de faute.

Si tel n'était pas le cas, le contenu, peu importe qu'il fût *a priori* licite ou illicite, serait fourni par le destinataire du service et, à sa demande³⁴⁴, stocké en toute neutralité par l'hébergeur. Se mettant alors dans une situation et une position de contrôleur des faits et gestes du destinataire du service, il semble logique que l'hébergeur ait un traitement différent de celui au titre duquel il est appelé à participer à « la lutte contre l'acceptation, le traitement et la diffusion de contenus illicites »³⁴⁵. Si bien qu'en ne bénéficiant dorénavant plus du régime spécial et indulgent de la responsabilité civile et pénale dont il est légalement déchu, l'hébergeur est en conséquence régi par celui du droit commun de la responsabilité.

En droit sénégalais, alors qu'au plan pénal l'article 461-62 du Code pénal cité plus haut pouvait jouer, au plan civil, il serait peu probable que ce ne fût pas l'article 142 du COCC qui ne régît pas sa situation. En effet, en vertu de cette disposition, « on est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre. »

Le même traitement lui serait alors réservé en droit français, sous l'empire de l'article 1384 alinéa 1^{er} du Code civil, lequel prévoit aussi qu' « on est responsable non seulement du dommage que l'on cause

³⁴³ Cass. Civ. 1^{ère}, 12 juill. 2012, Gaz. Pal. 25-26 juill. 2012, n° 208, p. 9, in Communication de Caroline LE GOFFIC, Revue Lamy droit de l'immatériel (RLDI) 2012/85, n° 2851.

³⁴⁴ Article 3 - 2 et 3 de la loi sur les transactions électroniques ; article 6 - I - 2 et 3 de la LCEN.

³⁴⁵ V. le point 6 de l'exposé des motifs de la loi sur les transactions électroniques, où il est prévu « la participation des hébergeurs et des fournisseurs d'accès à la lutte contre l'acceptation, le traitement et la diffusion de contenus illicites ».

par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre... ». En fait, l'article 1384 du Code civil énumère divers cas dans lesquels une personne qui n'est pas fautive peut être tenue d'indemniser une victime d'un dommage causé par autrui, dont elle a le contrôle, tel que par analogie, le serait ici l'hébergeur par rapport au destinataire de service, même si, comme c'est le cas dans le paragraphe précédent, en principe, le répondant dispose d'un recours auprès de l'auteur du dommage pour récupérer le montant des dommages-intérêts qu'il a été condamné à verser à la victime. Cette hypothèse retient d'autant plus l'attention que depuis l'arrêt BLIECK³⁴⁶, datant du 29 mars 1991, la cour de cassation française a décidé que la liste des cas de responsabilité du fait d'autrui de l'article 1384 alinéa 1^{er} du Code civil n'était plus limitative. Et, en condamnant sur le fondement dudit article l'association répondant de M. BLIECK, les juges estimaient que celle-ci « avait accepté la charge d'organiser et de contrôler, à titre permanent, le mode de vie de cet handicapé » mental.

Cet arrêt formulait ainsi un principe³⁴⁷ à savoir : désormais, c'était d'une façon générale que l'on était responsable du fait des personnes dont on avait la charge, notamment le contrôle comme c'est le cas, à titre analogique, de l'hébergeur et du destinataire de son service au sens des articles 3 - 2 et 3 de la loi sur les transactions électroniques et 6-I - 2 et 3 de la LCEN. Dans le même sillage, il est indiqué dans un rapport³⁴⁸ de la cour de cassation française dirigé par François TERRE, que : « la faute de la personne morale résulte de l'acte fautif de ses organes ou représentants ou d'un défaut d'organisation ou de fonctionnement. Une personne morale répond du dommage causé par une autre personne morale sur laquelle elle exerce un contrôle de droit ou de fait. »

Dans un arrêt du 14 juin 2016³⁴⁹, la cour d'appel de Paris a fait une lecture *a contrario* de l'article 6-I de la LCEN en refusant de condamner l'hébergeur *Wikimedia Foundation* pour une faute liée à l'édition de contenus illicites sur le site de l'encyclopédie *Wikipédia*. Dans cette espèce, la Cour d'appel a estimé que *Wikimedia* n'agissait « qu'en tant que service d'hébergement, en maintenant à titre gratuit des infrastructures et un cadre organisationnel qui permettaient de construire les projets *Wikimedia* dont celui du site encyclopédique *Wikipédia*. » Mieux, tout le contenu hébergé était « fourni par les utilisateurs sur lesquels *Wikimedia Foundation* » n'exerçait « aucun contrôle » ni ne jouait de « rôle actif ou éditorial, ce qui signifie que cette fondation ne surveille ni ne modifie aucun contenu stocké ».

En tous les cas, après avoir prévenu le fournisseur d'hébergement que s'il ne se limitait pas à son rôle neutre et passif d'hébergeur, il ne pourrait prétendre à aucune exonération de responsabilité, le

³⁴⁶ Cour de cassation, Assemblée plénière 29 mars 1991, pourvoi n° 89-15231, *Affaire BLIEK*. www.legifrance.gouv.fr, site visité le 30 septembre 2016 ; voir aussi in « *Présentation générale de la responsabilité civile : les faits générateurs, le fait d'autrui* », UCAD, FSJP, fiche TD, 2014/2015, Pr. A. A. DIOUF, Coord., Nd. F. LECOR, p. 41.

³⁴⁷ R. Frisson Marie-Anne, « *Commentaire de l'arrêt Blicck du 29 mars 1991, Cour de cassation, Assemblée plénière* », 2 janvier 2014, sur www.mafr.fr, site visité le 30 septembre 2016.

³⁴⁸ V. « *Pour une réforme du droit de la responsabilité civile* », Cour de Cassation, rapport, sous la direction de François TERRE, Paris, 2012, pp. 6-10. Voir sur www.courdecassation.fr ou <https://www.courdecassation.fr/IMG/reforme-droit-RC.pdf>, visité le 1^{er} octobre 2016.

³⁴⁹ CA de Paris, Pôle 1, 3^{ème} Ch., 14 juin 2016, *Mme X. / Wikimedia Foundation Inc.*, www.legalis.net, site visité le 1^{er} octobre 2016.

législateur a prescrit que celui-ci était présumé connaisseur des faits litigieux censés exister dans ses serveurs.

Paragraphe 2 : La présomption de connaissance des faits litigieux

La présomption de connaissance des faits litigieux entraîne, pour l'hébergeur, le retrait ou le fait de rendre inaccessibles les contenus tout aussi litigieux. Néanmoins, les destinataires de ses services sont soumis à l'exigence de notification (A) pour dénoncer les faits en cause ; faits et notification qu'ils devraient aussi prouver (B).

A : L'exigence de la notification

Le bénéficiaire, pour l'hébergeur, d'un régime de responsabilité exorbitant de droit commun est tel que la condition préalable pour engager sa responsabilité est de porter à sa connaissance les contenus illicites que le droit sénégalais qualifie à ce niveau de « faits litigieux ».

En pratique, il serait difficile et même impossible d'obtenir d'un hébergeur le contrôle de la totalité³⁵⁰ des faits qui ont lieu sur les sites qu'il héberge. Le législateur a alors mis en place un système de notification permettant aux utilisateurs de dénoncer des faits ou des contenus qu'ils prennent pour illicites. Une fois cette notification faite, l'hébergeur est alors présumé avoir connaissance des faits ou contenus dénoncés. En droit sénégalais, l'article 3-4 de la loi sur les transactions électroniques prévoit que la connaissance des faits litigieux est présumée acquise par les hébergeurs lorsqu'il leur est notifié une série d'éléments précis suivant un formalisme prédéfini, comme c'est le cas en France où la même procédure de notification est prévue à l'article 6-I-5 de la LCEN, rédigée dans les mêmes termes que ceux utilisés par le législateur sénégalais. Dès lors, la réception de la notification doit être promptement suivie, de la part de l'hébergeur, du retrait du contenu dénoncé, s'il se rend compte de son caractère manifestement illicite. D'ailleurs, en plus de la notification devant être faite par les utilisateurs, une autorité administrative, l'ARJEL par exemple, peut également saisir ce dernier pour le mettre en demeure d'arrêter les faits litigieux dans ses serveurs. S'il ne s'exécute pas, le juge pourra le lui imposer en la forme des référés³⁵¹.

En droit sénégalais, le législateur prescrit à l'article 7 du décret n° 2008-719 du 30 juin 2008 qu' « en cas de notification par écrit ou par voie électronique », les hébergeurs engageraient leur responsabilité s'ils laissaient en ligne « le contenu manifestement illicite ». Cependant, le droit sénégalais comme celui français ont consacré le délit d'abus de notification ou de fausse notification. Pour le premier, l'alinéa 2 du même article dispose : « l'abus de notification pour des faits non illicites est puni selon les dispositions de

³⁵⁰ En ce sens, les statistiques de 2015 sont suffisamment parlantes. En effet, en 2015, au moins 4 millions de fichiers ont été partagés par minute dans le monde sur l'ensemble du Net, 4 millions de recherches redirigées vers des sites Internet ont été effectuées par minute rien que sur Google, chaque jour ce sont en moyenne 830 000 nouveaux sites qui ont été mis en ligne, en moyenne 145 milliards d'emails ont été échangés par jour, 3,5 milliards d'internautes uniques ont été recensés dans l'année dont 2,2 milliards rien que sur les réseaux sociaux. Sources : www.journaldunet.fr et www.blogdumoderateur.com, sites visités le 9 octobre 2016.

³⁵¹ Article 61 de la 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, JORF n° 0110 du 13 mai 2010, voir aussi sur www.legifrance.gouv.fr, site visité le 25 août 2016.

l'article 431-43 de la loi sur la cybercriminalité », lequel prévoit que quiconque aura présenté aux hébergeurs « *un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'il sait cette information inexacte, sera puni d'un emprisonnement de six mois à un an et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement.* » Pour le second, l'article 6-I-4 de la LCEN prévoit à l'encontre de ces mêmes personnes la punition « *d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.* »

Dans le cadre de notifications bien faites, la cour d'appel de Paris a rendu un arrêt le 2 décembre 2014³⁵² condamnant l'hébergeur Dailymotion à verser 1,2 million d'euros de dommages et intérêts à plusieurs sociétés du groupe TF1 pour ne « *pas avoir promptement retiré de son site* » des vidéos leur appartenant, malgré les nombreux signalements de diffusion illicite de leurs programmes. La Cour a considéré qu'il y avait même « *566 manquements de Dailymotion à cette obligation de prompt retrait* » en laissant des vidéos illicites sur son site et donc dans ses serveurs entre « *7 et 104 jours après notification* », manquements constitutifs de faits de « *concurrence déloyale, parasitisme et contrefaçon.* »

Faudrait-il le retenir, au cas où la procédure de notification quant à l'existence de faits litigieux aurait commencé auprès d'éditeurs ou de fournisseurs de contenus, une fois qu'elle devrait concerner un hébergeur, une preuve dans ce sens devrait être nécessaire.

B : La preuve des faits et de la notification

L'exigence de preuve concerne plus l'utilisateur, personne physique ou morale, des services de l'hébergeur, que celui-ci. En effet, le législateur sénégalais et son homologue français l'ont prévue respectivement à l'article 3-4, points f) et g) de la loi sur les transactions électroniques et à l'article 6-I-5, tirets 5 et 6 de la LCEN.

La loi sénégalaise prévoit en ce sens qu'au moment de la notification à l'attention de l'hébergeur, l'utilisateur devrait non seulement se prémunir « *des justificatifs des faits* » litigieux, mais aussi « *la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification* ». Si, ni l'un ni l'autre ne pouvaient être contactés, ou s'ils l'étaient mais sans suite favorable, alors la notification devrait, en guise de preuve à l'attention de l'hébergeur, comporter « *la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.* »

Lorsque toutes les conditions de fond et de forme sont réunies, les juges font une application pragmatique des articles susmentionnés. A titre illustratif, l'on retiendra non seulement la première application de l'article 6 de la LCEN par le juge et qui a été favorable à l'hébergeur, en l'espèce la société

³⁵² CA de Paris, Pôle 5, 1ère Ch., 2 décembre 2014, *TF1 et autres / Dailymotion*. www.legalis.net, site visité le 1er octobre 2016.

*Free*³⁵³, mais aussi le fait que le TGI de Paris, dans une décision du 10 juillet 2009³⁵⁴, a fait une application stricte de ces dispositions en faveur de l'hébergeur *YouTube* qui, après avoir eu connaissance du caractère manifestement illicite d'un contenu, suite à une notification, a agi promptement pour en rendre l'accès impossible. Mais il faut dire qu'il n'est pas toujours facile de réunir toutes les conditions de forme et de fond prévues par le législateur. Or, la jurisprudence ne transige pas face au non-respect de celles-ci dans leur entièreté. D'abord, dans l'arrêt TF1 c/ Dailymotion, la Cour a estimé que « *le fait que le journal le Monde ait écrit que le match France/Italie de la coupe du monde de football de 1998 ait été diffusé sur TF1 et l'apparition du logo de TF1 dans la vidéo* » revendiquée par ce groupe, ne suffisaient pas comme « *justificatifs des faits* »³⁵⁵. Ensuite, dans un arrêt rendu le 17 février 2011, la Cour de cassation a retenu que « *la notification à l'hébergeur du caractère illicite des informations qu'il stockait devait contenir l'ensemble des mentions imposées par l'article 6-I-5 de la LCEN. À défaut du respect de cette formalité, Dailymotion n'avait pas à agir promptement pour retirer le contenu litigieux* »³⁵⁶.

Quoi qu'il en soit, au Sénégal, en vertu des dispositions de l'article 431-45 de la loi sur la cybercriminalité, l'hébergeur qui n'aura pas respecté les prescriptions de l'article 3 de la loi sur les transactions électroniques sera « *puni d'un emprisonnement de six mois à un an et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement.* »

Et même si elle était faite dans le strict respect du formalisme légalement requis, en cas de litige s'y rapportant, le juge a considéré que l'envoi en tant que tel, de la notification, devrait être prouvé. A travers une ordonnance de référé en date du 29 octobre 2007³⁵⁷, le TGI de Paris a estimé que la voie électronique n'était pas une preuve suffisante de notification, précisant qu'« *au regard des indications données sur le site, seule se trouve rapportée la preuve de l'envoi et non de sa réception* ». Par conséquent, la meilleure preuve serait alors « *un courrier adressé par la voie postale avec la preuve de sa réception* ».

La soumission de l'exonération de la responsabilité de l'hébergeur, à des conditions de réalisation, contribue à mettre en évidence son statut de prestataire purement technique et celui, circonstanciel, lui permettant d'exercer une autorité ou un contrôle sur le destinataire de ses services. N'empêche, le législateur prévoit qu'il soit déchargé des obligations générales de surveillance et de recherche.

³⁵³ TGI de Paris, Ord. Réf., 9 juillet 2004, *Groupama c/ Gérard D., Free*, sur www.legalis.net, site visité le 1er octobre 2016. Selon l'ordonnance de référé, « *sur l'absence de responsabilité de l'hébergeur, la société Free, hébergeur de ces sites, avait suspendu l'accès aux sites et adresses litigieux et s'était déclarée prête à transformer cette suspension en fermeture, conformément aux dispositions de l'article 6 de la LCEN, loi n°2004-575 du 21 juin 2004. Aucune responsabilité ne pouvait dès lors être retenue à l'encontre de l'hébergeur. Le Tribunal a donné acte à la société Groupama de son désistement à l'égard de la société Free.* » Ordonnance disponible également à travers le lien suivant <http://www.scaraye.com/article.php?a=143>, site visité le 1^{er} octobre 2016. Notons que *Free* joue ici un double rôle de fournisseur d'accès et de plateforme d'hébergement de blogs comme *Blogger* qui est 100% gratuit et appartient à Google, mais aussi *WordPress* qui est plutôt commercial sans oublier, au Sénégal, la plateforme *Seneweb*. Le juge étend l'exonération à ses types d'hébergeurs.

³⁵⁴ TGI de Paris, 3^{ème} Ch., 2^{ème} section, Jugement du 10 juillet 2009, *Bayard Presse / YouTube LLC.*, RLDI, n° 97, octobre 2013, p. 104.

³⁵⁵ CA de Paris, Pôle 5, 1^{ère} Ch., 2 décembre 2014, *TF1 et autres / Dailymotion*. www.legalis.net, site visité le 1er octobre 2016.

³⁵⁶ Cass. civ., 1^{ère} Ch., 17 février 2011, n° 09 – 15857, *Affaire Dailymotion*, Bull. civ. 2011, I, n° 32, RLDI, n° 97, octobre 2013, p. 104.

³⁵⁷ TGI de Paris, Ord. Réf., 29 octobre 2007, *Marianne B. et autres / Wikimedia Foundation*. www.legalis.net, site visité le 1^{er} octobre 2016.

CHAPITRE 2 : L'exonération des obligations générales de surveillance et de recherche

L'exonération de l'obligation générale de surveillance (Section 1^{ère}) et de l'obligation générale de recherche (Section 2), au profit des hébergeurs, est une consécration légale aussi bien au Sénégal qu'en France.

Section 1^{ère} : L'exonération de l'obligation générale de surveillance

Sur Internet, les données envoyées par les utilisateurs et stockées par les hébergeurs sont si importantes³⁵⁸ que leur maîtrise est extrêmement difficile. La loi sur les transactions électroniques et la loi pour la confiance dans l'économie numérique posent, comme un des grands principes de gestion commune d'une Toile sécurisée, l'exonération de l'obligation générale de surveillance qui a une étendue (Paragraphe 1^{er}) ponctuée par la consécration d'une obligation spéciale de surveillance et d'information (Paragraphe 2).

Paragraphe 1^{er} : L'étendue de l'exonération

L'étendue de l'exonération de l'obligation générale de surveillance couvre non seulement le stockage des informations (A), mais aussi leur nature (B).

A : Le stockage des informations

Les informations dont il s'agit sont non seulement celles qui sont déjà stockées, mais aussi les informations devant l'être. En droit sénégalais tout comme en droit français, ce sont les articles 3-5 de la loi sur les transactions électroniques et 6-I-7 de la loi pour la confiance dans l'économie numérique qui prévoient la dispense des fournisseurs d'hébergement de l'obligation générale de surveillance des contenus stockés. En clair, tant qu'ils se seront comportés comme tels, même à titre gratuit, ils ne seront « *pas soumis à une obligation générale de surveiller les informations* » qu'ils stockent.

La directive sur le commerce électronique en fait même une interdiction aux termes de son article 15. En effet, le législateur communautaire prescrit qu'il y a « *absence d'obligation générale en matière de surveillance* » ; absence en vertu de laquelle « *les Etats membres ne doivent pas imposer aux prestataires, pour la fourniture des services ... une obligation générale de surveiller les informations qu'ils transmettent ou stockent.* »

En 2007, la jurisprudence française a considéré qu'à partir du moment où un contenu faisait l'objet d'une notification de la part de son titulaire des droits, l'hébergeur convaincu de son caractère manifestement illicite, devait non seulement retirer l'ensemble des contenus identiques qu'il stockait déjà,

³⁵⁸ En ce sens, cf. les statistiques de 2015. *Op. cit.* note 350.

postés par différents fournisseurs de contenus, mais aussi procéder de manière préventive, à une surveillance ciblée et illimitée pour en empêcher une réapparition du fait de nouveaux utilisateurs. Cette forme de surveillance, qui semblait ériger en une obligation de non réapparition des contenus litigieux, découlait notamment, pour ne citer qu'elles, de la décision rendue le 19 octobre 2007 par le TGI de Paris dans le cadre de l'affaire dite « *Tranquillity Bay* »³⁵⁹, suivie de celle rendue par le tribunal du commerce de Paris le 20 février 2008 concernant l'affaire « *Le monde selon Bush* »³⁶⁰.

Mais dès 2012, la Cour de cassation, par deux arrêts rendus le même jour, à savoir le 12 juillet 2012³⁶¹, a mis à mal cette obligation établie par les juges, considérant que cette dernière constituait plutôt « *une obligation générale de surveillance* » qui ne saurait être mise à la charge des hébergeurs *Google France* et *Google Inc.* La Cour a précisé la nécessité de l'envoi d'une nouvelle notification de retrait du contenu litigieux qui est réapparu, pour que ces hébergeurs eussent « *effectivement connaissance de son caractère illicite et de sa localisation et [fussent] alors tenus d'agir promptement pour le retirer ou en rendre l'accès impossible* », sans quoi, leur responsabilité ne pouvait être engagée.

C'est dire que non seulement l'appréhension des contenus devrait se faire au cas par cas, mais aussi il n'y a lieu ni de mettre en place un dispositif de surveillance générale de contenus éventuellement similaires à ceux ayant déjà fait l'objet de mesures de retrait ou d'inaccessibilité après notification, ni de filtrer de manière disproportionnée et continue les prochaines mises en ligne de données. Mais à défaut du filtrage, des hébergeurs comme *YouTube*³⁶², *Twitter*³⁶³, *Google*³⁶⁴, *Dailymotion*³⁶⁵, etc. ont, pour plus de diligence et de célérité dans la procédure de notification de contenus « *inappropriés* »³⁶⁶, prévu des boutons de signalement très pratiques qui, même s'ils sont considérés comme « *insuffisants* »³⁶⁷ par le juge, ouvrent des formulaires relativement complets, à remplir et à poster à l'hébergeur concerné.

D'où une réflexion sur la nature des informations à traiter.

³⁵⁹ TGI de Paris, 3ème Ch., 2ème Sect., Jugement du 19 octobre 2007, *Zadig Productions et autres / Google Inc, Afa*, voir sur www.legalis.net, site visité le 3 octobre 2016.

³⁶⁰ TC de Paris, 8ème Ch., Jugement du 20 février 2008, *Flach Film et autres / Google France, Google Inc*, voir sur www.legalis.net, site visité le 3 octobre 2016.

³⁶¹ Cass. Civ 1^{ère} Ch., 12 juillet 2012, Pourvoi n° 11-13.669, *Sté Google France et Sté Google Inc. c/ Sté Bac films et Sté The Factory*; et Cass. Civ 1^{ère} Ch., 12 juillet 2012, Pourvoi n° 11-15.165, *Sté Google France et autres c/ Sté Auféminin.com*, Source : www.courdecassation.fr, site visité le 3 octobre 2016.

³⁶² Sur YouTube : http://www.youtube.com/t/copyright_notice, site visité le 3 octobre 2016.

³⁶³ Sur Twitter : <https://support.twitter.com/articles/82753#specific-violations>, site visité le 3 octobre 2016.

³⁶⁴ Sur Google : <https://support.google.com/legal/troubleshooter/1114905?hl=fr>, site visité le 3 octobre 2016.

³⁶⁵ Sur Dailymotion : <https://faq.dailymotion.com/hc/fr/requests/copyrightform-notification>, site visité le 3 octobre 2016.

³⁶⁶ C'est le mot qui revient le plus dans presque toutes les Conditions Générales d'Utilisation (CGU) de ces hébergeurs.

³⁶⁷ TGI de Paris, Ord. Réf., 29 octobre 2007, *Marianne B. et autres / Wikimedia Foundation*, voir sur www.legalis.net, site visité le 1^{er} octobre 2016.

B : La nature des informations

Au sens du droit sénégalais de l'informatique, notamment de l'article 3-22 de la loi n° 2008-41 du 20 août 2008 portant sur la cryptologie³⁶⁸, l'information est un « *élément de connaissance, exprimé sous forme écrite, visuelle, sonore ou numérique, susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué* ». Elle est parmi « *les principales ressources économiques et stratégiques de la société de l'information [et] fait l'objet d'une protection appropriée aux plans civil, administratif et pénal* »³⁶⁹

Examinée à l'aune de ces dispositions, il serait difficile de concevoir que la nature des informations que stockent les hébergeurs, ajoutée à leur quantité qui est inestimable, ne soit pas importante. D'où l'exonération de l'obligation générale de surveillance qui leur a été accordée et qui restera en vigueur tant que ses conditions³⁷⁰ de réalisation, en rapport avec la nature³⁷¹ et le caractère des contenus, seront respectées. Au cas contraire, l'hébergeur est tenu de les retirer ou d'en rendre l'accès impossible. L'attitude de l'hébergeur dépendra en partie de la réception préalable d'une notification faisant « *mention des dispositions légales* »³⁷² devant lui permettre de vérifier la nature du contenu pour en constater l'illicéité. L'utilisateur procédant à la notification devra toutefois se plier à « *l'obligation de précision* »³⁷³ y compris en ce qui concerne les URL³⁷⁴ litigieuses, s'abstenant ainsi de faire des réclamations « *larges, vagues et générales* »³⁷⁵. En ce sens, les juges ont estimé dans plusieurs décisions que la seule « *prétention* »³⁷⁶ de détenir des droits sur des œuvres ne saurait suffire à en faire des contenus illicites.

Pour autant qu'il veuille une Toile sans informations qui soient surveillées de manière générale et illimitée par les prestataires techniques, notamment les hébergeurs qui y détiennent le monopole du stockage permanent, le législateur n'en demeure pas moins alerte et précautionneux face aux éventuelles informations pouvant contenir le meilleur comme le pire, au point de prescrire à la charge de ces derniers une obligation spéciale de surveillance et d'information.

³⁶⁸ JORS N° 6441 du Samedi 6 décembre 2008, voir aussi sur www.jo.gouv.sn, site visité le 2 janvier 2016.

³⁶⁹ Article 4 de la LOSI.

³⁷⁰ Cf. articles 3-5, al. 1^{er} de la loi sur les transactions électroniques et 6-I-7, al. 1^{er} de la LCEN

³⁷¹ B. Armel, « *L'hébergement et le stockage de données médicales sensibles* », article, CGV Expert, Avril 2012, p.1, voir aussi sur www.cgv-expert.fr ou en suivant le lien http://www.cgv-expert.fr/article/hebergement-stockage-donnees-medicales-sensibles_43.htm, site visité le 20 septembre 2016.

³⁷² *Op.cit.* note 361.

³⁷³ TGI de Paris, Ord. Réf., 18 décembre 2007, *M. Jean-Yves L. et SARL L. Anonyme c/ SA Dailymotion*, sur www.legifrance.gouv.fr, site visité le 1^{er} octobre 2016.

³⁷⁴ URL, Anglais pour « *Uniform Resource Locator* », est une adresse Web. L'URL permet par exemple de localiser une page d'information sur un serveur, elle sert d'une façon générale à identifier des pages et des sites Internet. Source : www.justaskgemalto.com, site visité le 2 octobre 2016.

³⁷⁵ *Op. cit.* note 373 ; voir aussi l'article 3-4, e) de la loi sur les transactions électroniques et l'article 6-I-5, tiret 4 de la LCEN.

³⁷⁶ TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Mezrahi c/ Youtube* ; et TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Mezrahi c/ Google* ; et TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Magdane c/ Youtube*. Source : www.legifrance.gouv.fr, site visité le 3 octobre 2016.

Paragraphe 2 : La consécration d'une obligation spéciale de surveillance et d'information

Dans le cadre de sa fonction, l'hébergeur peut recevoir une demande de l'autorité judiciaire (A) mettant à sa charge une obligation spéciale de surveillance ; laquelle est motivée par la sauvegarde de l'intérêt général, complétée par l'obligation d'information de l'autorité compétente (B).

A : La demande de l'autorité judiciaire

Circonstancielle, la demande de l'autorité judiciaire semble d'abord une exception au principe légale d'exonération de la surveillance générale des informations stockées et à stocker par les hébergeurs. Car, si ces derniers, « *qui assurent, même à titre gratuit, par la mise à disposition au public des biens et services, le stockage* »³⁷⁷ de ces informations, ne sont pas soumis à une telle obligation, ils le sont moins dans le cadre d'une enquête judiciaire, allant même jusqu'à se voir imposés une surveillance ciblée et temporaire.

En effet, au Sénégal, en vertu de l'article 3-5, alinéa 2 de la loi sur les transactions électroniques, l'absence d'une obligation générale de surveillance est, à l'égard des hébergeurs, « *sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire* ». Cette prescription, dont l'application procède de l'article 8 du décret n° 2008-719 du 30 juin 2008, siège de « *l'obligation de contrôle spécifique* », indique qu'à la demande de l'autorité judiciaire, les hébergeurs ont l'obligation spéciale, sauf disposition contraire, de « *procéder à toute activité de surveillance ciblée ou temporaire des informations qu'ils stockent, en vue de prévenir ou de faire cesser un dommage occasionné par le contenu d'un service de communication par voie électronique.* »

En France aussi, l'exonération de la surveillance générale des contenus est prescrite au bénéfice des hébergeurs dans les mêmes conditions qu'au Sénégal, ainsi que l'obligation de « *surveillance ciblée et temporaire* »³⁷⁸ qui y revêt parfois le caractère d'une obligation de collaboration. En effet, dans le cadre d'une enquête cybercriminelle, à la demande des magistrats, des juges d'instruction ou des juges des libertés et de la détention, des cyberpatrouilles³⁷⁹ sont organisées conjointement par la police, la gendarmerie et la douane, en collaboration avec des hébergeurs pour obtenir des preuves d'activités illicites³⁸⁰.

Par ailleurs, par un arrêt du 12 juillet 2012, la Cour de cassation a cassé une décision de la cour d'appel de Paris condamnant *Google Inc.* et *Google France* à une « *surveillance illimitée* » des vidéos du

³⁷⁷ Article 3-2 de la loi sur les transactions électroniques.

³⁷⁸ Article 6-I-7 alinéa 2 de la LCEN.

³⁷⁹ T-B. Anmonka Jeanine-Armelle, « *La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'ouest* », thèse, Université de Paris Descartes, 2015, pp. 288-291 : « *La cyberpatrouille consiste dans la surveillance de sites ciblés, la filature virtuelle sur Internet, pendant un temps bien défini en fonction de la gravité et de la sensibilité des infractions* ».

³⁸⁰ *Ibidem*.

film intitulé « *L'affaire Clearstream* ». La Cour de cassation a estimé « *que si l'autorité judiciaire peut mettre à la charge d'un hébergeur une activité de surveillance, c'est à la condition que cette surveillance soit temporaire* »³⁸¹

Certes, la demande à adresser par l'autorité judiciaire aux hébergeurs, personnes physiques ou morales, concerne la mise en œuvre d'une obligation de surveillance ciblée et temporaire, mais elle trouve son efficacité dans la sauvegarde de l'intérêt général et l'impératif, pour ceux-ci, de porter un certain nombre d'informations à la connaissance de toute autorité compétente.

B : La sauvegarde de l'intérêt général et l'information de l'autorité compétente

La sauvegarde de l'intérêt général occupe une place non négligeable parmi les objectifs poursuivis par le législateur à travers la consécration d'un régime dérogatoire de responsabilité aux hébergeurs. Cette sauvegarde passe, entre autres, par le fait de coopérer avec les autorités compétentes en termes de mise à leur disposition de certaines informations.

Le législateur sénégalais a ainsi prévu que la sauvegarde de l'intérêt général attaché à la répression de certains infractions voire de leur simple apologie³⁸², devrait amener les hébergeurs à concourir à la lutte engagée contre elles. Pour ce faire, ils sont tenus de « *mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance* »³⁸³ la présence de contenus illicites sur leurs plateformes ou sur les sites qu'ils hébergent. A ce propos, en France, par une ordonnance de référé du 13 avril 2016, le TGI de Paris a ordonné à l'hébergeur nommé « *Association Egalite et Réconciliation* » de se conformer « *dans un délai d'un mois, au nom de l'intérêt général* »³⁸⁴, aux dispositions de l'article 6-I-7 alinéas 3 et 4 de la LCEN qui détaillent les infractions susmentionnées, comme l'article 3-5 alinéas 3 et 4 de la loi sur les transactions électroniques.

En plus de la sauvegarde de l'intérêt général, les hébergeurs ont « *l'obligation d'informer promptement les autorités publiques compétentes de toutes activités illicites...qui leur sont signalées et qu'exercent les destinataires de leurs services, et de rendre public les moyens qu'elles consacrent à la lutte contre ces activités illicites.* »³⁸⁵ Au Sénégal, l'article 9 du décret n° 2008-719 du 30 juin 2008³⁸⁶ prévoit que l'information à l'attention des autorités compétentes se fasse « *directement ou indirectement* » une fois que les hébergeurs ont une connaissance de « *l'existence d'un contenu en ligne manifestement illicite* »,

³⁸¹ Cass. Civ 1^{ère} Ch., 12 juillet 2012, pourvoi n° 11-13.669, *Sté Google France et Sté Google Inc. c/ Sté Bac films* ; voir sur www.courdecassation.fr, site visité le 3 octobre 2016.

³⁸² Article 3-5, al. 3 de la loi sur les transactions électroniques.

³⁸³ *Idem*, al. 4.

³⁸⁴ TGI de Paris, Ord. Réf., 13 avril 2016, *UEJF et AIPJ / Egalite et Réconciliation*, voir sur www.legalis.net, site visité le 3 octobre 2016.

³⁸⁵ Article 3-5, al. 3 et 4 de la loi sur les transactions électroniques.

³⁸⁶ Il s'agit du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

non sans « agir promptement pour retirer ces contenus ou pour en rendre l'accès impossible ». L'obligation d'information à la charge des hébergeurs s'étend au fait de communiquer à l'autorité judiciaire des informations classées comme secret professionnel, car en vertu de l'article 5, point 2, alinéa 3 de la loi sur les transactions électroniques, ce secret n'est pas opposable à cette autorité.

A l'opposé, l'alinéa 2 du même point fait obligation aux hébergeurs, du respect de « l'obligation de secret professionnel pour tout ce qui concerne la divulgation des éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée » par les points 1 (les éditeurs professionnels) et 2, alinéa 1^{er} (les éditeurs non professionnels) de l'article 5 ci-mentionné, sous réserve d'une part des conditions prévues par l'article 363³⁸⁷ du Code pénal, d'autre part de la « révélation des éléments d'identification personnelle par la personne concernée »³⁸⁸. S'ils manquaient à ces obligations, les hébergeurs personnes physiques ou dirigeants de droit ou de fait d'une personne morale, seraient punis en vertu de l'article 431-46 de la loi sur la cybercriminalité, « d'un d'emprisonnement de six mois à un an et d'une amende de 200 000 francs à 2 000 000 francs ou de l'une de ces deux peines seulement. »

En droit français, abstraction faite des sanctions prévues, ce sont les mêmes conditions de mise en œuvre de l'obligation de sauvegarde de l'intérêt général, de celles d'information et de respect du secret professionnel, qui sont prescrites par le législateur aux termes de l'article 6-I-7 et 6-III-2 de la LCEN.

Faudrait-il le retenir, le bénéfice de l'exonération de l'obligation générale de surveillance, accordé aux hébergeurs dans le cadre du strict exercice de leur fonction, est couplé par le législateur à celui de l'exonération de l'obligation générale de recherche.

³⁸⁷ Article 363 du Code pénal : « Le secret professionnel n'est jamais opposable au juge qui, pour les nécessités des investigations qu'il accomplit ou ordonne, peut en délier ceux qui y sont astreints... »

³⁸⁸ Article 17, *Op. cit.* 386.

Section 2 : L'exonération de l'obligation générale de recherche

Légalement consacrée, l'exonération de l'obligation générale de recherche est mise en œuvre à des niveaux (Paragraphe 1^{er}) bien déterminés. Mais l'hébergeur qui en bénéficie devra se plier aussi à une obligation particulière de recherche et de moyens (Paragraphe 2).

Paragraphe 1^{er} : Les niveaux de mise en œuvre de l'exonération

L'exonération de l'obligation générale de recherche, accordée par le législateur à l'hébergeur, se réalise à deux niveaux : l'absence de recherche des faits révélateurs des activités illicites (A) et celle de recherche des circonstances révélatrices desdites activités (B).

A : L'absence de recherche des faits révélateurs des activités illicites

Un fait consiste en tout événement susceptible de produire des effets de droit et d'avoir des conséquences juridiques³⁸⁹. En droit sénégalais, le législateur³⁹⁰, à l'instar de son homologue français³⁹¹, a prescrit au bénéfice de l'hébergeur l'exonération de toute obligation générale de recherche si cette recherche devait concerner les faits indiquant des activités illicites sur les sites dont il stocke les contenus.

Aux termes de son article 15, la directive sur le commerce électronique³⁹² a plutôt fait une interdiction pour les États membres d'imposer aux hébergeurs « *une obligation générale de rechercher activement des faits révélant des activités illicites* ». Dans son premier rapport³⁹³ sur l'application de cette directive, la « *Commission au parlement européen, au conseil et au comité économique et social européen* » a retenu qu'imposer la recherche tous azimuts, sur Internet, des faits révélateurs des activités illicites équivaldrait, en pratique, à faire faire aux prestataires intermédiaires, en l'espèce les hébergeurs, « *une recherche impossible qui déboucherait sur une charge disproportionnée* » pour eux. Ce qui, toutefois, n'empêche pas les autorités publiques des États membres d'imposer une telle obligation « *dans un cas spécifique clairement défini* ».

En d'autres termes, comme pour l'obligation générale de surveillance qu'il s'abstiendrait d'ordonner aux fournisseurs d'hébergement, un juge ne devrait pas non plus enjoindre à ces derniers de procéder à une recherche générale, systématique et intemporelle desdits faits.

³⁸⁹ Définition de Larousse.fr, sur <http://www.larousse.fr/dictionnaires/francais/fait/32729>, site visité le 4 octobre 2016.

³⁹⁰ Cf. article 3-5, al. 1^{er} de la loi sur les transactions électroniques.

³⁹¹ Cf. article 6-I-7, al. 1^{er} de la LCEN

³⁹² Dir. Cons. CE n° 2000/31, 8 juin 2000, JOCE 17 juillet 2000, n° L 178, pp. 1-16.

³⁹³ Cf. « *Premier rapport sur l'application 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")* », Bruxelles, 21 novembre 2003, p. 15.

C'est ainsi que, par un arrêt rendu dans ce sens le 16 février 2012³⁹⁴, la Cour de Justice des l'Union Européenne (CJUE) a considéré que l'injonction faite par un juge à l'hébergeur « *Sabam* », était « *contraire* » aux dispositions prévues par la directive susmentionnée, notamment à son article 15.

A côté des faits révélant des activités illicites et que l'hébergeur devra s'abstenir de rechercher conformément à l'exonération légale dont il bénéficie, l'on constate que la même dérogation lui est accordée quant aux circonstances révélatrices desdites activités.

B : L'absence de recherche des circonstances révélatrices des activités illicites

Faits particuliers qui entourent et accompagnent un événement, les circonstances constituent surtout un élément secondaire d'une situation donnée³⁹⁵.

En droit sénégalais, même si elles doivent permettre la découverte d'activités illicites développées sur Internet par les utilisateurs des services offerts par les hébergeurs, ces circonstances ne sauraient faire l'objet d'une obligation générale de recherche à la charge de ces derniers. Ce sont ainsi des prescriptions du législateur³⁹⁶, inspirées de celles de son homologue français³⁹⁷ et qui prévoient que les hébergeurs « *ne sont pas soumis à une obligation générale de rechercher des circonstances révélant des activités illicites.* »

En droit communautaire européen, c'est encore l'article 15 de la directive sur le commerce électronique qui fait interdiction aux Etats membres d'imposer cette obligation aux hébergeurs. En conséquence, la restriction faite au juge et consistant à ne pas enjoindre le respect d'une telle obligation, *a priori* réputée inexistante à l'égard de l'hébergeur, est appliquée par différentes juridictions. En effet, par un arrêt du 4 avril 2013³⁹⁸, la cour d'appel de Paris a confirmé une ordonnance entreprise par le TGI de Paris faisant application de l'article 6-I-7 de la LCEN en considérant que « *la société JFG Networks, en tant qu'hébergeur, n'était pas soumise à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* » ; encore qu'il y avait « *absence de trouble manifestement illicite caractérisé par les propos de l'article incriminé, et donc de contenu manifestement illicite* ».

Toutefois, rien n'empêche un hébergeur d'effectuer de manière volontaire, sur sa propre initiative, des contrôles et des recherches sur les sites qu'il héberge³⁹⁹. L'avantage est que cette intervention peut lui permettre d'asseoir sa crédibilité et son image de marque.

³⁹⁴ CJUE, 3^{ème} Ch., 16 février 2012, *Sabam c/ Netlog*, Affaire n° C-360/10, <http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=FR>, site visité le 4 octobre 2016.

³⁹⁵ Définition de Larousse.fr, sur <http://www.larousse.fr/dictionnaires/francais/circonstance/16137>, site visité le 4 octobre 2016.

³⁹⁶ Cf. article 3-5, al. 1^{er} de la loi sur les transactions électroniques.

³⁹⁷ Cf. article 6-I-7, al. 1^{er} de la LCEN.

³⁹⁸ CA de Paris, Pôle 1, 2^{ème} Ch., 04 avril 2013, *Rose B. / JFG Networks*, sur www.legalis.net, site visité le 4 octobre 2016.

³⁹⁹ *Op. cit.* note 157 ; voir aussi V. Christophe, « *Les hébergeurs de sites web : victimes ou régulateurs de la société de l'information ?* », revue DCCR (Droit de la consommation – Consumentenrecht), n° 68, Doctrine, éd. Larcier, 2005, p. 41

En ce sens, par une ordonnance de référé en date du 4 décembre 2015⁴⁰⁰, le TGI de Paris, qui a condamné l'hébergeur *LBC France* - et éditeur en même temps du site *leboncoin.fr* - pour « *pratique commerciale trompeuse, à la publication d'un article, à ses frais, et dans trois journaux ou magazines différents choisis par la société Goyard St-Honoré* », a cependant considéré que « *la recherche de circonstances permettant de constater des activités illicites que LBC avait entreprise en installant un logiciel pointant dans les annonces faites par les destinataires de ses services, les textes allant à l'encontre des bonnes mœurs et de la préservation des droits des tiers, n'induit en rien un rôle éditorial et n'est pas exclusif de la qualification d'hébergeur de la société LBC* ».

Dès lors, l'exonération accordée à l'hébergeur quant à l'obligation générale de recherche semble respectée voire protégée dans sa mise en œuvre ; laquelle, encadrée, ne laisse pas moins une brèche ouverte où peut s'engouffrer ce prestataire technique toutes les fois qu'il le désire. Cette suite d'opportunités est, toutefois, atténuée par le choix du législateur de consacrer, à la charge de ce dernier, une obligation particulière de recherche et de moyens.

Paragraphe 2 : La consécration d'une obligation particulière de recherche et de moyens

En consacrant une obligation particulière de recherche à la charge des hébergeurs, le législateur a prescrit des mécanismes pour sa mise en œuvre (A), non sans prévoir dans le même temps une obligation particulière de moyens (B) qu'il leur a aussi imposée.

A : Les mécanismes de mise en œuvre de l'obligation particulière de recherche

La mise en œuvre de l'obligation particulière de recherche faite aux hébergeurs passe par un certain nombre de mécanismes judiciaires et administratifs.

Les mécanismes judiciaires sont notamment prévus, en droit sénégalais, à l'article 3-6 de la loi sur les transactions électroniques, et presque mot pour mot en droit français, à l'article 6-I-8 de la LCEN. Ainsi, le juge compétent peut-il prescrire, « *en référé ou sur requête* » d'abord à tout hébergeur personne physique ou morale, exerçant sa fonction à titre professionnel ou à titre gratuit, ou, à défaut, à tout fournisseur d'accès, « *toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». *A priori*, l'expression « *toute mesure* » peut faire penser à toutes sortes de mesures à la portée de l'hébergeur. Cela semble certes envisageable, mais le cas échéant il renverrait à l'obligation générale de recherche. Or celle-ci fait déjà

⁴⁰⁰ TGI de Paris, 3^{ème} Ch., 2^{ème} Section, jugement du 4 décembre 2015, *Goyard St-Honoré / LBC France*, sur www.legalis.net, site visité le 5 octobre 2015.

l'objet d'une exonération légale⁴⁰¹ et son injonction est interdite⁴⁰² y compris au juge⁴⁰³. Si bien que les procédures spéciales prévues par le législateur aux termes des articles évoqués ci-dessus ne peuvent que concerner la recherche particulière des contenus illicites, au cas par cas, en vue de prévenir ou de faire cesser les dommages que ces derniers peuvent occasionner. A titre illustratif, en France, il s'agit du référé et de la requête dits « *LCEN* », mais aussi du référé dit « *ARJEL* ».

Dans les premiers cas, vu l'urgence ou les conditions particulières au moment des faits, ponctuées par une violation à laquelle il faut mettre fin ou qu'il faut immédiatement prévenir, le juge des requêtes ou le juge des référés met en œuvre le principe de subsidiarité, prévu par l'article 6-I-8 de la LCEN, en ordonnant à l'hébergeur sinon de les retirer de ses serveurs, du moins de bloquer l'accès aux contenus illicites en cause. Cependant, si l'hébergeur est introuvable ou qu'il refuse de collaborer, comme c'est le cas dans l'« *affaire Les Editions Gallimard* »⁴⁰⁴ (où l'hébergeur, la société « *Iweb* » basée au Canada, avait ignoré l'ordonnance sur requête du juge français), le juge peut alors s'adresser aux différents fournisseurs d'accès chez qui les contenus litigieux s'affichent, afin qu'ils bloquent leur accès à partir du territoire français.

Dans le second cas, plutôt réservé aux jeux de hasard et d'argent en ligne, et prévu par l'article 61 de la loi n° 2010-476 du 12 mai 2010⁴⁰⁵, après une mise en demeure infructueuse envoyée à un opérateur de jeux ou de paris en ligne illégaux, le président de l'ARJEL saisit le président du TGI de Paris d'une part, aux fins d'ordonner à son hébergeur, en la forme des référés, à rechercher et arrêter l'accès aux services proposés par l'opérateur insoumis, à défaut, à son fournisseur d'accès, d'autre part, aux fins de voir prescrire, en la forme des référés, toute mesure destinée à faire cesser le référencement du site de l'opérateur.

En ce qui concerne les mécanismes administratifs, en droit français, ils concernent principalement la possibilité pour l'administration de faire directement injonction aux hébergeurs de rechercher et bloquer des sites considérés comme « *incitant à la commission d'actes de terrorisme ou en faisant l'apologie et [des] sites diffusant des images et représentations de mineurs à caractère pornographique* »⁴⁰⁶ pour prévenir ou faire cesser des dommages occasionnés par leurs contenus réputés illicites. Cela s'entend

⁴⁰¹ Cf. articles 3-5, al. 1^{er} de la loi sur les transactions électroniques et 6-I-7, al. 1^{er} de la LCEN

⁴⁰² Cf. article 6-I-7, al. 1^{er} de la LCEN.

⁴⁰³ CA de Paris, Pôle 1, 2^{ème} Ch., 04 avril 2013, *Rose B. / JFG Networks*, sur www.legalis.net, site visité le 4 octobre 2016.

⁴⁰⁴ TGI de Paris, Ord. Réf., 28 juin 2011, *Numéricable, SFR et autres / Les Editions Gallimard*; cette ordonnance de référé qui retrace tous les faits, a rétracté l'ordonnance sur requête, en date du 10 juin 2011, ayant donné raison aux Editions demanderesse et fait bloquer l'ensemble des contenus litigieux, simplement pour vice de procédure, notamment pour violation des articles 493 et 812 du Code de procédure civile de France, voir sur www.legalis.net, site visité le 1^{er} octobre 2016.

⁴⁰⁵ Il s'agit de la 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, JORF n° 0110 du 13 mai 2010, voir aussi sur www.legifrance.gouv.fr, site visité le 25 août 2016.

⁴⁰⁶ Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. JORF n°0031 du 6 février 2015 page 1811, texte n° 71/162, sur www.legifrance.gouv.fr.

en application des dispositions de l'article 12 de la loi n° 2014-1353 du 13 novembre 2014⁴⁰⁷, qui insère l'article 6-1 dans la LCEN, et de son décret d'application n° 2015-125 du 5 février 2015⁴⁰⁸.

Ces dispositions permettent ainsi à l'Office central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) qui dépend de la Direction centrale de la police judiciaire, de réclamer⁴⁰⁹ aux hébergeurs de sites qualifiés de sensibles la recherche, la vérification et le retrait des contenus illicites, sans demander l'autorisation d'un juge ; ceci, « 24 heures »⁴¹⁰ après celles, parmi les quelque 3500⁴¹¹ notifications faites par semaine, restées sans suite escomptée et qui le sont par les internautes *via* la plateforme officielle de signalement dite « PHAROS⁴¹² ». Et si l'hébergeur ignore l'injonction, ce sera aux fournisseurs d'accès de recevoir de cette autorité administrative la même injonction. Dans le même temps, le ministère de l'intérieur transmet la liste des adresses électroniques des « sites méconnaissant les dispositions des articles 227-23 et 421-2-5 du code pénal »⁴¹³ aux fournisseurs d'accès à Internet afin qu'ils procèdent, dans les vingt-quatre heures, au blocage desdits sites.

A côté de l'obligation particulière de recherche imposée aux hébergeurs par le législateur, qui a aussi autorisé une autorité administrative à faire bloquer des sites Internet sans que le juge judiciaire en ait été informé, l'on peut analyser l'obligation particulière de moyens.

B : L'obligation particulière de moyens

Les obligations de moyens imposées aux prestataires techniques sont nombreuses. Si toutes s'appliquent directement ou indirectement⁴¹⁴ aux fournisseurs d'accès à Internet, il y en a dont les hébergeurs sont déchargés. C'est le cas, en droit sénégalais, des obligations prévues à l'article 677-38⁴¹⁵ de la loi sur la cybercriminalité, à l'article 3-1 de la loi sur les transactions électroniques et aux articles 3 et 5 du décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

⁴⁰⁷ Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. JORF n° 0263 du 14 novembre 2014, voir aussi sur www.legifrance.gouv.fr, site visité le 16 septembre 2016.

⁴⁰⁸ *Op. cit.* note 406.

⁴⁰⁹ Article 5, al. 2, *idem*

⁴¹⁰ Article 3, *idem*.

⁴¹¹ Source : Nextinpact.com, voir sur <http://www.nextinpact.com/news/100300-dans-coulisses-plateforme-signalement-pharos.htm>, site visité le 5 octobre 2016.

⁴¹² "PHAROS" : Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements. Pour plus de détails, voir le « Site officiel de signalement des contenus illicites sur Internet », à savoir « Internet-signalement.gouv.fr » dont l'URL est <https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>, site visité le 5 octobre 2016.

⁴¹³ Cf. Objet du décret n° 2015-125 du 5 février 2015. *Op. cit.* note 406.

⁴¹⁴ Indirectement, en référence au principe de subsidiarité et à la responsabilité en cascade prévus, par exemple, aux articles 3 et 5 de la loi sur les transactions électroniques.

⁴¹⁵ Article 677-38 de la loi portant sur la cybercriminalité : « Si les nécessités de l'information l'exigent, le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel. »

Cette dernière obligation impose, par exemple, aux fournisseurs d'accès à Internet de mettre gratuitement à la disposition des utilisateurs, des moyens techniques appropriés, efficaces, accessibles et aptes à faire identifier les erreurs commises par les utilisateurs dans la saisie des données et les corriger le cas échéant, à rendre plus sûre la navigation des mineurs sur Internet en restreignant leurs accès, tout en facilitant par ailleurs l'accès à un outil de contrôle parental à jour⁴¹⁶.

Examinées à l'aune de ces éléments de comparaison, les obligations de moyens incombant aux hébergeurs seraient, par conséquent, particulières. Elles sont de plusieurs ordres. En effet, sous l'empire de l'article 4 de la loi sur les transactions électroniques, les hébergeurs ont l'obligation de détenir et de conserver les données⁴¹⁷ de nature à « *permettre l'identification de quiconque a contribué à la création des contenus* » des services dont ils sont prestataires.

Mieux, l'article 11 du décret mentionné ci-dessus impose aux hébergeurs de mettre les autorités judiciaires, à leur demande, dans les conditions « *d'obtenir les données de nature à permettre l'identification de l'auteur d'un contenu qu'ils hébergent* ». S'ils ne le faisaient pas, ils engageraient alors leur responsabilité au titre de l'article 677-44 de la loi sur la cybercriminalité. Cette article prévoit à l'encontre de tout hébergeur, « *personne physique ou dirigeant de droit ou de fait d'une personne morale qui n'aura pas conservé les éléments d'information* » évoqués ci-devant, ni n'aura déféré à la demande d'une autorité judiciaire d'obtenir communication desdits éléments, « *un emprisonnement de six mois à un an et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement.* » Autant dire que le législateur sénégalais attache du prix au respect de cette obligation par l'hébergeur.

Prévue en droit français à l'article 6-II de la LCEN, la mise en œuvre de cette obligation donne la possibilité à l'autorité compétente d'entrer en possession d'éléments pouvant, le cas échéant, faciliter la traçabilité de personnes déterminées et de faire avancer, par exemple, une enquête judiciaire dans le sens de la manifestation de la vérité. Cela est d'autant plus probable que l'article 677-35 de la loi sur la cybercriminalité prévoit que si les nécessités de l'information l'exigent, le juge d'instruction peut faire injonction à toute personne, en l'espèce à l'hébergeur, « *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* ».

L'obligation particulière de moyens, à laquelle est assujetti l'hébergeur, profite également aux éditeurs⁴¹⁸ auxquels il doit « *fournir des moyens techniques* » appropriés leur permettant, eux aussi, de

⁴¹⁶ Cf. *supra* : 1^{ère} Partie, Section 1^{ère}, Paragraphe 2, (B) : Les obligations de moyens et d'information.

⁴¹⁷ Pour les caractéristiques de ces données, cf. Article 3-4 de la loi sur les transactions électroniques, article 6-II de la LCEN et article 1^{er} du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, J.O.R.F. n° 0050 du 1 mars 2011, texte 32 sur 170.

⁴¹⁸ Cf. *supra*, 1^{ère} Partie, Chapitre 2, Section 1^{ère}, Paragraphe 2, (A) : Les obligations au profit des éditeurs, des autorités et des tiers.

converser l'ensemble des données d'identification les concernant, comme cela est prévu à l'article 5 de la loi sur les transactions électroniques et à l'article 6-III de la LCEN.

Toutefois, la mise à disposition par les hébergeurs, des données détenues et conservées, n'a pas suffi au législateur sénégalais qui a prévu, en vertu de l'article 14 du décret susmentionné, qu'au-delà de cela, les autorités compétentes, notamment judiciaires, pussent elles-mêmes s'introduire facilement, directement et en permanence dans leurs bases de données pour chercher les informations dont elles auraient besoin, certainement dans le cadre d'une perquisition informatique, y compris pour traquer les cyber-malfaiteurs sous le couvert de l'anonymat⁴¹⁹. Les autorités judiciaires sont d'autant plus fondées à le faire que les articles 677-36 et 677-37 de la loi sur la cybercriminalité les y autorisent. C'est ainsi que « *lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire sénégalais, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.* »⁴²⁰

Cette même possibilité est offerte aux autorités judiciaires françaises, en vertu de l'obligation particulière de moyens fait aux hébergeurs, notamment sur lesquels elles jouissent d'une compétence territoriale, de procéder à des perquisitions informatiques dans les données de connexions de cyber-malfaiteurs. Ainsi, grâce à ces moyens et cette méthode, le juge français a-t-il mis en œuvre, pour la première fois, le 8 août 2016, les dispositions de la loi n° 2016-731 du 3 juin 2016 dite « *loi Urvoas* »⁴²¹ en particulier celles de son l'article 18, codifiées respectivement aux articles 421-2-5-2⁴²² et 421-2 5-1⁴²³ du Code pénal, en condamnant un homme de 31 ans à la peine maximale prévue en l'espèce, à savoir « *2 ans d'emprisonnement et 30 000 euros d'amende* » pour avoir « *consulter habituellement* »⁴²⁴ des sites Internet considérés comme incitant « *directement à la commission d'actes de terrorisme, [ou] faisant l'apologie de ces actes* ».

⁴¹⁹ *Op. cit.* note 379.

⁴²⁰ Article 677-36, al. 1^{er} de la loi portant sur la cybercriminalité.

⁴²¹ Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n° 0129 du 4 juin 2016, texte 1 / 119, voir sur www.legifrance.gouv.fr, site visité le 18 octobre 2016.

⁴²² Article 421-2-5-1 : « *le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures prévues à l'article 6-1 de la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'article 706-23 du code de procédure pénale est puni de cinq ans d'emprisonnement et de 75000 € d'amende.* »

⁴²³ Article 421-2-5-2 : « *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30000 € d'amende. Le présent article n'est pas applicable lorsque la consultation est effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice.* »

⁴²⁴ TGI de Chartres, jugement du 8 août 2016. Inédit. Source : www.droit-technologie.org, ou suivre le lien <http://www.droit-technologie.org/actuality-1821/consultation-de-sites-djihadistes-premiere-condamnation-exemplaire-e.html>, site visité le 27 septembre 2016.

CONCLUSION

Récente et surtout en construction, la responsabilité des prestataires techniques, à savoir les fournisseurs d'accès à Internet et les hébergeurs, est de ce fait, sujette à plusieurs interprétations sous-tendues, d'une part par le caractère protéiforme des concepts qui entrent dans leur définition et celle de l'ensemble des acteurs de la communication au public en ligne, d'autre part par la rapidité et la diversité qui caractérisent le développement des technologies de l'information et de la communication.

Moins d'un quart de siècle après l'entrée en vigueur, au Sénégal comme en France, du dispositif de mise en œuvre de la responsabilité de ces prestataires techniques, il serait trop tôt voire prétentieux de parler de bilan y compris à mi-chemin. Une chose est sûre en revanche, pendant ces années, les juges ont dit le droit ; parfois difficilement à cause de la finesse qui frise l'inexistence de frontières objectives entre l'étendue de l'exonération encadrée de la responsabilité à laquelle ces prestataires techniques sont soumis et le droit commun qui revêt, dans ce cas précis, un caractère exceptionnel.

Pendant ce temps, explosent les transactions électroniques en particulier et, en général, l'économie numérique, modifiant les équilibres en matière de commission de fautes pour en avoir créé de nouvelles tout en dématérialisant certaines parmi celles connues jusque-là.

Mais le législateur suit tant bien que mal ces fulgurants changements non sans avoir en ligne de mire l'immatérialité de certaines fautes voire, en matière répressive, de certaines infractions. La consécration de la perquisition informatique et du fait de rendre un nombre inestimable d'informations indisponibles, comme prévu en droit sénégalais par exemple par les articles 677-36 et 677-37 de la loi portant sur la cybercriminalité, ceci sans déplacement physique d'un point A à un point B, y compris à l'international, est entre autres une preuve de la détermination du législateur de relever les défis auxquels il a fait face toutes ces années-là.

Pour ce faire, le législateur a mis en adéquation et même concilié l'aménagement de la responsabilité des prestataires techniques, acteurs incontournables d'Internet, avec l'intangibilité des procédures judiciaires mises en œuvre au nom de l'intérêt général et de l'ordre public et dont l'autorité éponyme est dépositaire du « *pouvoir discrétionnaire* »⁴²⁵, à côté de celles administratives réservées à des autorités qualifiées et généralement désignées à l'instar de la CDP au Sénégal et de l'OCLCTIC en France, entre autres.

Au fait, parmi les instruments majeurs choisis par le législateur pour mieux contrecarrer les effets démultiplicateurs d'Internet et, le cas échéant, dommageables des contenus illicites, il convient de retenir non seulement les procédures en référé ou sur requête qui sont des procédures d'urgence dont la célérité est

⁴²⁵ Selon le "JURIDICTIONNAIRE", actualisé au 13 juillet 2015, page 289, « le juge est investi du pouvoir discrétionnaire d'écartier les obstacles qui causeraient un retard dans le déroulement de la procédure. Ses prérogatives discrétionnaires sont des compétences ou des attributs qui se rattachent à des pouvoirs de décision. »

sans conteste apte à faire face à toutes sortes d'agissements litigieux, mais également l'inopposabilité du secret professionnel à l'autorité judiciaire.

Cependant, en pratique, le caractère transnational d'Internet et la liberté des éditeurs et fournisseurs de contenus de faire héberger leurs sites et stocker leurs données par des prestataires techniques de n'importe quel pays, notamment des Etats-Unis d'Amérique, mais aussi la profusion des réseaux sociaux et des plateformes d'hébergement de vidéos dont la majorité est de droits étrangers - *Google, Facebook, Twitter, Youtube, Telegram, WhatsApp, Instagram*, etc. - rendent presque toujours difficile voire impossible l'application correcte des dispositions nationales sénégalaises et françaises.

Il en résulte que les dommages occasionnés par les contenus illicites hébergés par ces prestataires techniques étrangers sont difficiles à faire cesser ou à prévenir. Les autorités compétentes se rabattent sur les fournisseurs d'accès à Internet exerçant leurs activités dans les limites de leurs frontières nationales pour, par exemple, faire bloquer l'accès auxdits contenus ; mais cela ne permet ni le retrait de ces derniers des serveurs en cause, ni la cessation des dommages occasionnés, sous d'autres cieux.

Si bien que seules les conventions judiciaires en vigueur, en état de fonctionner correctement et qui, *a priori*, n'entravent en rien la liberté d'expression telle qu'appréhendée par les législateurs des pays étrangers signataires, pourraient aider à prévenir ou à faire cesser les dommages en question.

Ces conventions sont notamment visées à l'article 113-12 du code pénal français qui dispose que « *la loi pénale française est applicable aux infractions commises au-delà de la mer territoriale, dès lors que les conventions internationales et la loi le prévoient* » et, en filigrane à l'article 677-36 alinéa 2 de la loi portant sur la cybercriminalité, et donc du code pénal sénégalais, selon lequel si les données « *sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur* ».

A ces difficultés, s'ajoutent l'apparition des "*applications mobiles*" se comptant par millions et qui supplantent systématiquement les logiciels traditionnels et la problématique du "*Web profond*" qu'aucune convention internationale d'entraide judiciaire ne contrôle. D'où la nécessité, en tout cas pour le Sénégal, d'évaluer régulièrement la pratique des dispositions en vigueur, aboutissant à la production de nouvelles, plutôt adaptées aux différentes mutations d'Internet.

L'allègement et la simplification de la notification des contenus illicites, qui est déjà suffisamment encadrée par la loi sur les transactions électroniques et la LCEN, et dont l'abus et le dévoiement sont pénalisés, semblent aussi s'imposer au sens où les technologies de l'information et de la communication

existantes actuellement sont dotées d'une intelligence artificielle suffisante pour constater la véracité d'un signalement.

En ce qui nous concerne, cet exercice portant sur « *la responsabilité des prestataires techniques* » aura été une réflexion tournée vers l'avenir en ce sens qu'Internet n'a pas fini de révéler ses secrets, loin s'en faut, mais il traînera forcément les imperfections du travail d'un étudiant de Master 2.

Ce mémoire ne saurait en effet égaler la réflexion, sur le même sujet, d'un professionnel ni d'un spécialiste d'Internet encore moins celui d'un professeur d'Université, qui plus est, de droit.

Ebauche, l'espérons-nous, d'une éventuelle prochaine réflexion d'étudiants comme nous, à coup sûr plus pointue et mieux structurée, elle ne prétend nullement avoir fait le tour de la question tant celle-ci est vaste, instable et évolutive. D'ailleurs, la rapidité avec laquelle Internet évolue ne cautionnerait pas qu'un mémoire d'étudiant rédigé en 2016, pût tenir tête à ses nombreuses mutations et surtout à sa longévité.

ANNEXES

TITRE PREMIER. - LIBERTE DE COMMUNICATION PAR VOIE ELECTRONIQUE.

Chapitre premier. - Communication au public par voie électronique.

Chapitre II. - Prestataires techniques de services au public utilisant les technologies de l'Internet.

Art. 3. - 1) Les personnes dont l'activité est d'offrir un accès à des services au public par le biais des technologies de l'information et de la communication sont tenues de mentionner dans les contrats de leurs abonnés l'existence de moyens techniques permettant de restreindre l'accès à certains services ou au moins de les sélectionner. Les moyens techniques, dépendant de la nature de la prestation, sont précisés par décret.

2) Les personnes physiques ou morales qui assurent, même à titre gratuit, par la mise à disposition au public des biens et services, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou 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.

L'alinéa précédent du présent article ne s'applique pas lorsque de destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

3) Les personnes visées au point 2 du présent article ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicite ou si, dès le moment où elle en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

4) La connaissance des faits litigieux est présumée acquise par les personnes désignées au point 2 du présent article lorsqu'il leur est notifié les éléments suivants :

- a) la date de la notification des faits litigieux ;
- b) si le notifiant est une personne physique : nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ;
- c) si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;
- d) le nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
- e) la description des faits illicites et leur localisation précise ;
- f) les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
- g) la copie de la correspondance adressée à l'auteur ou 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.

5) Les personnes visées aux points 1 et 2 du présent article ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.

Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie infantile, les personnes mentionnées ci-dessus doivent concourir à la lutte contre de tels agissements.

A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur sont signalées et qu'exercent les destinataires de leurs services, et, d'autre part, de rendre public les moyens qu'elles consacrent à la lutte contre ces activités illicites.

Tout manquement aux obligations définies à l'alinéa précédent est puni en vertu des dispositions légales en vigueur.

6) Le juge compétent peut prescrire, en référé ou sur requête, à toute personne mentionnée au point 2 du présent article ou, à défaut, à toute personne mentionnée au point 1 du présent article, toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication public en ligne.

Art. 4. - Les personnes mentionnées aux points 1 et 2 de l'article 3 de la présente loi détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires

Les personnes mentionnées aux points 1 et 2 de l'article 3 de la présente loi fournissent aux personnes qui éditent un service de communication ou public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 5 de la présente loi.

L'autorité judiciaire peut requérir la communication auprès des prestataires mentionnés aux points 1 et 2 de l'article 3 de la présente loi, des données mentionnées au premier article.

Le traitement de ces données est soumis aux dispositions de la loi sur la protection des données à caractère personnel.

Un décret, pris après avis de la Commission des Données Personnelles définit les données mentionnées au premier alinéa du présent article et détermine la durée et les modalités de leur conservation.

Art. 5. - 1) Les personnes dont l'activité est d'éditer un service de communication au public par le biais des technologies de l'Internet mettent à disposition du public, dans un stand ouvert :

a) s'il s'agit de personnes physiques, leur nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et du crédit mobilier, le numéro de leur inscription ;

b) s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier ou au répertoire national des entreprises et associations, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;

c) le nom du directeur ou du codirecteur de la publication du service de communication au public par voie électronique et, le cas échéant, celui du responsable de la rédaction ;

d) le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone du prestataire mentionné au point 2 de l'article 3 de la présente loi.

2) Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire, sous réserve de lui avoir communiqué des éléments d'identification personnelle prévus par la présente loi.

Les personnes mentionnées au point 2 de l'article 3 de la présente loi sont assujetties au secret professionnel dans les conditions prévues à l'article 363 du Code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée.

Ce secret professionnel n'est pas opposable à l'autorité judiciaire.

Art. 6.- Toute personne nommée ou désignée dans un service de communication au public utilisant les technologies de l'Internet dispose d'un droit de réponse, sans préjudice des demandes de notification ou d'opposition au message qu'elle peut adresser au service.

La demande d'exercice du droit de réponse est adressée au directeur de publication ou lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée au point 2 de l'article 3 de la présente loi qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois (3) mois à compter de la mise à disposition du public du message justifiant cette demande.

Un décret fixe les modalités d'application du présent article.

Art. 7. - Lorsque les personnes visées au point 1 de l'article 3 de la présente loi invoquent, à des fins publicitaires, la possibilité qu'elles offrent de télécharger des fichiers dont elles ne sont pas les fournisseurs, elles font figurer dans cette publicité une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique.

...

Fait à Dakar, le 25 janvier 2008.

Abdoulaye WADE.

Par le Président de la République :

Le Premier Ministre, Cheikh Hadjibou SOUMARE.

ANNEXES - 02

**Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.
J.O. n° 6439 du samedi 22 novembre 2008**

Le présent projet de décret est pris en application des dispositions de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

Les précisions apportées ont trait notamment aux conditions :

- 1) d'exercice et de responsabilité des prestataires techniques ;
- 2) d'exercice du droit de réponse dans un service de communication en ligne ;
- 3) de transmission électronique des documents ou des actes administratifs.

Telle est l'économie du présent projet de décret.

Le Président de la République,

Vu la Constitution, notamment en ses articles 43 et 76 ;

Vu la loi n° 90-07 du 28 juin 1990 relative à l'organisation et au contrôle des entreprises du secteur parapublic et au contrôle des personnes morales de droit privé bénéficiant du concours financier de la puissance publique ;

Vu la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques ;

Vu le décret n° 2004-1038 du 23 juillet 2004 fixant les règles d'organisation et de fonctionnement de l'Agence de l'Informatique de l'Etat (ADIE) ;

Vu le décret n° 2007-826 du 19 juin 2007 portant nomination du Premier Ministre ;

Vu le décret n° 2008-362 du 7 avril 2008 portant répartition des services de l'Etat et du contrôle des établissements publics, des sociétés nationales et des sociétés à participation publique entre la Présidence de la République, la Primature et les ministères ;

Sur le rapport du Premier Ministre,

Décrète :

Chapitre premier. - Dispositions générales.

Article premier. - Le présent décret a pour objet de fixer les conditions d'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, notamment celles relatives à la sécurité des transactions électroniques.

Art. 2. - Au sens du présent décret, on entend par :

- 1) Prestataires techniques de services utilisant les technologies de l'Internet : les personnes, physiques ou morales, mentionnées au point 1 de l'article 3 de la loi sur les transactions électroniques ;
- 2) Contenus manifestement illicites : des contenus d'une gravité avérée et dont le caractère illicite ne semble pas discutable, notamment les contenus à caractère pornographique ou faisant l'apologie des crimes de guerre ou portant manifestement atteinte à l'ordre public ou aux bonnes mœurs.

Chapitre II. - Mesures techniques :

Art. 3. - En application du point 1 de l'article 3 de la loi sur les transactions électroniques, les moyens techniques doivent être appropriés, efficaces et accessibles en vue, notamment :

- 1) d'identifier les erreurs commises dans la saisie des données et de les corriger le cas échéant ;
- 2) de rendre plus sûre la navigation des mineurs sur les nouvelles technologies en restreignant les accès à l'Internet selon le profil de l'utilisateur connecté ;
- 3) de faciliter l'accès à un outil de contrôle parental à jour, performant et sans surcoût pour l'utilisateur ;
- 4) de proposer des mesures techniques de filtrage.

Art. 4. - Les prestataires techniques mentionnés au point 1 de l'article 2 du présent décret doivent, d'une part, assurer la mise à jour régulière de ces moyens techniques et, d'autre part, en informer les utilisateurs.

Chapitre III. - Responsabilités des prestataires techniques.

Art. 5. - Les utilisateurs peuvent engager la responsabilité des prestataires techniques lorsqu'aucune mesure technique prévue à l'article 3 du présent décret n'a pas été proposée.

Art. 6. - les prestataires techniques sont exonérés de leur responsabilité lorsqu'ils se contentent de faire du stockage automatique ou temporaire de l'information ou de jouer un rôle d'intermédiation dans la transmission de celle-ci à condition :

- 1) qu'ils ne sélectionnent pas le destinataire de la transmission ;
- 2) qu'ils ne soient pas à l'origine de la transmission ;
- 3) que les activités de transfert et de fourniture d'accès visent exclusivement à l'exécution de la transmission ou de la fourniture d'accès ;
- 4) qu'ils ne modifient pas les informations faisant l'objet de la transmission ;
- 5) qu'ils exécutent une décision d'une autorité judiciaire ou administrative visant le retrait de l'information ou l'interdiction de son accès.

Art. 7. - En application du point 4 de l'article 3 de la loi sur les transactions électroniques, en cas de notification par écrit ou par voie électronique, les prestataires techniques engagent leur responsabilité si elles laissent en ligne le contenu manifestement illicite.

L'abus de notification pour des faits non illicites est puni selon les dispositions de l'article 431-43 de la loi sur la cybercriminalité.

Chapitre IV. - Obligation de contrôle des prestataires techniques.

Art. 8. - Sauf disposition contraire, en application du point 5 de l'article 3 de la loi sur les transactions électroniques, les prestataires techniques sont tenues à une obligation de contrôle spécifique afin de détecter d'éventuelles infractions.

A ce titre, ils doivent procéder à toute activité, de surveillance ciblée ou temporaire des informations qu'ils transmettent ou stockent, demandée par l'autorité judiciaire, en vue de prévenir ou de faire cesser un dommage occasionné par le contenu d'un service de communication par voie électronique.

Art. 9. - Conformément aux dispositions prévues au point 5 de l'article 3 de la loi sur les transactions électroniques, les prestataires techniques doivent, directement ou indirectement, informer les autorités compétentes, dans les meilleurs délais, de l'existence d'un contenu en ligne manifestement illicite.

Ils doivent également agir promptement pour retirer ces contenus ou pour en rendre l'accès impossible conformément aux dispositions légales en vigueur.

Art. 10. - Les prestataires techniques doivent mettre en place, conformément au point 5 de l'article 3 de la loi sur les transactions électroniques, un dispositif facilement accessible et visible, permettant à toute personne de porter à leur connaissance tout contenu en ligne manifestement illicite.

Le dispositif consiste à mettre à la disposition des utilisateurs un accès par le biais d'un formulaire de signalement d'abus permettant d'informer, soit le prestataire du service concerné, soit les autorités compétentes, tout contenu en ligne manifestement illicite.

Chapitre V. - Conservation des éléments d'identification personnelle.

Art. 11. - Les prestataires techniques doivent mettre en œuvre un dispositif technique permettant de conserver les éléments d'information visés par l'article 5 de la loi sur les transactions électroniques.

A cet effet, ils défèrent dans les meilleurs délais aux demandes des autorités judiciaires visant à obtenir, soit les données de nature à permettre l'identification de l'auteur d'un contenu qu'ils hébergent, soit les données portant sur l'identification des personnes utilisatrices des services qu'ils fournissent.

Art. 12. - Les prestataires techniques ont une obligation de résultat en matière de conservation des données de nature à permettre l'identification de quiconque qui a contribué à la création du contenu en ligne.

Ils engagent leur responsabilité par négligence, conformément à l'article 431-44 de la loi sur la cybercriminalité, si les données qu'ils détiennent sont manifestement fantaisistes et ne permettent pas l'identification envisagée.

Art. 13. - Les données conservées portent exclusivement sur les éléments permettant l'identification des utilisateurs des services fournis par les prestataires techniques.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées.

Art. 14. - Les prestataires techniques, prévues par l'article 3 de la loi sur les transactions électroniques, doivent permettre aux autorités compétentes un accès facile, direct et permanent aux informations prévues par les points 1 et 2 de l'article 5 de la loi susmentionnée.

Art. 15. - En application des points 1 et 2 de l'article 5 de la loi sur les transactions électroniques, le défaut de mise à disposition au public des informations prévues par ces dits textes est passible de sanctions prévues par l'article 431-46 de la loi sur la cybercriminalité.

Chapitre VI. - Secret professionnel.

Art. 16. - L'obligation de secret prévu à l'article 5 de la loi sur les transactions électroniques s'impose à toutes les personnes dont l'activité est d'offrir un accès en ligne à des services au public par le biais des technologies de l'Internet notamment les éléments d'identification personnelle qui leur sont confiés dans le cadre de leur activité professionnelle.

Art. 17. - Sauf disposition contraire, l'obligation de secret cesse lorsque la révélation des éléments d'identification personnelle a été faite par la personne concernée.

...

Fait à Dakar, le 30 juin 2008.
Abdoulaye WADE.
Par le Président de la République :
Le Premier Ministre,
Cheikh Hadjibou SOUMARE.

**TITRE Ier : DE LA LIBERTÉ DE COMMUNICATION EN LIGNE
CHAPITRE II : Les prestataires techniques.**

Article 6

Modifié par Loi n° 2016-444 du 13 avril 2016 - art. 1

I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public 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.

Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code.

2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public 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 pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou 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.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un 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.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

4. Le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 Euros d'amende.

5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants :

-la date de la notification ;

-si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;

-les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;

-la description des faits litigieux et leur localisation précise ;

-les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;

-la copie de la correspondance adressée à l'auteur ou 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.

6. Les personnes mentionnées aux 1 et 2 ne sont pas des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.

7. Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.

Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie infantile, de l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal.

A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

Compte tenu de l'intérêt général attaché à la répression des activités illégales de jeux d'argent, les personnes mentionnées aux 1 et 2 mettent en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes en la matière. Elles informent également leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi.

Tout manquement aux obligations définies aux quatrième et cinquième alinéas est puni des peines prévues au 1 du VI.

8. L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

II.- Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.

L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.

Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.

III.-1. Les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert :

a) S'il s'agit de personnes physiques, leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ;

b) S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;

c) Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 précitée ;

d) Le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du prestataire mentionné au 2 du I.

2. Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.

Les personnes mentionnées au 2 du I sont assujetties au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. Ce secret professionnel n'est pas opposable à l'autorité judiciaire.

IV.-Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service.

La demande d'exercice du droit de réponse est adressée au directeur de la publication ou, lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée au 2 du I qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois mois à compter de la mise à disposition du public du message justifiant cette demande.

Le directeur de la publication est tenu d'insérer dans les trois jours de leur réception les réponses de toute personne nommée ou désignée dans le service de communication au public en ligne sous peine d'une amende de 3 750 Euros, sans préjudice des autres peines et dommages-intérêts auxquels l'article pourrait donner lieu.

Les conditions d'insertion de la réponse sont celles prévues par l'article 13 de la loi du 29 juillet 1881 précitée. La réponse sera toujours gratuite.

Un décret en Conseil d'Etat fixe les modalités d'application du présent IV.

V.-Les dispositions des chapitres IV et V de la loi du 29 juillet 1881 précitée sont applicables aux services de communication au public en ligne et la prescription acquise dans les conditions prévues par l'article 65 de ladite loi.

VI.-1. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies aux quatrième et cinquième alinéas du 7 du I du présent article ni à celles prévues à l'article 6-1 de la présente loi, de ne pas avoir conservé les éléments d'information visés au II du présent article ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments.

Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce code. L'interdiction mentionnée au 2° de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

2. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie au III, de ne pas avoir respecté les prescriptions de ce même article.

Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce code. L'interdiction mentionnée au 2° de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

Article 6-1

Créé par Loi n° 2014-1353 du 13 novembre 2014 - art. 12

Lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du code pénal ou contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du même code le justifient, l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi ou aux personnes mentionnées au 2 du I du même article 6 de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. Elle en informe simultanément les personnes mentionnées au 1 du I de l'article 6 de la présente loi.

En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux personnes mentionnées au même 1 la liste des adresses électroniques des services de communication au public en ligne contrevenant auxdits articles 421-2-5 et 227-23. Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. Toutefois, en l'absence de mise à disposition par la personne mentionnée au III du même article 6 des informations mentionnées à ce même III, l'autorité administrative peut procéder à la notification prévue à la première phrase du présent alinéa sans avoir préalablement demandé le retrait des contenus dans les conditions prévues à la première phrase du premier alinéa du présent article.

L'autorité administrative transmet les demandes de retrait et la liste mentionnées, respectivement, aux premier et deuxième alinéas à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés pour la durée de son mandat dans cette commission. Elle ne peut être désignée parmi les personnes mentionnées au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête.

L'autorité administrative peut également notifier les adresses électroniques dont les contenus contreviennent aux articles 421-2-5 et 227-23 du code pénal aux moteurs de recherche ou aux annuaires, lesquels prennent toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne. La procédure prévue au troisième alinéa du présent article est applicable.

La personnalité qualifiée mentionnée au même troisième alinéa rend public chaque année un rapport d'activité sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de demandes de retrait, le nombre de contenus qui ont été retirés, les motifs de retrait et le nombre de recommandations faites à l'autorité administrative. Ce rapport est remis au Gouvernement et au Parlement.

Les modalités d'application du présent article sont précisées par décret, notamment la compensation, le cas échéant, des surcoûts justifiés résultant des obligations mises à la charge des opérateurs.

Tout manquement aux obligations définies au présent article est puni des peines prévues au 1 du VI de l'article 6 de la présente loi.

Fait à Paris, le 21 juin 2004.
JACQUES CHIRAC

Par le Président de la République :
Le Premier ministre,
JEAN-PIERRE RAFFARIN

Le ministre d'Etat, ministre de l'économie,
des finances et de l'industrie,
NICOLAS SARKOZY

Le garde des sceaux, ministre de la justice,
DOMINIQUE PERBEN

Le ministre de la culture
et de la communication,
RENAUD DONNEDIEU DE VABRES

La ministre de l'outre-mer,
BRIGITTE GIRARDIN

Le ministre délégué à l'industrie,
PATRICK DEVEDJIAN

**Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité.
J.O. n° 6406 du samedi 3 mai 2008**

Article premier.

Il est inséré après l'article 431-6 du code pénal un titre III intitulé « Des infractions liées aux technologies de l'information et de la communication » qui comprend les articles 431-7 à 431-65 ainsi rédigés :

TITRE III. - Des infractions Liées aux Technologies de l'Information et de la Communication.

Chapitre Préliminaire - Terminologie.

Article 431-7.

Au sens de la présente loi, on entend par :

1. Communication électronique : toute mise à la disposition 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 ;
2. Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;
3. Raciste et xénophobe en matière des technologies de l'information et de la communication : 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 ;
4. Mineur : toute personne âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant ;
5. 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 ;
6. 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 Premier. - Atteintes aux systèmes informatiques.

Section Première - atteintes à la confidentialité des systèmes informatiques.

Article 431-8.

Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 431-9.

Quiconque se sera maintenu ou aura tenté de se maintenir frauduleusement dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Section II. - atteintes à l'intégrité des systèmes informatiques.

Article 431-10.

Quiconque aura entravé ou faussé ou aura tenté d'entraver ou de fausser le fonctionnement d'un système informatique sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs.

Section III. - Atteintes à la disponibilité des systèmes informatiques.

Article 431-11.

Quiconque aura accédé ou tenté d'accéder frauduleusement, introduit ou tenté d'introduire frauduleusement des données dans un système informatique, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Chapitre II. - Atteintes aux données informatisées.

Section Première. - Atteintes générales aux données informatisées.

Article 431-12.

Quiconque aura intercepté ou tenté d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-13.

Quiconque aura endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, modifié ou tenté de modifier, frauduleusement des données informatisées, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-14.

Quiconque aura produit ou fabriqué un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-15.

Est puni des mêmes peines celui qui, en connaissance de cause, aura fait usage ou tenté de faire usage des données obtenues dans les conditions prévues à l'article 431-14 de la présente loi.

Article 431-16.

Quiconque aura obtenu frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique, sera puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 5.000.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Section II. - Atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel.

Article 431-17.

Quiconque aura, même par négligence, procédé ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-18.

Quiconque aura, même par négligence, procédé ou fait procéder à un traitement qui a fait l'objet de la mesure prévue au point 1 de l'article 30 de la loi sur les données à caractère personnel, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-19.

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par l'article 19 de la loi sur les données à caractère personnel précitée, quiconque n'aura pas respecté, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission des Données Personnelles, sera puni d'un d'emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-20.

Quiconque aura, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi sur les données à caractère personnel précitée, procédé ou fait procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-21.

Quiconque aura procédé ou fait procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 71 de la loi sur les données à caractère personnel précitée, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-22.

Quiconque aura collecté des données à caractère personnel par un moyen frauduleux, déloyal ou illicite, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-23.

Quiconque aura procédé ou fait procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne conformément aux dispositions de l'article 68 de la loi sur les données à caractère personnel, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-24.

Quiconque aura, hors les cas prévus par la loi, mis ou conservé sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou qui sont relatives à la santé ou à l'orientation sexuelle de celui-ci, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Les dispositions du premier point du présent article sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 431-25.

Quiconque aura, hors les cas prévus par la loi, mis ou conservé sur support ou mémoire informatique des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté, sera puni des mêmes peines.

Article 431-26.

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, sera puni des mêmes peines, quiconque aura procédé à un traitement :

- 1) sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ainsi que des dispositions prises pour leur traitement, leur conservation et leur protection ;
- 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 431-27 :

Quiconque aura conservé des données à caractère personnel au-delà de la durée nécessaire prévue par l'article 35 de la loi sur les données à caractère personnel, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-28.

Quiconque aura, hors les cas prévus par la loi, traité à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée nécessaire prévue par l'article 35 de la loi sur les données à caractère personnel sera puni des mêmes peines.

Article 431-29.

Quiconque, détenant des données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, aura détourné ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission des Données Personnelles autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-30.

Quiconque aura recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, porté, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Lorsque la divulgation prévue à l'alinéa précédent du présent article a été commise par imprudence ou négligence, le responsable sera puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 300.000 francs à 5.000.000 francs ou de l'une de ces deux peines seulement.

Dans les cas prévus aux deux alinéas du présent article, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 431-31.

Sera puni d'emprisonnement de six mois à deux ans et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement, quiconque aura entravé l'action de la Commission des Données Personnelles :

- 1) soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel ;
- 2) soit en refusant de communiquer à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- 3) soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée où qui ne présentent pas ce contenu sous une forme directement accessible.

Chapitre III. - Autres abus.

Article 431-32.

Quiconque aura produit, vendu, importé, détenu, diffusé, offert, cédé ou mis à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues par les articles 431-8 à 431-16 de la présente loi 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, sera puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 431-33.

Quiconque aura participé à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente loi, sera puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Chapitre IV. - Infractions se rapportant au contenu.

Section Première - Pornographie infantile.

Article 431-34.

Quiconque aura produit, enregistré, offert, mis à disposition, diffusé, transmis une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'un emprisonnement de cinq (5) à dix (10) ans et d'une amende de 5.000.000 à 15.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-35.

Quiconque se sera procuré ou aura procuré à autrui, importé ou fait importer, exporté ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'un emprisonnement de cinq (5) à dix (10) ans et d'une amende de 5.000.000 francs à 15.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-36.

Sera puni des mêmes peines, celui qui possède 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.

Sera puni des mêmes peines, quiconque aura facilité l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 431-37.

Les infractions prévues par la présente loi, lorsqu'elles ont été commises en bande organisée, seront punies du maximum de la peine prévue à l'article 431-23 de la présente loi.

Section III. - Autres atteintes se rapportant au contenu

Article 431-38.

Quiconque aura créé, téléchargé, diffusé ou mis 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 sera puni d'un emprisonnement de six (6) mois à sept (7) ans et d'une amende de 1.000.000 francs à 10.000.000 francs.

Article 431-39.

La 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 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 sera puni d'un emprisonnement de six (6) mois à sept (7) ans et d'une amende de 1.000.000 à 10.000.000 francs.

Article 431-40.

L'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 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 sera puni d'un emprisonnement de six (6) mois à sept (7) ans et d'une amende de 1.000.000 à 10.000.000 francs.

Article 431-41.

Quiconque aura intentionnellement nié, approuvé ou justifié des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique, sera puni d'un emprisonnement de six (6) mois à sept (7) ans et d'une amende de 1.000.000 francs à 10.000.000 francs.

Article 431-42.

En cas de condamnation, le tribunal pourra prononcer la confiscation des matériels équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions prévues aux articles 431-8 à 431-41 de la présente loi.

Chapitre V. - Infractions liées aux activités des prestataires techniques de services de communication au public par voie électronique.

Article 431-43.

Quiconque aura présenté aux personnes mentionnées au 2° de l'article 3 de la loi sur les transactions électroniques, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, sera puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-44.

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux points 1 et 2 de l'article 3 de la loi sur les transactions électroniques, qui n'aura pas satisfait aux obligations définies au quatrième alinéa du point 5 de l'article 3 de la loi sur les transactions électroniques, n'aura pas conservé les éléments d'information visés à l'article 4 alinéa 1 de la loi susvisée ou n'aura pas déféré à la demande d'une autorité judiciaire d'obtenir communication desdits éléments sera puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement.

Article 431-45.

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie à l'article 3 de la loi sur les transactions électroniques, n'ayant pas respectée les prescriptions de ce même article sera puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement.

Article 431-46.

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie à l'article 3 de la loi sur les transactions électroniques, n'ayant pas respectée les prescriptions prévues à l'article 5 de la même disposition sera puni d'un an d'emprisonnement de six (6) mois à un (1) an et d'une amende de 200 000 francs à 2 000 000 francs ou de l'une de ces deux peines seulement.

Article 431-47.

Tout directeur de publication est tenu de publier la réponse portant sur l'exercice du droit de réponse, en application de l'article 6 de la loi sur les transactions électroniques, vingt quatre (24) heures, après la réception de la demande sous peine d'une amende de 200 000 à 20 000 000 FCFA, sans préjudice de toutes autres peines prévues par la législation en vigueur.

Article 431-48.

Les dispositions de l'article 431-44 de la présente loi s'appliquent pour tout manquement à l'obligation d'information du consommateur prévue par l'article 10 de la loi sur les transactions électroniques.

Article 431-49.

Le refus d'un fournisseur électronique de biens ou de services de rembourser les montants reçus d'un consommateur qui exerce son droit de rétraction est passible d'un d'emprisonnement de six (6) mois à un (1) an et d'une amende de 200 000 francs à 2 000 000 francs ou de l'une de ces deux peines seulement.

Article 431-50.

Sera puni d'un emprisonnement d'un (1) mois à un (1) an et d'une amende de 500 000 à 10 000 000 francs, ou l'une de ces peines seulement, celui qui aura trompé l'acheteur sur l'identité, la nature ou l'origine du bien vendu, en livrant frauduleusement un bien autre que celui commandé et acheté par le consommateur.

Chapitre VI. - Infractions liées à la publicité par voie électronique.

Article 431-51.

Quiconque aura méconnu les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celles de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie numérique, telles que prévues par l'article 15 de la loi sur les transactions électroniques sera puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement.

Article 431-52.

Quiconque aura réalisé des publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, en violation de l'article 14 de la loi sur les transactions électroniques sera puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 100.000 francs à 500.000 francs ou de l'une de ces deux peines seulement.

Chapitre VII. - Atteintes aux biens.

Article 431-53 :

La soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol.

Article 431-54.

Lorsque les infractions ont été commises par le biais d'un système informatique, il ne pourra être prononcé le sursis à l'exécution des peines.

Article 431-55.

Lorsque le délit a été commis par le biais d'un système informatique, les peines prévues à l'alinéa 1er de l'article 379 pourront être portées au double.

Article 431-56.

Quiconque aura reçu des informations personnelles, confidentielles ou celles qui sont protégées par le secret professionnel, usant des manœuvres frauduleuses quelconques, soit en faisant usage de faux noms ou de fausses qualités, sera puni des peines prévues à l'alinéa 1er de l'article 379.

Article 431-57.

Ceux qui auront recelé des informations enlevées, détenues ou obtenues à l'aide d'un crime ou d'un délit, seront punis des peines prévues à l'alinéa précédent.

Chapitre VIII. - Infractions commises par tous moyens de diffusion publique.

Article 431-58.

Sont considérés comme moyens de diffusion publique : la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique.

Article 431-59.

Sera puni d'un emprisonnement de 6 mois à 7 ans, d'une amende de 500 000 francs à 10 000 000 francs ou l'une de ces deux peines seulement quiconque aura :

1. fabriqué ou détenu en vue d'en faire commerce, distribution, location, affichage ou exposition ;
2. importé ou fait importer, exporté ou fait exporter, transporté ou fait transporter sciemment aux mêmes fins ;
3. affiché, exposé ou projeté aux regards du public ;
4. vendu, loué, mis en vente ou en location, même non publiquement ;
5. offert, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;
6. distribué ou remis en vue de leur distribution par un moyen quelconque.

Tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs.

Le maximum de la peine sera prononcé lorsque les faits ci-dessus visés ont un caractère pornographique.

Le condamné pourra en outre faire l'objet, pour une durée ne dépassant pas six mois, d'une interdiction d'exercer, directement ou par personne interposée, en droit ou en fait, des fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publication périodiques.

Quiconque contreviendra à l'interdiction visée ci-dessus sera puni des peines prévues au présent article.

Chapitre IX. - Atteintes à la défense nationale.

Article 431-60.

Sera coupable de trahison et puni de la perpétuité tout sénégalais, qui :

- 1) livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que se soit un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;
- 2) s'assure, par quelque moyen que se soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisée ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
- 3) détruit ou laisse détruire tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère. »

Article 431-61.

Sera puni du maximum des travaux forcés à temps, tout sénégalais ou tout étranger qui, dans l'intention de les livrer à tout pays tiers, rassemblera des renseignements, objets, documents, procédés, données ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense nationale ».

Sera puni de la détention criminelle de dix à vingt ans, tout gardien, tout dépositaire par fonction ou par qualité d'un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de défense nationale, qui sans intention de trahison ou d'espionnage, l'aura :

- 1) détruit, soustrait, laissé détruire ou soustraire, reproduit ou fait reproduire ;
- 2) porté ou laissé porter à la connaissance d'une personne non qualifiée ou du public.

La peine sera celle de la détention criminelle de cinq à dix ans si le gardien ou le dépositaire a agi par maladresse, imprudence, inattention, négligence ou inobservation des règlements.

Chapitre X. - Responsabilité pénale.

Article 431-62.

Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Les peines encourues par les personnes morales sont :

- 1) l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;
- 2) la dissolution, lorsque la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq (5) ans, détournée de son objet pour commettre les faits incriminés ;
- 3) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- 4) la fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- 5) l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ;
- 6) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ;
- 7) l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;
- 8) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;
- 9) l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

Article 431-63.

Cependant exception faite des infractions de presse commises par le biais de l'Internet, les crimes, délits et contraventions prévus à la section IV du chapitre IV du titre I du livre III du code pénal, lorsqu'ils sont commis par le biais d'un support de communication numérique, sont soumis au régime de la responsabilité de droit commun ».

Article 431-64.

S'il y a condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction, en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement.

Le juge peut faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction, à toute personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

La violation des interdictions prononcées par le juge sera punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 300.000 francs à 5.000.000 francs. »

Article 431-65.

En cas de condamnation à une infraction commise par le biais d'un support de communication numérique, le juge ordonne à titre complémentaire la diffusion au frais du condamné, par extrait, de la décision sur ce même support.

La publication prévue à l'alinéa précédent doit être exécutée dans les 15 jours suivant le jour où la condamnation est devenue définitive.

Le condamné qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa précédent sera puni des peines prévues par le code pénal.

Si dans le délai de quinze jours (15) jours après que la condamnation soit devenue définitive, le condamné n'a pas diffusé ou fait diffuser cet extrait, les peines prévues au présent article seront portées au double. »

Article 2.

Il est inséré au livre quatrième du code procédure pénal un titre XVI intitulé « De la procédure en matière d'infractions commises au moyen des technologies de l'information et de la communication comprenant les articles 677-34 à 677-42 ainsi rédigés :

Titre XVI. - DE LA PROCEDURE EN MATIERE D'INFRACTIONS COMMISES AU MOYEN DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION.

Chapitre premier : prescription en matière d'infractions commises par le biais de réseaux numériques.

Article 677-34.

Les crimes, délits et contraventions prévus à la section IV du chapitre IV du titre I du livre III du code pénal, lorsqu'ils sont commis par le biais de réseaux informatiques se prescrivent dans les délais et suivant les distinctions établies par les articles 431-12 à 431-16 de la loi sur la cybercriminalité, à compter de la cessation de l'activité délictueuse en ligne. »

Chapitre II. - Conservation rapide de données informatisées archivées.

Article 677-35.

Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires.

Le gardien des données ou une toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret.

Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

Chapitre III. - Perquisition et de la saisie informatique.

Article 677-36.

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire sénégalais, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. »

Article 677-37.

Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

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

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le juge d'instruction ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Lorsque la mesure prévue à l'alinéa 2 de l'article 677-37 de la présente loi n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Le juge d'instruction informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées. »

Chapitre IV. - interception des données informatisées.

Article 677-38.

Si les nécessités de l'information l'exigent, le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

Le fournisseur d'accès est tenu de garder le secret.

Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel. »

Article 677-39.

L'officier de police judiciaire peut, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par les articles 667-35 à 677-38 de la présente loi. »

Chapitre V : Preuve électronique en matière pénale.

Article 677-40.

L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier conformément aux dispositions de l'article 40 de la loi sur les transactions électroniques.

Article 677-41.

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

Article 677-42.

Le procureur de la République avise le président de la Commission des Données Personnelles de toutes les poursuites relatives aux infractions aux présentes dispositions et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'audience de jugement.

La juridiction d'instruction ou de jugement peut appeler le président de la Commission des Données Personnelles ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Le juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie.

Art. 3.- Les modalités d'application de la présente loi seront prises par décret.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Dakar, le 25 janvier 2008
Abdoulaye WADE
Par le Président de la République
Le Premier Ministre
Cheikh Hadjibou SOUMARE

CONVENTION

- Convention Européenne des Droits de l'Homme, *Library of the Court, Bulletin of the Court*, 2015-3.

DIRECTIVE

- Directive n° 2000/31/CE 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 dite «directive sur le commerce électronique», JOCE 17 juillet 2000, n° L 178.

CONSTITUTION

- La Constitution de la République du Sénégal du 22 janvier 2001.

LOIS et CODES

Sénégal

- Loi n° 2008-10 du 25 janvier 2008 portant Loi d'Orientation sur la Société de l'Information (LOSI). JORS n° 6406 du Samedi 3 mai 2008.
- Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS n° 6439 du Samedi 22 novembre 2008.
- Loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité, JORS n° 6406 du Samedi 3 mai 2008.
- Loi n° 2001-15 du 27 décembre 2001 portant Code des télécommunications, JORS N° 6030 du samedi 16 février 2002.
- Loi n° 2011-01 du 04 février 2011 portant Code des télécommunications, JORS, N° 6576 du Lundi 4 mars 2011, page 273.
- Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, JORS n° 6406 du Samedi 3 mai 2008.
- Loi n° 2008-41 du 20 août 2008 portant sur la cryptologie. JORS N° 6441 du Samedi 6 décembre 2008.
- Code des Obligations Civiles et Commerciales (COCC).
- Code pénal.
- Code de procédure pénale.

France

- Loi n° 2004-575 du 21 juin 2004 pour la Confiance dans l'Economie Numérique. JORF n° 143 du 22 juin 2004 texte n° 2/108 page 11168.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. JORF n° 0235 du 8 octobre 2016, p. 7, Texte 1.
- Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. JORF n° 0129 du 4 juin 2016, texte 1 / 119.
- Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication. JORF du 1 octobre 1986 page 11755.
- 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. JORF n° 0110 du 13 mai 2010.
- Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. JORF n° 0263 du 14 novembre 2014.
- Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. JORF n° 0139 du 18 juin 1998, p. 09255.
- Loi du 29 juillet 1881 sur la liberté de la presse. JORF du 30 juillet 1881 page 4201.
- Loi n° 52-336 du 25 mars 1952 modifiant l'article 42 de la loi du 29 juillet 1881 sur la liberté de la presse. JORF n° 0075 du 26 mars 1952 page 3253.
- Code des postes et des communications électroniques.
- Code civil.
- Code pénal.

DECRETS

- Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques. JORS n° 6439 du Samedi 22 novembre 2008.
- Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée. JORF n° 0001 du 1 janvier 2012.
- Décret n° 2008-721 du 30 juin 2008, portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel. JORS n° 6443 du samedi 20 décembre 2008, pp. 1169-1177.
- Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. JORF n° 0050 du 1 mars 2011, texte 32 sur 170.
- Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. JORF n°0031 du 6 février 2015 page 1811, texte n° 71/162.

OUVRAGES GENERAUX et SPECIAUX

- PAPA ASSANE TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*, L'Harmattan, Paris, 2014,
- PHILIPPE BOURE, *Le droit et Internet : les enjeux présents et futurs de la société de l'information*, L'Hermès, Paris, 2002.
- OLIVIER SAGNA, CHRISTOPHE DRUN et STEVEN HUTER, *Histoire de l'Internet au Sénégal : 1989 – 2004*, University of Oregon Libraries, USA, 2013.
- JACQUES CHEVALLIER, *L'État postmoderne*, LGDJ, 2e éd, Paris, 2004.
- ALAIN SERIAUX et MARC BRUSCHI, *Le commentaire de textes juridiques : lois et règlements*, 2ème éd., Ellipses, Paris, 2007.
- CHRISTINE CARL, *La responsabilité des intermédiaires techniques*, La Documentation Française. Paris, 2004.
- JEAN-MICHEL RODES, GENEVIEVE PIEJUT et EMMANUELE PLAS, *La mémoire de la société de l'information*, Jouve, Paris, 2003.
- NICOLAS CURIEN, PIERRE-ALAIN MUET, *La société de l'information*, La Documentation française, Paris, 2004.
- JEAN-DENIS PELLIER, *Le principe de l'unité des fautes civile et pénale à l'épreuve de la loi du 10 juillet 2000*, Université Paul Cézanne – Aix-Marseille III, 2005.
- FRANÇOIS TERRE, PHILIPPE SIMLER et YVES LEQUETTE, *Droit civil, Les obligations*, 2ème éd. Dalloz, 2002.
- CHAÏM PERELMAN et RAYMOND VANDER ELST, *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984.
- MARIUS TCHENDJOU, *Droit des obligations*, Vuibert, Coll. Vuibert Droit, Paris, 2015.
- ANDRE LUCAS, JEAN DEVEZE et JEAN FRAYSSNET, *Le droit de l'informatique et de l'Internet*, PUF, Paris, 2001.
- VERBIEST THIBAUT ET W. ETIENNE, *Le droit de l'Internet et de la société de l'information*, Larcier, Bruxelles, 2001.
- ANDRE TUNC, *Responsabilité civile et dissuasion des comportements antisociaux, Aspects nouveaux de la pensée juridique*, Mélanges, Ancel, 1975, t. I.
- MARCEL PLANIOL, *Traité élémentaire de droit civil*, 4e éd., 1952, n° 907.
- PAUL CASSIA, *La sécurité juridique, un "nouveau" principe général du droit aux multiples facettes*, Dalloz, 2006.
- ETIENNE WERY, *Sexe en ligne : aspects juridiques et protection des mineurs*, Larcier, Bruxelles, 2004.
- SANDRINE PINA, *La connaissance pure du droit et ses limites*, Vrin, Paris, 2000.
- PATRICK TORT, *Evolutionnisme et linguistique*, Vrin, Paris, 1980.

THESES

- ABDOUL AZIZ DIOUF, *Essai sur le régime juridique des noms de domaine*, Université d'Orléans, 2010.
- JEANINE-ARMELLE TANO-BIAN ANMONKA, *La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'ouest*, Université de Paris Descartes, 2015.
- JULIE ANGENOT, *L'exonération de responsabilité au profit des hébergeurs s'étend-elle aux gestionnaires de sites participatifs et aux exploitants de forums de discussion ?*, Université Catholique de Louvain, 2015.
- CLEMENT MARGAINE, *La capacité pénale*, Université Montesquieu, Bordeaux IV, 2011.
- MAIWENN TASCHER, *Les revirements de jurisprudence de la Cour de Cassation*, Université de Franche-Comté, Besançon, 2011.
- CECILE NLEND, *La protection du mineur dans le cyberspace*, Université de Picardie Jules Verne, Amiens, 2007.
- LYDIE DUTHEIL-WAROLIN, *La notion de vulnérabilité de la personne physique en droit privé*, Université de Limoges, 2004.

ARTICLES et CHRONIQUES

Revue, Bulletins et Magazines

- PAPA ASSANE TOURE, *Cinq ans de droit pénal des technologies de l'information et de la communication (2008 – 2013) : chronique de jurisprudence sénégalaise*, Cour Suprême, Dakar, Bull. d'Info., Décembre 2015, n° 7 – 8.
- BERTRAND MATHIEU, *La normativité de la loi : une exigence démocratique*, Cahiers du Conseil constitutionnel, n° 21, Paris, janvier 2007.
- BENOIT MOORE, *De l'acte et du fait juridique ou d'un critère de distinction incertain*, Revue Juridique Thémis, Montréal, 1997.
- TIMOTHY WU, *Network Neutrality, Broadband Discrimination*, dans "Journal of Telecommunications and High Technology Law", n° 2, New York, 2003.
- ETIENNE MONTERO, *La responsabilité des prestataires intermédiaires de l'Internet*, Ubiquité, n° 5, juin 2000.
- LIONEL THOUMYRE, *La responsabilité pénale et extracontractuelle des acteurs de l'Internet*, Lamy Droit des Médias et de la Communication, Etude 464, 2009.
- BART VAN BESIEN, *La responsabilité des gestionnaires de forums de discussion "non commerciaux"*, A. & M., 2010, n° 2010/5.
- VERBIEST THIBAUT, LIONEL THOUMYRE, *Responsabilités sur Internet : Le mannequin et l'hébergeur*, Cour d'appel de Paris, Arrêt rendu en 10 février 1999, *Estelle H. c/ Valentin L.*, Juriscom, 25 février 1999.

- PIRES P. ALVARO, *La rationalité pénale moderne, la société du risque et la juridicisation de l'opinion publique*, Revue Sociologie et Sociétés, vol. 33, n°1, Université d'Ottawa, Ontario, Canada, 2001.
- LIONEL THOUMYRE, *Comment les hébergeurs français sont devenus juges du manifestement illicite*, Juriscom, 28 juillet 2004.
- OPHELIE FONDEVILLE ET ANNE-SOPHIE JOUANNON, *Le "manifestement illicite", mystérieux point de rencontre entre la victime et l'hébergeur*, Juriscom, 7 avril 2008.
- FRANÇOIS DIESSE, *Les applications de l'article 1147 du Code civil de 1804 à 2004*, RGD, vol. 34, n° 3, 2004.
- VALERIE SEDALLIAN, *Principes généraux du droit de la responsabilité et responsabilité des acteurs de l'internet*, Légamedia, Paris, 2002.
- VERBIEST THIBAUT et MARIE DE BELLFROID, *Filtrage et responsabilité des prestataires techniques de l'internet : retour sur l'affaire SABAM C/ Tiscali*, Chroniques et Opinions, Legipresse n°246, Novembre 2007.
- PASCAL REYNAUD, *Le fournisseur d'accès et la conservation des données engendrées par les communications électroniques*, Communication Commerce électronique, n° 6, juin 2005.
- AGATHE LEPAGE, *Liberté d'expression, responsabilité et forums de discussion*, Comm. Com. Electr., n°6, janvier 2003.
- H. CHRISTINE, *La responsabilité des acteurs de l'Internet dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, Contrats Concurrence Consommation, n° 11, 2004.
- P. JURGITA PETRAUSKAITE, *L'évolution du régime de la responsabilité de l'hébergeur*, Chronique, Paris, Lamy, 2004.
- ARMEL BENERAB, *L'hébergement et le stockage de données médicales sensibles*, CGV Expert, Avril 2012.
- CHRISTOPHE VERDURE, *Les hébergeurs de sites web : victimes ou régulateurs de la société de l'information ?*, DCCR, n° 68, Doctrine, Larcier, 2005.

Journaux

- MAÏA MAZAURETTE, *La pornographie comme revanche*, Lemonde.fr du 09 octobre 2016.
- OLIVIER ITEANU, *Peut-on assimiler un hébergeur au directeur de publication d'un magazine de presse ?*, Journal Du Net, 7 novembre 2000.
- JULIEN ELMALEH, *La responsabilité civile*, Fiche 14, La Gazette des Communes, 2000.
- MARIE-ANNE FRISSON LA ROCHE, *Commentaire de l'arrêt Blicq du 29 mars 1991, Cour de cassation, Assemblée plénière*, Mafr.fr, 2 janvier 2014.

JURISPRUDENCE

Cour européenne

- CJUE, 2^{ème} Ch., 19 octobre 2016, *Patrick Breyer c / Bundesrepublik Deutschland*, Affaire C-582/14, www.curia.europa.eu.
- CJUE, Gde. Ch., 12 juillet 2011, *L'Oréal c/ EBay International*, Affaire n°C-324/09, www.curia.europa.eu.
- CJUE, 3^{ème} Ch., 16 février 2012, *Sabam c/ Netlog*, Affaire n° C-360/10, www.curia.europa.eu.

Conseil constitutionnel - France -

- Décision n° 2004/496 DC du 10 juin 2004 du Conseil constitutionnel. JORF du 22 juin 2004, p. 11182, texte n° 3, Recueil, p. 101.

Cours

- Ass. Plén., 29 mars 1991, pourvoi n° 89-15231, *Affaire Bliet*. www.legifrance.gouv.fr
- Ass. Plén., 19 mai 1988, Dalloz, 1988-513, 2000. p. 4
- Cass. Civ., 1ère ch., 3 nov. 2016, Arrêt n° 1184, Pourvoi n° 15-22.595, *Cabinet Peterson c/ Groupe Logisneuf et autres*. www.courdecassation.fr
- Cass. Civ. 1ère, 12 juill. 2012, *Gaz. Pal.* 25-26 juill. 2012, Comm. de Caroline L- G, RLDI 2012/85, n° 2851, obs. L. Costes.
- Cass. Civ 1ère Ch., 12 juillet 2012, Pourvoi n° 11-13.669, *Sté Google France et Sté Google Inc. c/ Sté Bac films et Sté The Factory*, www.courdecassation.fr
- Cass. Civ 1ère Ch., 12 juillet 2012, Pourvoi n° 11-15.165, *Sté Google France et autres c/ Sté Auféminin.com*, www.courdecassation.fr.
- Cass. Civ., 1ère Ch., 17 février 2011, n° 09 – 15857, *Nord-Ouest Production et autres c/ Dailymotion*, Bull. civ. 2011, I, n° 32, RLDI, n° 97, octobre 2013, p. 104
- Cass. Civ. (2ème Ch.), 18 février 2010, *Active communication Ltd (Act Com) c/ Ville de Marseille*. www.legalis.net.
- Cass. Civ., 1ère Ch. 20 novembre 1990, pourvoi n°89-12580, www.courdecassation.fr.
- Cass. Crim. 15 janv. 2008 : Dr. Pén. 2008, Comm. n° 71 ; JCP 2008, II, 10082, note J.-Y. MARECHAL.
- Cass. Crim., 20 juin 2006, Bull. Crim. n° 188, Dr. Pén. 2006, comm. n° 128.
- Cass. Crim, 8 janvier 1998, *Affaire Ricard*, inédit.
- Cass. Crim, 17 novembre 1992, n° 91-84.848, *Légipresse* 1993, n° 98, III, p. 1 et s.
- Cass. Crim. 15 novembre 1990 Bull. Crim. 1990 n°388 ; 17 novembre 1992 Les Petites Affiches 12 avril 1993, n°44.
- Cass. Crim, 15 novembre 1990, Bull. Crim, n°388 ; novembre 1992 Les Petites Affiches 12 avril 1993, n°44.
- Cass. Com. 21 janvier 2014, *Darty Télécom c/ Arjel*, www.legalis.net.
- Cass. Com. 27 avril 2009, *Davis films c/ Dailymotion*, www.legalis.net.
- C.A. Dakar, n° 356 du 25 mars 2011, *affaire Palluci*, inédit.

- CA de Paris, Pôle 1, 3ème Ch., 14 juin 2016, *Mme X. / Wikimedia Foundation Inc.*, www.legalis.net.
- CA de Paris, Pôle 5, 1ère Ch., 2 décembre 2014, *TF1 et autres / Dailymotion*, www.legalis.net.
- CA de Paris, Pôle 1, 2ème Ch., 04 avril 2013, *Rose B. / JFG Networks*, www.legalis.net.
- C.A. Paris (2ème ch.), 03 décembre 2010, *Google vidéo c/ Zadig Production*, www.legalis.net.
- C.A Paris, 14 février 2010, *Omar et Fred et autres c/ Dailymotion*, www.legalis.net.
- CA Paris, 4 nov. 2006, *SA Tiscali (Telecom Italia), AFA, France Telecom et a. c/UEJF, J'Accuse, SOS Racisme et a.*, Legipresse n°246, nov. 2007, p. 160.
- CA Paris, 14ème Ch, Sect. A, 10 février 1999, *Estelle H. c/ Valentin L.*, www.altern.org.
- CA de Paris, 1re ch. B, 19 juin 1998, Dalloz, 1998, IR, p. 204.

Tribunaux

- TRHC Dakar, n° 2715 du 19 juin 2012, *affaire des jeunes filles de Grand-Yoff*, inédit.
- TRHC Dakar, n° 1159 du 16 mars 2010, *affaire Palluci*, inédit.
- TRHC de Dakar, n° 499/ 2008 du 5 septembre 2008, *affaire de la Direction du Traitement Automatique de l'Information (DTAI)*, inédit.
- TGI Paris, 17e ch. correctionnelle, 7 septembre 2016, *Avocats sans frontières, Licra, SOS Racisme c/ M. X.*, www.legalis.net.
- TGI de Paris, Ord. Réf., 13 avril 2016, *UEJF et AIPJ / Egalite et Réconciliation*, www.legalis.net.
- TGI de Paris, 3ème Ch., 2ème Section, jugement du 4 décembre 2015, *Goyard St-Honoré / LBC France*, www.legalis.net.
- TGI de Paris 17ème Ch. Civ., 23 octobre 2013, *Bruno L. Ressources et actualisation c/ Google Inc., Google France*, www.legalis.net.
- TGI Paris, réf., 4 avr. 2013, RLDI 2013/94, n° 3129, p. 51.
- TGI Paris, Ord. Réf., *Claude Guéant c/ Free et autres*, 10 février 2012. www.legalis.net.
- TGI Paris, 17e ch., 14 nov. 2011, *Olivier M. c/ Sté Prisma Presse et a.*, www.legalis.net.
- TGI de Paris, Ord. Réf., 28 juin 2011, *Numéricâble, SFR et autres / Les Editions Gallimard*, www.legalis.net.
- TGI de Paris 17ème Ch. 5 septembre 2010, commentaire de Jérôme HUET pp. 429-430. Legipresse n°278, pp. 426 à 430. Décembre 2010.
- TGI de Paris, Ord. Réf., 5 mars 2009, *Roland Magdane et autres c/ YouTube*, www.legalis.net
- T.G.I. Paris (réf.), 15 décembre 2008, *Claire L. c/ Mehdi K.*, www.legalis.net.

- T.G.I. Paris, 14 nov. 2008, *Jean-Yves Lafesse et autres c/ Youtube et autres*, www.legalis.net.
- TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Mezrahi c/ Google*, www.legifrance.gouv.fr.
- TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Magdane c/ Youtube*, www.legifrance.gouv.fr.
- TGI de Draguignan, 15 mai 1992, Petites affiches 23 nov. 1992, p. 12, obs. Huet J.
- TGI de Paris, 3ème Ch., 2ème Sect., Jugement du 19 octobre 2007, *Zadig Productions et autres / Google Inc, Afa*, www.legalis.net.
- T.G.I. Paris, 19 octobre 2007, *Zadig Production c/ Google vidéo*, www.legalis.net.
- T.G.I. Paris (3ème ch.), 15 avril 2008, *Omar et Fred et autres c/ Dailymotion*, www.legalis.net
- TGI de Nanterre, 1ère Ch., Sect. A, 24 mai 2000, *Union des Etudiants Juifs de France (Uejf) / SA Multimaniam Production*, www.legalis.net.
- TGI de Paris, 3ème Ch., 2ème section, Jugement du 10 juillet 2009, *Bayard Presse / YouTube LLC.*, RLDI, n° 97, octobre 2013, p. 104.
- TGI de Paris, Ord. Réf., 9 juillet 2004, *Groupama c/ Gérard D., Free*, www.legalis.net.
- TGI de Paris, Ord. Réf., 29 octobre 2007, *Marianne B. et autres / Wikimedia Foundation*, www.legalis.net.
- TGI de Chartres, jugement du 8 août 2016. *Inédit*.
- TC de Paris, 8ème Ch., Jugement du 20 février 2008, *Flach Film et autres / Google France, Google Inc*, www.legalis.net.
- TGI de Paris, Ord. Réf., 18 décembre 2007, *M. Jean-Yves L. et SARL L. Anonyme c/ SA Dailymotion*, www.legifrance.gouv.fr.
- TGI de Paris, Ord. Réf., 9 janvier 2008, *R. Mezrahi c/ Youtube*, www.legifrance.gouv.fr.

DELIBERATION

- CDP : Délibération n° 2014-016 du 30 avril 2014 mettant en demeure Tigo Sénégal pour non déclaration de fichiers, bases de données et systèmes contenant des informations nominatives et pratiques de prospection directe non conforme à la législation.

RAPPORTS, TRAVAUX et CONFERENCES

- *Rapport "Mesurer la société de l'information 2015 : résumé analytique"*, ITU, Genève, 2015.
- *Rapport "Pour une réforme du droit de la responsabilité civile"*, sous la direction de FRANÇOIS TERRE, Cour de cassation, Paris, 2012.
- *7ème Rapport de l'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP) sur le préjudice subi par la France à cause de la cybercriminalité*, Paris, 2011.
- *Rapport explicatif de la Convention sur la cybercriminalité* », *Série des traités européens n°185*, Budapest, 23 novembre 2001.
- *Premier rapport sur l'application 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")*, Bruxelles, 21 novembre 2003.
- ABDOUL AZIZ DIOUF, *Présentation générale de la responsabilité civile : les faits générateurs, le fait d'autrui*, (Coord. Nd. F. LECOR), UCAD, FSJP, fiche TD, 2014/2015.
- PAPA ASSANE TOURE, *Conférence sur la coopération contre la cybercriminalité : la cyberstratégie de répression de la cybercriminalité au Sénégal, présentation de la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité*, Strasbourg, France, 23-25 mars 2010.

ENCYCLOPEDIAS

- Encyclopædia Universalis.
- Wikipédia.

DICTIONNAIRES

- Larousse.
- Juridictionnaire.
- Le Dictionnaire de droit criminel.
- Le Jargon Français, le dictionnaire d'informatique francophone.

APERCU

Sites consultés :

18 sites officiels, 39 sites spécialisés, 04 sites généralistes.

Principales extensions concernées :

.sn .fr .eu .int .org .net .com

SITES OFFICIELS

1. www.gouv.sn
2. www.jo.gouv.sn
3. www.justice.gouv.sn
4. www.cdp.sn
5. www.adie.sn
6. www.artpsenegal.sn
7. www.ansd.sn
8. www.conseil-constitutionnel.fr
9. www.legifrance.gouv.fr
10. www.journal-officiel.gouv.fr
11. www.courdecassation.fr
12. www.arcep.fr
13. www.asmp.fr
14. www.internet-signalment.gouv.fr
15. www.curia.europa.eu
16. www.echr.coe.int
17. www.bceao.int
18. www.itu.int

SITES SPECIALISES

DROIT

1. www.dictionnaire-juridique.com
2. www.juricaf.org
3. www.ledroitcriminel.fr
4. www.legalis.net
5. www.juriscom.net
6. www.droitconstitutionnel.org
7. www.droit-technologie.org
8. www.legavox.fr
9. www.saif.fr
10. www.erudit.org
11. www.mafr.fr
12. www.scaraye.com
13. www.planetoscope.com

INFORMATIQUE

1. www.biz-en-or.com
2. www.hitek.fr
3. www.reseau-informatique.prestataires.com
4. www.webrankinfo.com
5. www.commentcamarche.net
6. www.info-digitale.com
7. www.journaldunet.com
8. www.nextinpact.com
9. www.blogdumoderateur.com

AUTRES

1. www.futura-science.com
2. www.statista.com
3. www.e-enfance.org
4. www.numericable.fr
5. www.orange.sn
6. www.orange.fr
7. www.expressotelecom.sn
8. www.tigo.sn
9. www.faq.dailymotion.com
10. www.support.twitter.com
11. www.support.google.com
12. www.agenceecofin.com
13. www.universalis.fr
14. www.larousse.fr
15. www.youtube.com
16. www.bloomberg.com
17. www.centre-hubertine-auclert.fr

SITES GENERALISTES

1. www.lemonde.fr
2. www.wikipedia.org
3. www.altern.org
4. www.lagazettedescommunes.com

TABLE DES MATIERES

AVERTISSEMENT.....	I
ÉPIGRAPHE.....	II
DEDICACE.....	III
REMERCIEMENTS.....	IV
ACRONYMES.....	V
SIGLES.....	VI
ABREVIATIONS.....	VIII
SOMMAIRE.....	X
INTRODUCTION.....	1
<i>PREMIERE PARTIE : La responsabilité dérogatoire des fournisseurs d'accès à Internet.....</i>	09
<i>CHAPITRE 1^{er} : L'irresponsabilité principielle.....</i>	12
<i>Section 1^{ère} : L'absence a priori de la responsabilité civile et pénale.....</i>	12
<i>Paragraphe 1^{er} : L'exigence de neutralité et d'exclusivité fonctionnelles.....</i>	14
<i>A : La neutralité fonctionnelle.....</i>	14
<i>B : L'exclusivité fonctionnelle.....</i>	16
<i>Paragraphe 2 : L'exécution d'une décision de l'autorité judiciaire ou administrative.....</i>	17
<i>A : L'exécution d'une décision de l'autorité judiciaire.....</i>	17
<i>B : L'exécution d'une décision de l'autorité administrative.....</i>	19
<i>Section 2 : L'engagement de la responsabilité du fait personnel.....</i>	21
<i>Paragraphe 1^{er} : Le fournisseur d'accès à Internet à l'origine de la transmission du contenu et la sélection du destinataire.....</i>	21
<i>A : Le fournisseur d'accès à Internet à l'origine de la transmission du contenu.....</i>	21
<i>B : La sélection du destinataire du contenu.....</i>	23
<i>Paragraphe 2 : La sélection et la modification du contenu.....</i>	25
<i>A : La sélection du contenu.....</i>	25
<i>B : La modification du contenu.....</i>	26
<i>CHAPITRE 2 : Les obligations d'information, de moyens, de surveillance, de contrôle et de résultat.....</i>	28
<i>Section 1^{ère} : Les obligations d'information et de moyens.....</i>	28
<i>Paragraphe 1^{er} : L'obligation d'information.....</i>	28
<i>A : L'information à l'attention des abonnés et des tiers.....</i>	28
<i>B : L'information à l'attention des autorités compétentes.....</i>	30
<i>Paragraphe 2 : L'obligation de moyens.....</i>	33

A : Les moyens au profit des éditeurs, des autorités compétentes et des tiers.....	33
B : Les moyens de protection des mineurs.....	34
Section 2 : L'obligation minimale de surveillance et les obligations de contrôle et de résultat.....	38
Paragraphe 1 ^{er} : L'obligation minimale de surveillance.....	38
A : La surveillance ciblée et temporaire.....	38
B : La prévention et la cessation du dommage.....	39
Paragraphe 2 : Les obligations de contrôle, de résultat et de secret.....	41
A : L'obligation de contrôle.....	41
B : Les obligations de résultat et de secret.....	42
SECONDE PARTIE : La responsabilité aménagée des hébergeurs	46
CHAPITRE 1^{er} : L'exonération limitée de responsabilité	48
Section 1 ^{ère} : L'exonération de la responsabilité civile et pénale.....	48
Paragraphe 1 ^{er} : La méconnaissance, condition de l'exonération.....	49
A : La méconnaissance de l'illicéité du contenu.....	49
B : La méconnaissance des faits, circonstances et activités générateurs du contenu illicite.....	50
Paragraphe 2 : L'obligation de prompt réaction dès connaissance du forfait.....	51
A : Le retrait du contenu illicite.....	51
B : Le fait de rendre inaccessible le contenu illicite.....	54
Section 2 : Les limites à l'exonération de la responsabilité civile et pénale.....	57
Paragraphe 1 ^{er} : L'autorité ou le contrôle de l'hébergeur sur le destinataire.....	57
A : L'autorité de l'hébergeur sur le destinataire.....	57
B : Le contrôle exercé par l'hébergeur sur le destinataire.....	59
Paragraphe 2 : La présomption de connaissance des faits litigieux.....	61
A : L'exigence de la notification.....	61
B : La preuve des faits et de la notification.....	62
CHAPITRE 2 : L'exonération des obligations générales de surveillance et de recherche	64
Section 1 ^{ère} : L'exonération de l'obligation générale de surveillance.....	64
Paragraphe 1 ^{er} : L'étendue de l'exonération.....	64
A : Le stockage des informations.....	64
B : La nature des informations.....	66
Paragraphe 2 : La consécration d'une obligation spéciale de surveillance et d'information.....	67
A : La demande de l'autorité judiciaire.....	67
B : La sauvegarde de l'intérêt général et l'information de l'autorité compétente.....	68
Section 2 : L'exonération de l'obligation générale de recherche.....	70
Paragraphe 1 ^{er} : Les niveaux de mise en œuvre de l'exonération.....	70
A : L'absence de recherche des faits révélateurs des activités illicites.....	70
B : L'absence de recherche des circonstances révélatrices des activités illicites.....	71
Paragraphe 2 : La consécration d'une obligation particulière de recherche et de moyens.....	72

<i>A : Les mécanismes de mise en œuvre de l'obligation particulière de recherche</i>	72
<i>B : L'obligation particulière de moyens</i>	74
CONCLUSION	77
ANNEXES	I
Annexe 01.....	II
Annexe 02.....	IV
Annexe 03.....	VII
Annexe 04.....	XI
BIBLIOGRAPHIE	XX
WEBOGRAPHIE	XXVIII
TABLE DES MATIERES	XXX