



HAL
open science

LA PROTECTION DU MINEUR DANS LE CYBER ESPACE

Cecile Valerie Nlend

► **To cite this version:**

Cecile Valerie Nlend. LA PROTECTION DU MINEUR DANS LE CYBER ESPACE. domain_other.
universite de picardie Jules Verne, 2007. Français. NNT : . tel-00432247

HAL Id: tel-00432247

<https://theses.hal.science/tel-00432247>

Submitted on 15 Nov 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LA PROTECTION DU MINEUR DANS LE CYBERESPACE

Thèse pour l'obtention du grade de docteur de l'université de Picardie Jules Verne

Discipline : Droit public

Cécile NLEND

En date du 30 novembre 2007

Directeur de thèse :

M. Jean-Marc THOUVENIN

Professeur de droit communautaire à l'Université de Paris X
Nanterre

Membres du jury :

M. Rémy HERNU

Professeur de droit communautaire à l'Université de
Valenciennes

M. Régis CHEMAIN

Maître de conférences de droit communautaire à l'Université de
Paris X Nanterre, Rapporteur

M. Philippe GUTTINGER

Maître de conférences (HDR) à l'Université Paris X, Rapporteur

J'adresse mes remerciements à Monsieur Jean-Marc THOUVENIN pour ses conseils dans la poursuite et la conduite de mes travaux.

Toute ma gratitude à ma famille sans qui rien n'aurait été possible et mes remerciements à tout ceux qui m'ont soutenu par devers tout Une Mention spéciale à mes parents, ma famille et à tous ceux qui ont contribué de manière directe ou indirecte à la réalisation de ces travaux.

Enfin je dédie cette thèse à mes enfants présents et à venir, que le cyberspace puisse être pour eux un endroit et lieu plus sûrs.

**LA PROTECTION DU MINEUR DANS
LE CYBERESPACE**

INTRODUCTION

PREMIERE PARTIE : LES DROITS ET OBLIGATIONS DU MINEUR DANS LE CYBERESPACE

TITRE 1. LES DROITS ET LIBERTÉS FONDAMENTAUX DU MINEUR DANS LE CYBERESPACE

Chapitre 1. LES DROITS INDIVIDUELS DU MINEUR DANS LE CYBERESPACE

§1. Les données personnelles du mineur dans le cyberspace

§2. Le droit à la vie privée du mineur.

Chapitre 2. LES LIBERTÉS INDIVIDUELLES DU MINEUR DANS LE CYBERESPACE

§1. La liberté d'expression du mineur dans le cyberspace

§2. Les droits d'auteur du mineur dans le cyberspace

Titre 2. LA SANCTION JURIDIQUE DES DROITS ET OBLIGATIONS DU MIENUR DANS LE CYBERESPACE

Chapitre 1. LA CAPACITÉ JURIDIQUE DU MINEUR DANS LE CYBERESPACE

§1. Le contrat électronique conclu par un mineur

§2. La responsabilité du mineur découlant de l'exercice de ses droits et libertés fondamentaux dans le Cyberspace

Chapitre 2. LA SANCTION DES MANQUEMENTS DU MINEUR AUX DROITS ET OBLIGATIONS D'AUTRUI DANS LE CYBERESPACE

§1. Les infractions liées au statut d'auteur ou d'éditeur de contenus du mineur

§2. La criminalité informatique du mineur

DEUXIÈME PARTIE : LES DROITS ET OBLIGATIONS DES TIERS Á L'ÉGARD DU MINEUR DANS LE CYBERESPACE

Titre 1. LES TUTEURS LÉGAUX RESPONSABLES DES MINEURS

Chapitre 1. LES MOYENS DE PROTECTION DU MINEUR DANS LE CYBERESPACE

§1. La protection *a priori* du mineur dans le cyberspace

§2. La protection *a posteriori* du mineur dans le cyberspace

Chapitre 2. LA RESPONSABILITÉ DES TUTEURS LÉGAUX DU FAIT DES MINEURS

§1. La responsabilité civile des tuteurs légaux du mineur

§2. La responsabilité pénale des tuteurs légaux du mineur

Titre 2. LES TIERS RESPONSABLES DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE

Chapitre 1. LA RESPONSABILITÉ DES INTERMÉDIAIRES DU FAIT DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE

§1. Le régime de responsabilité de droit commun des intermédiaires techniques du cyberspace

§2. Le régime spécifique de la responsabilité des intermédiaires techniques dans le cyberspace : *La Loi pour la Confiance dans l'Economie Numérique (LCEN)*

Chapitre 2. LA RÉPRESSION DE LA CRIMINALITÉ CONTRE LES MINEURS DANS LE CYBERESPACE

§1. La cybercriminalité à l'encontre des mineurs

§2. La sanction des cybercriminels

CONCLUSION

PRINCIPALES ABRÉVIATIONS

AAARGH	Association des anciens amateurs de récits de guerre et d'holocauste
ADAMI	Administration des droits des artistes et des musiciens interprètes
ADSL	Asymmetric Digital Subscriber Line
AFA	Association de fournisseurs d'accès
AGESSA	Association pour la gestion de la sécurité sociale des auteurs
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Network
Art.	Article
B2i	Brevet informatique et Internet
BRCI	Brigade centrale pour la répression de la criminalité informatique
CA	Cour d'appel
Cass.	Cour de cassation
Cass. Crim.	Chambre criminelle de la Cour de cassation
CDA	Communication decency act
CE	Conseil d'Etat
CE	Communautés Européennes
CEDH	Cour Européenne de Droits de l'Homme
Civ. 1 ^{ère}	Première chambre civile de la Cour de cassation
CLEMI	Centre de liaison et de l'enseignement et des médias d'information
Coll.	Collection
Com. com. électr.	Commission du commerce électronique
CNIL	Commission Nationale Informatique et Libertés
COPA	Child online protection act
CPPA	Child pornography prevention act
CPI	Code de propriété intellectuelle
CREDOC	Centre de recherche pour l'étude et l'observation des conditions de vie
CSA	Conseil supérieur de l'audiovisuel
D.	Recueil Dalloz
DGPN	Direction générale de la police nationale
DNRABP	Division nationale de la répression des atteintes aux biens et aux personnes

ECPAT	End child pornography and trafficking
EEE	Espace Economique Européen
FAI	Fournisseurs d'accès Internet
FAQ	Frequently asked questions
FTC	Federal Trade commission
HALDE	Haute autorité de lutte contre les discriminations et pour l'égalité
HTML	Hypertext Mark-Up Language
HTTP	Hypertext Transfer Protocol
Gaz pal	Gazette du palais
GOR	Groupe d'opération de recherche
IAC	Interactive age check
ILO	International labour organization
IRCGN	Institut de recherche criminelle de la gendarmerie nationale
IWF	Internet watch foundation
IP	Internet Protocol
IFCLA	International Federation of Computer Law Association
IRC	Internet relay chat
ICQ	I seek you
JCP	Jurisclasseur périodique (La Semaine juridique)
JO ou JORF	Journal officiel de la République française
JOCE	Journal officiel des Communautés européennes
JUDEX	Système JUDiciaire de Documentation et d'EXploitation
LCEN	Loi pour la confiance dans l'économie numérique
MIT	Massachussetts Institute of Technology
MODEM	Abréviation MOdulateur/DEModulateur
NTI	Nouvelles technologies de l'information
NTIC	Nouvelles technologies de l'information et de la communication
NUA	Network user adress
OCDE	Organisation de coopération et de développements économiques
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
PANAM	Service des Personnes âgées, mineurs et atteintes aux mœurs
P2P	Peer to Peer

PUF	Presses universitaires de France
QFP	Questions fréquemment posées
RFDA	Revue française de droit administratif
RIDA	Revue internationale de droit administratif
TCI	Transmission Control Protocol
TGI	Tribunal de grande instance
TI	Tribunal d'instance
UISE	Union internationale de secours aux enfants
UNAF	Union nationale des associations familiales
SCCP	Société civile des producteurs phonographiques
SITT	Service de l'informatique et des traces technologique
STRJD	Service technique de recherche judiciaire et de documentation
UCLA	University of California in Los Angeles
URL	Uniform Resources Locator
WWW	World Wide Web

INTRODUCTION

Internet est considéré à ce jour comme la plus grande invention du millénaire. Internet constitue une avancée considérable, comparable aux inventions telles que l'imprimerie ou le téléphone¹. C'est une véritable révolution, qui n'a épargné aucun domaine. L'ampleur de son influence sur tout et tous laisserait croire que l'on peut tout faire sur : faire ses courses en lignes (denrées alimentaires, vêtements, mobiliers, etc.); faire certaines démarches administratives en ligne comme remplir sa déclaration annuelle de revenus, télécharger des formulaires administratifs. On peut acheter, payer en ligne, faire des recherches, lire son journal, écouter et/ou télécharger de la musique, communiquer, faire de la politique, apprendre (des systèmes de cours particulier en ligne se développent), etc. Tout semble possible dans le cyberspace, le meilleur comme le pire. L'internaute n'est soumis à aucune contingence spatio-temporelle. Internet est ouvert 24h/24, toute l'année sans aucune interruption, et fait fi des fuseaux horaires. Internet tient ces caractéristiques de sa genèse.

Internet doit sa création aux militaires, il révolutionnera par la suite le monde de la recherche scientifique. Par la suite Internet s'est affranchi de ses créateurs, s'est banalisé et, ce faisant a affecté toute la société dans ses multiples formes et secteurs.

On estime que le nombre d'internautes a dépassé le cap du milliard en 2005². Computer Industry Almanach³ estimait précisément à 934 millions⁴ le nombre de personnes connectées

¹ Richard Swetenham, « Le plan d'action pour une utilisation plus sûre d'Internet », Société de l'information, NTI et Union européenne, Revue du Marché commun et de l'Union européenne n°436 mars 2000, p.161.

² Arnaud Dufour, Solange Ghernaouti_Hélie, Internet, Que sais-je ? PUF 2006, p.11

³ Voir Computer Industry Almanach, www.c-i-a.com

⁴ 70,88% de ces 934 millions d'internautes sont regroupés dans 15 pays, le top 15 :

1/ Etats-Unis	185.550	soit 19,86% ;
2/ Chine	99.800	soit 10,68% ;
3/ Japon	78.050	soit 8,35% ;
4/ Allemagne	41.880	soit 4,48% ;
5/ Inde	36.970	soit 3,96%
6/ Royaume-Uni	33.110	soit 3,54%
7/Corée du Sud	31.670	soit 3,39%
8/ Italie	25.530	soit 2,73%

à Internet en décembre 2004. Selon la même source, ce nombre devrait atteindre 1,35 milliard en 2007. En France, les instituts d'analyse de marché situent le nombre d'internautes à environ 25 millions pour le second trimestre 2005⁵. Le vocable Internet recouvre plusieurs activités. Les qualifications d'Internet sont à adapter selon la matière traitée.

I/ Les qualifications d'Internet

Internet est une révolution technique et sociale du fait qu'il n'a épargné que très peu de domaines de la société. L'informatique, les médias, les modes de communication entre les personnes, etc. Une seule définition d'Internet ne suffirait pas à couvrir les multiples aspects de cet outil. Internet a une implication technique, sociale et juridique avec des répercussions dans chacun de ces domaines dont les définitions d'Internet doivent tenir compte.

A. Qualification générique

Le terme Internet fait communément référence au réseau de couverture mondiale qui rassemble utilisateurs et systèmes informatiques. Ce réseau offre des services de mise en relation et de transfert de données entre des entités distantes. Il permet d'accéder à des données informatiques, de les partager, et de réaliser de nombreux services reposant sur le transfert d'informations⁶. C'est une technique qui facilite les communications et les relations entre internautes.

9/ France	25.470	soit 2,73%
10/ Brésil	22.320	soit 2,39%
11/ Russie	21.230	soit 2,27%
12/ Canada	20.450	soit 2,19%
13/ Mexique	13.880	soit 1,49%
14/ Espagne	13.440	soit 1,44%
15/ Australie	13.010	soit 1,39%

Source : NUA, <http://www.c-i-a.com/pr0904.htm>

⁵ Voir à ce sujet la synthèse tenue à jour par le Journal du Net, <http://www.journaldunet.com/chiffres-cles.shtml>, ou consulter les publications et études réalisées en France par le Benchmark Group, www.benchmark.fr

⁶ Arnaud Dufour, Solange Ghernaouti_Hélie, Internet, Que sais-je ? PUF 2006.

B. Qualification technique

Internet est l'acronyme de l'expression anglaise « *internetworking of networks* ». Acronyme qui deviendra par contraction Internet. Internet n'est pas uniquement un réseau mais plutôt un ensemble de réseaux qui, par le biais d'un langage commun, parvient à faire communiquer tous les outils de la technologie numérique⁷. Il s'appuie sur un protocole de communication qui permet aux ordinateurs connectés du monde entier, d'échanger des données. La connexion et la transmission de ces données sont assurées par l'intermédiaire des lignes téléphoniques. Il ne faudrait pas pour autant assimiler Internet au réseau téléphonique ; les ordinateurs échangent des données numériques, tandis que les lignes téléphoniques ne véhiculent que des signaux analogiques (son, voix). D'où la nécessité d'un Modem (Modulateur – Démodulateur) qui convertit le numérique en analogique et inversement⁸. Le Modem est l'un des instruments de la banalisation d'Internet. Avec la banalisation d'Internet auprès des profanes, la question de la régulation juridique d'Internet est apparue et n'a cessé de se poser depuis.

C. Qualification juridique

Internet est un service de communication qui regroupe plusieurs fonctionnalités lui permettant d'être défini comme tel. La qualification juridique d'Internet n'est pas globale. Les fonctionnalités d'Internet sont régies de manière sectorielle par des textes juridiques spécifiques. Selon la fonctionnalité concernée d'Internet, sa qualification juridique nécessitera une adaptation.

1. Internet est un service commercial.

Les personnes morales et physiques réalisent de nombreux échanges commerciaux et financiers par le biais du réseau Internet. Le commerce électronique (e-commerce pour *electronic commerce* ou cybercommerce) y a une grande importance et, ne se limite pas à la

⁷ Philippe Bouré, Le droit et Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002, p.7-8.

⁸ Le Monde 19 avril 2000, Jean-Michel Maman.

seule vente en ligne. Il recouvre l'ensemble des activités liées à l'achat en amont de la vente (publicité, marketing, préparation de l'achat, aide à la décision, comparaison des prix, etc.) ; pendant la vente (catalogue, sélection et configuration des produits, paiements en ligne, etc.) ; ou en aval de la vente (service après vente, support technique, etc.)⁹. La qualification juridique d'Internet dans ce cas de figure est celle qui correspond au commerce avec des adaptations nécessaires eu égard aux caractéristiques spécifiques du commerce en ligne, c'est le cas par exemple s'agissant des textes régissant les contrats électroniques.

2. Internet est un multimédia ou hypermédia¹⁰.

Il faut entendre par là que, c'est un support unique qui permet la diffusion de plusieurs médias, de manière associée (image et son, texte et son...), ou dissociée (texte seul, image seule...). L'unanimité n'est pas de mise lorsqu'il s'agit de qualifier Internet de média. La difficulté en la matière tient à la diversité de ses applications. Ces diverses applications relient Internet à plusieurs cadres juridiques jusque là hermétiques les uns aux autres. La nature d'Internet génère une cohabitation de plusieurs cadres juridiques ce qui a pour résultat de donner naissance à de nouveaux cadres, de nouvelles qualifications juridiques.

- La messagerie électronique, les forums de discussion et les chats sont des applications qui permettent l'échange de messages, fichiers en différé comme en simultané. La qualification juridique à retenir est celle de la communication privée ou publique. La communication privée entre individus par courrier électronique s'apparente au courrier postal traditionnel et tombe dans le cadre de la Loi postale.
- La téléphonie par Internet est une alternative à la téléphonie traditionnelle et devrait tomber sous le coup de l'application de la loi sur les télécommunications.
- Les sites de presse écrite, la diffusion d'informations sur Internet quel qu'en soit le support (blogs, sites et pages personnel, etc.) peuvent être assimilés à l'activité traditionnelle de la presse. Ils devraient se voir appliquer la loi de 1881 qui réglemente le statut de la presse. Internet est un outil permettant d'éditer et de diffuser de

⁹ Arnaud Dufour, Solange Ghernaouti-Hélie, Internet, Que sais-je ? PUF 2006.

¹⁰ Philippe Bouré, Le droit et Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002, p.14.

l'information simplement et rapidement gratuitement ou non par le biais de différents supports : forums, sites personnalisés, blogs, pages spécialisées, etc. La qualification juridique d'Internet dans ce cas s'aligne (avec quelques adaptations) sur la législation sur la presse.

- Les radios et télévisions se multipliant sur la Toile, dépendent quant à elles du régime de la loi de 1986 telle que modifiée par la loi du 1^{er} août 2000 et qui détermine le cadre de la communication audiovisuelle¹¹. De l'avis de Philippe Bourré, reconnaître à Internet le statut de média reviendrait à : remettre en cause l'ensemble des statuts respectifs auxquels il est rattaché ; dissoudre des cadres juridiques dans un droit uniformisé applicable à toutes les entreprises sans tenir compte de leurs spécificités respectives¹². Dans le même temps il milite pour une qualification juridique d'Internet comme média audiovisuel, qui le rapprocherait du statut opposable aux entreprises de radios et de télévisions¹³.

II/ La naissance et l'évolution d'Internet

A. La genèse

C'est aux Etats-Unis que l'idée d'un réseau mondial utilisant la technique de la commutation de paquets va naître. En **1957**, le Ministère de la défense américaine crée l'agence ARPA (Advanced Research Project Agency) dont l'objectif est de renforcer les développements scientifiques susceptibles d'être utilisés à des fins militaires¹⁴. Dans une autre version, la paternité d'Internet est attribuée aux militaires. Les Etats-Unis souhaitent réagir au lancement du premier vaisseau spatial Spoutnik par les Soviétiques. L'objectif des Américains était de dominer l'URSS sur le plan de la télécommunication. En pleine Guerre froide les moyens de communication existants étaient basés sur la technologie des réseaux téléphoniques centralisés. Une attaque nucléaire sur les points névralgiques aurait rendu

¹¹ Ibid., p.15.

¹² Ibid.

¹³ Il dit pour soutenir cette idée que, « *tout comme la radio ou la télévision, interne permet aux utilisateurs de se divertir, de s'informer, de s'instruire par le biais d'un appareil de réception prévu à ces usages au travers de millions de sites amateurs ou professionnels qu'il présente* », Philippe Bourré, Le droit et Internet, préc., p.15.

¹⁴ Philippe Bouré, Le droit et Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002, p.8.

l'utilisation du réseau impossible. Les chercheurs américains avaient pour mission de proposer à l'armée un moyen de mettre en place un réseau de communication militaire capable de résister aux attaques nucléaires.

En **1969**, des chercheurs réussissent à relier entre eux quatre des ordinateurs de l'Université de Californie (UCLA : University of California in Los Angeles). C'est la naissance de l'Arpanet. Afin de donner une portée universelle à ce nouveau réseau, il était nécessaire de mettre au point un langage qui puisse être commun à l'ensemble des ordinateurs qui viendraient enrichir le réseau. A cette fin est créé en **1974** Internetnetwork Working Group dont la mission consistait à élaborer le protocole commun requis. Le fruit de ces recherches sera la création du TCP-IP (*Transmission Control Protocol, Internet Protocol*), véritable point de départ d'Internet contemporain¹⁵. L'accessibilité à l'ensemble des citoyens a été facilitée par la simplification de l'instrument informatique grâce, notamment à la création en **1989** du World Wide Web (www)¹⁶. Le www est la réunion de trois éléments fondamentaux que sont :

- le protocole d'hypertexte « *Hypertext Transfer Protocol* » symbolisé par les initiales « http ». Cela correspond à un standard permettant aux ordinateurs de lier les documents entre eux ;
- le « Uniform Ressources Locator » ou URL, est le standard permettant de trouver un document en tapant simplement une adresse ;
- le langage HTML (Hypertext Markup Language) rend possible la création de documents multimédias sur le net tout en les reliant grâce à l'HyperText¹⁷.

En **1991**, Gopher voit le jour. C'est une nouvelle application permettant la publication de documents sur Internet. En l'espace de quelques mois des centaines de serveurs Gopher sont mis en place dans les universités et les bibliothèques du monde entier. Cet outil aujourd'hui disparu a grandement facilité l'accès à l'information et aux applications Internet. Il a ouvert la

¹⁵ . Philippe Bouré, Le droit et Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002

¹⁶ C'est le physicien Tim Berners-Lee qui va élaborer le World Wide Web dont les initiales correspondent aux www utilisées devant l'adresse de certains sites Internet.

¹⁷ Philippe Bouré, Le droit et Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002.

voie aux notions de navigation et de liens entre les documents répartis sur un ensemble de serveurs¹⁸.

En **1993**, le NCSA MOSAIC est distribué gratuitement. Il s'agit d'une interface permettant au grand public de naviguer sur le réseau mondial. Ce logiciel aujourd'hui connu sous l'appellation de « Netscape » sera utilisé majoritairement par les internautes jusqu'à son remplacement par le logiciel Microsoft : « Internet explorer » qui est pré installé sur l'ensemble des ordinateurs personnels vendus dans le monde¹⁹.

L'Institut Forrester Research prévoyait 50 millions d'internautes à la fin du XXe siècle mais en 2000, ils seront chiffrés à plus de 250 millions²⁰.

B. Les arrière-pensées de la création d'Internet

L'objectif initial d'Internet était de permettre aux Etats-Unis de se prémunir contre une attaque nucléaire, en permettant le transport d'informations par paquets à même de se reconstituer à l'arrivée²¹. La paternité d'Internet est militaire²² et universitaire. « La présence d'anciens chercheurs universitaires à des postes de gestion a permis au net de se développer selon des principes d'autogestion, caractéristique du monde scientifique²³. Pour résumer, Internet a été conçu pour n'être qu'un moyen de communication au service de l'armée américaine, mais il sera rapidement « colonisé » par les chercheurs et les étudiants, avant d'être annexé par toute la planète.

¹⁸ Arnaud Dufour, Solange Ghernaouti_Hélie, Internet, Que sais-je ? PUF 2006.

¹⁹ Ibid.

²⁰ Etude Forrester Research et Informatiques Magazine, juillet-août

²¹ Des « routeurs », qui sont attachés à l'ordinateur de départ et aux différents nœuds dans le réseau jouent en quelque sorte le rôle d'aiguilleur ; chaque router choisit d'envoyer le message à un ordinateur de stockage (serveur) correspondant. Un message est découpé en morceaux ou « paquets », et ces morceaux peuvent très bien arriver à destination par des routes différentes, pour être rassemblés à l'arrivée, Richard Swetenham, « Le plan d'action pour une utilisation plus sûre d'Internet », Société de l'information, NTI et Union européenne, Revue du Marché commun et de l'Union européenne n°436 mars 2000, p.161.

²² Sur les origines militaires d'Internet, voire Ch. Huitema, Et Dieu créa Internet, Eyrolles 1999, p. 59 et s.

²³ P. Himanen, L'Ethique hacker et l'esprit de l'ère de l'information, Exils Editeur 2001, p. 172.

C. L'évolution technique et idéologique d'Internet

Internet devait être une arme technologique déjouant toute attaque nucléaire et rendant impossible la destruction du réseau de communication américain grâce à la conception technique d'Internet imaginé comme une hydre. Les messages diffusés par ce biais étaient transportés en petits paquets individuels représentant les multiples têtes de l'hydre ; ces petits paquets devaient suivre des routes différentes et ne reconstituer le message initial qu'à destination. Ainsi le message dans sa globalité ne pouvait être intercepté puisque dématérialisé. Il n'existait plus de point névralgique du message, ce faisant ce dernier devenait quasiment « invulnérable ».

Au fil du temps, Internet est devenu un outil de la recherche scientifique à part entière. Il a effacé les contingences spatio-temporelles entre les chercheurs, en leur permettant à moindre coût et de manière quasi instantanée d'échanger sur leurs travaux, leurs recherches. Internet a intégré cette capacité d'adaptation à tous les usages et à tous les usagers.

La vulgarisation d'Internet a coïncidé avec un développement exponentiel. Dans un laps de temps très court, des individus, des groupes, des organisations se sont appropriés cet outil comme un moyen alternatif de communication et d'échange de renseignements. De nouveaux usages et utilisations en ont vite découlés²⁴.

L'innovation technologique d'Internet s'est doublée d'une évolution idéologique ayant des incidences sur son fonctionnement. Internet est le produit d'une période de l'histoire qui lui a imprimé des marques caractéristiques, et dont-il a du mal à se défaire ou plutôt dont-on a du mal à le défaire. Réseau décentralisé non hiérarchisé, vecteur de l'idéologie libérale par opposition à la conception de centralisme dans laquelle le pouvoir était concentré (selon le modèle soviétique où toute diffusion d'information était contrôlée par le pouvoir). Un esprit libertaire sous-tend depuis l'origine l'existence et le fonctionnement d'Internet²⁵.

²⁴ UNESCO, Les Droits de l'homme dans le cyberspace, Collection Droit du cyberspace, Paris Economica, Unesco 2005, Préface de Henk A.M.J. ten Have (Directeur de la Division de l'éthique des sciences et des technologies, UNESCO)

²⁵ S'agissant de cet esprit libertaire qui aurait prévalu à la création d'Internet, Philippe Bouré semble ne pas adhérer totalement à cette idée. Selon lui, le Politique a été présent dès l'origine d'Internet. Voir l'introduction de son ouvrage « Le droit et Internet. Les enjeux présents et futurs de la société de l'information », 1ère édition L'Hermès. Il cite pour ce faire Serge Regourd en disant que, l'étude historique qui suit a pour vertu « de faire

Actuellement Internet est toujours décentralisé. Il n'existe pas de réglementation unique d'Internet, celles existantes ne sont pas toujours convergentes. Il n'existe pas de hiérarchie unique et commune reconnue comme telle dans le cyberspace. Les plus fervents des internautes ont du mal à accepter toute limitation de liberté, *a fortiori* toute incursion du droit jugée intrusive dans le cyberspace. La Netiquette à leurs yeux, devrait être la seule règle ayant cours dans le cyberspace.

III/ Les enjeux d'Internet

L'évolution d'Internet, bien qu'elle doive l'essentiel de son envergure aux évolutions technologiques ne s'y limite pas. Les enjeux en cause vont au-delà de sa seule dimension technique.

A. Les enjeux techniques

On se réfère au réseau en parlant du concept d'autoroute de l'information. Ce concept intègre la mise à disposition au public via des infrastructures de communication à haut débit, d'un ensemble de services publics ou marchands. Dans un premier temps ce concept était dissocié d'Internet. Contrairement à ce qui avait été imaginé, ce ne sont pas les services de visiophonie ou de téléphonie numérique qui ont permis au réseau de se développer, mais plutôt les services de publication d'information (le Web) et de communication (la messagerie électronique)²⁶. Le succès d'Internet repose, du point de vue des infrastructures, sur sa capacité à exploiter celles existantes, sans exiger la mise en place de nouvelles lignes.

B. Les enjeux politiques

L'un des plus gros enjeux du développement d'Internet tient à la maîtrise des technologies numériques. Internet bénéficie d'une surexposition médiatique face au téléphone mobile qui a paradoxalement connu dans la même période un développement deux fois plus important²⁷

apparaître comme axe problématique constant cette surdétermination du politique sur les processus d'édiction des règles juridiques à ce domaine ».

²⁶ Arnaud Dufour, Solange Ghernaouti-Hélie, Internet, Que-sais-je ? PUF 2006, p. 99.

²⁷ La barre de deux milliards de téléphones mobiles utilisés dans le monde a été franchie en 2005.

sans susciter autant l'attention²⁸ générale. Cette "surmédiatisation" s'explique partiellement par la complexité d'Internet. Le développement très rapide d'Internet s'appuie sur l'utilisation d'infrastructures existantes. Une légitimation n'était pas nécessaire dans le cadre de l'intervention et de la planification de l'Etat dans le cadre de la mise en place de l'accès universel²⁹ à Internet. Il semble acquis aujourd'hui que le rôle de l'Etat se situe plutôt dans l'encadrement d'Internet que dans l'interventionnisme absolu.

C. Les enjeux éthiques

Internet est un réseau transnational qui se joue des contingences géographiques et frontalières. Le caractère mondial du réseau en a fait un lieu de rencontres où s'affrontent parfois une multitude de cultures, auxquelles sont associées autant d'éthiques³⁰. L'éthique a plusieurs dimensions ; elle ne recouvre pas les mêmes valeurs partout et pour tous. Selon la localisation géographique, des agissements seront jugés ou appréhendés différemment s'agissant d'Internet. Cette prise en considération éthique a un impact important dans la gestion internationale de conflits générés par le cyberspace ou la gestion de la cybercriminalité.

D. Les enjeux juridiques

Avec la vulgarisation d'Internet, la question de la réglementation de cet outil s'est très vite posée. L'idéologie libertaire qui a sous-tendu la création d'Internet entendait en faire un espace de liberté par excellence ou la vigilance mutuelle des usagers du réseau, les règles de bonnes conduites, en somme la Netiquette serait la règle. L'autorégulation devait suffire à réglementer les échanges des internautes dans le cyberspace. Cette volonté affichée par la communauté du cyberspace a pu entraîner certaines personnes, peu au fait de la régulation du réseau à parler de « vide juridique ». Cette assertion leur a valu les foudres des spécialistes. On peut affirmer sans grand risque que cette conclusion était et est toujours inexacte. Tous les acteurs d'Internet que ce soit des personnes physiques ou morales résident dans un pays

²⁸ Arnaud Dufour, Solange Ghernaouti-Hélie, Internet, Que-sais-je ? PUF 2006

²⁹ On a cru dans un premier temps que, l'accès aux services des autoroutes de l'information nécessiterait des infrastructures techniques lourdes et coûteuses. Dans ce contexte, l'Etat devait jouer un rôle moteur dans la mise en place des réseaux et dans la fourniture gratuite d'un accès pour tous.

³⁰ Arnaud Dufour, Solange Ghernaouti-Hélie, Internet, Que-sais-je ? PUF 2006, p.107.

déterminé ; ils sont donc soumis aux lois en vigueur dans le pays concerné³¹ indépendamment du fait qu'il s'agisse de vie virtuelle. Des droits spéciaux seront adaptés aux différentes fonctionnalités d'Internet.

La doctrine de manière unanime a pointé l'inexactitude de cette affirmation en soutenant qu'Internet n'était en aucun cas à l'abri de l'application du droit positif³². Bien loin de cette idée reçue, il n'est pas exagéré d'affirmer qu'Internet souffre au contraire d'un excès de législations applicables³³. Le chevauchement de législations s'explique par plusieurs éléments.

- Au niveau national, il est à noter que Internet se situe aux confluent de diverses techniques de communication permettant d'effectuer des activités aussi diverses que la distribution de courrier, la télévision, le commerce, la téléphonie, l'édition, etc. Il est susceptible selon l'activité concernée de nécessiter l'application d'une ou plusieurs de ces législations.
- Au niveau international, Internet se jouant des frontières physiques peut voir les activités des internautes incriminées simultanément dans plusieurs Etats ; ces derniers peuvent légitimement se saisir du litige et mettre en œuvre leur législation respective dans des décisions contradictoires.

Quoi qu'il en soit, les enjeux juridiques de la naissance et du développement du cyberspace peuvent s'articuler autour de trois points essentiels :

- l'application du droit dans le cyberspace
- la question de l'application du droit commun ou d'un droit spécifique au cyberspace
- la question du choix de la législation dans des litiges de dimension transnationale.

³¹ Richard Swetenham, « Le plan d'action pour une utilisation plus sûre d'Internet », Société de l'information, NTI et Union européenne, Revue du Marché commun et de l'Union européenne n°436 mars 2000, p.161.

³² Cf. par exemple « Internet serait-il un no man's land juridique ? Lamy droit de l'informatique, n° 81 mai 1996 B p.1 ; « Du droit applicable dans le « village planétaire », au titre de l'usage immatériel des œuvres » par Pierre-Yves Gautier, D.1996 I p.131 ; « Des réseaux aux autoroutes de l'information : Révolution technique ? Révolution juridique ? Par F. Olivier et E. Barbery, J.C.P. 1996 éd. G I n° 3926.

³³ Voir le site Le Chêne & le Gland, Droit et Internet, « Fourniture d'accès à Internet et responsabilité pénale », <http://www.canevet.com/doctrine/resp-fai.htm>

IV/ Les services et applications d'Internet

Le réseau Internet offre une multitude de services aux utilisateurs, la seule condition étant d'être équipé d'un ordinateur, d'être relié au réseau et de disposer de logiciels adéquats.

A. La messagerie électronique

La messagerie électronique permet un échange de messages textuels entre deux ou plusieurs internautes, par le biais d'une boîte aux lettres et d'une adresse électronique toutes deux individuelles. Les boîtes aux lettres sont hébergées sur des serveurs de messagerie (Hotmail, Yahoo, AOL, etc.). Ils fonctionnent 24 heures sur 24 et peuvent recevoir ou envoyer des messages en permanence. La messagerie est un outil asynchrone.

B. La messagerie instantanée

C'est un service de messagerie qui constitue une extension de la boîte et de l'adresse électroniques de l'internaute. Ce service permet à l'internaute de communiquer en temps réel et de manière instantanée avec des interlocuteurs qui ont été préalablement déterminés souvent à partir du répertoire de la messagerie initiale. La messagerie instantanée (MSN, Yahoo, etc.) peut être textuelle, vidéo et/ou audio. Il est possible grâce à une Webcam et à un microphone de faire une visioconférence.

C. Les chats et forums de discussion

Ce sont des espaces de libre échange sur le web, entre des internautes qui ne se connaissent pour la plupart pas. Ils se retrouvent autour d'un thème qui les intéresse tous. Il s'agit de conversations simultanées avec des interlocuteurs ayant la particularité de s'abriter derrière des pseudonymes. Ces conversations instantanées ont un caractère très volatile et sont considérées pour la plupart comme des communications publiques puisque les interlocuteurs ne sont pas prédéfinis. Une nuance est à apporter s'agissant des chat-room notamment

lorsqu'il s'agit d'apartés entre des interlocuteurs d'un chat souhaitant avoir une conversation "privée", ce type de conversation pourrait alors s'apparenter à une communication privée.

D. Les moteurs de recherche

Ce sont des outils de recherche d'Internet. A partir de mots clefs définis par l'internaute, les moteurs de recherche se chargent de scanner le cyberspace pour ressortir les résultats classés par pertinence.

E. Les blogs

Il s'agit de pages personnelles ou d'un nouveau genre de journal intime en ligne. Ce journal peut se résumer en des textes seuls ou des textes accompagnés d'illustrations. La popularité et l'explosion des blogs s'expliquent par le fait que leur gestion ne nécessite que très peu de connaissances techniques.

F. Le commerce électronique

Le développement du réseau Internet a été accéléré par « l'intrusion » de l'économie et plus précisément par l'avènement du commerce en ligne. Internet est très vite une immense vitrine mondiale. Les relations qui se nouent via les réseaux numériques³⁴ font fi des notions d'espace et de temps, des territoires et des frontières étatiques. Les échanges sont quasiment instantanés et ne nécessitent comme outils qu'un ordinateur et une connexion au réseau, quel que soit l'endroit où l'on se situe dans le monde. L'évolution du commerce électronique parallèlement à Internet est telle qu'il est fréquemment identifié à Internet bien que ce dernier propose de multiples autres services.

³⁴ Mission interministérielle sur Internet présidée par I. Falque-Pierrotin, Internet Enjeux juridiques : La documentation française, Paris 1997. – Rapport du Conseil d'Etat, Internet et les réseaux numériques : La documentation française, Paris 1998, étude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998.

V/ Le cyberspace : le territoire d'Internet

A. Définition du cyberspace

Qu'est ce que le cyberspace ? « On parle fréquemment, par opposition au monde réel, ou physique³⁵, du cyberspace (cyberespace en français). Le mot cyberspace est la contraction du préfixe cyber et du mot espace. Le préfixe « cyber » est emprunté au terme « cybernétique », créé à partir du grec *kubernêsis* qui signifie au sens propre « l'action de diriger ou de gouverner »³⁶. Le terme cybernétique a été popularisé en 1948 par le mathématicien américain Norbert Wiener³⁷. Il définissait la cybernétique comme l'étude de la commande et de la communication chez l'animal et dans la machine³⁸. Le mot cyberspace a formellement été créé en 1984 par William Gibson dans son roman « Neuromancien »³⁹. « Le cyberspace est constitué, d'une part, de personnes de tous pays, de toutes cultures et de toutes langues, de tous âges, de toutes professions, qui offrent et demandent des informations et, d'autre part, d'un réseau mondial d'ordinateurs interconnectés grâce aux infrastructures [convertissant] sous forme numérique les informations offertes et demandées »⁴⁰.

B. Les "citoyens " du cyberspace

On entend par citoyens du cyberspace ou internautes tous les acteurs qui interagissent sur la Toile. Contrairement à la définition dans la vie réelle, être citoyen ne suppose aucune condition d'âge, de nationalité, etc. Toute personne qui dispose d'une connexion Internet et qui en fait usage est un cybernaute à part entière. Tout le monde peut surfer plus ou moins librement dans le cyberspace à condition de respecter les règles juridiques régissant la matière. Le cyberspace n'est en aucun cas constitutif d'un vide juridique qui rejaillirait sur ses utilisateurs.

³⁵ P.Y Gautier ; De la prescription des infractions commises sur Internet...et dans le monde physique : D.2002, chron. p.1852.

³⁶ Olivier Iteanu, Tous cybercriminels, Jacques-Marie Laffont Editeur 2004, p.21.

³⁷ C'est un mathématicien qui a jeté les bases d'une science nouvelle destinée à couvrir tous les phénomènes mettant en jeu des mécanismes de traitement de l'information. Norbert Wiener, *Cybernetics or control and communications in the animal and the machine*, 1948.

³⁸ Ses travaux visaient à savoir comment les messages étaient transmis et reçus, tant au travers des machines que dans me système nerveux animal.

³⁹ A. Lepage, *Libertés et droits fondamentaux à l'épreuve d'Internet* : Litec, p.3

⁴⁰ Les dimensions internationales du droit du cyberspace ; Collection droit du cyberspace

C. Le mineur dans le cyberspace

Le mineur dans le cyberspace est défini selon les mêmes conditions que le mineur en droit réel. Il est communément admis que c'est l'individu âgé de moins de dix-huit ans. La difficulté repose dans l'identification du mineur comme tel sur Internet. L'anonymat joue un rôle prépondérant dans le cyberspace notamment sur les comportements des internautes. Les internautes s'imaginent souvent à tort pouvoir se dissimuler impunément dans les interstices du cyberspace. Cette dissimulation englobe la dissimulation de son identité réelle derrière une ou de multiples identités virtuelles (les pseudos) ; la dissimulation de ses activités, etc.

L'identification du mineur pose de réels problèmes s'agissant de son utilisation d'Internet, quelque soit le point de vue que l'on prend en considération. Partant du postulat que le mineur est un acteur à part entière du cyberspace, il a des droits et des obligations qui régissent son utilisation de cet outil (**Première Partie**). La nuance devra être apportée sur l'étendue de ces droits et obligations en concordance avec la spécificité de son statut juridique et de la nature intrinsèque d'Internet. Par ailleurs, le mineur engage par son fait et du fait des préjudices dont il est la victime dans le cyberspace des responsabilités (**Deuxième Partie**) de différents acteurs directs ou non d'Internet.

PREMIERE PARTIE : LES DROITS ET OBLIGATIONS DU MINEUR DANS LE CYBERESPACE

L'avènement des nouvelles technologies, a constitué à n'en pas douter une révolution pour tous. Agathe Lepage dans son ouvrage « Libertés et droits fondamentaux à l'épreuve d'Internet⁴¹ », se référant à cet avènement parle de « l'onde de choc d'Internet ». Internet de son point de vue « semble avoir conquis droit de cité en apportant avec lui son lot d'innovations voire, certains n'hésiteront pas à le proclamer, de révolutions [...] de nombreux domaines de la pensées ont été vivifiés par leur rencontre avec Internet »⁴².

La vocation du droit à s'appliquer à Internet est désormais un fait avéré ; il demeure cependant une interrogation quant à savoir s'il doit lui être appliqué un droit spécifique se démarquant du droit préexistant⁴³.

Tout virtuel qu'on le définisse, le cyberspace constitue un lieu où se nouent des relations contractuelles générant des effets réels. L'intrusion de la vie réelle dans ce monde virtuel, immatériel, se jouant des frontières physiques a vite fait naître des inquiétudes tant chez les autorités régulatrices que chez les cybernautes.

La rapidité des flux transfrontaliers, la volatilité des contenus, l'anonymat organisé, sont entre autres des caractéristiques du cyberspace ayant créé un sentiment d'insécurité.

Internet est une structure décentralisée véhiculant « [...] une philosophie libertaire qui voudrait que, le cyberspace soit un [territoire] totalement libre, car soumis à aucune

⁴¹ Ouvrage paru aux Editions du Jurisclasseur ; Litec

⁴² Ibid. p.2

⁴³ « Pour des raisons diverses, il fut souvent soutenu que le droit ne pouvait guère prétendre à réglementer le cyberspace : soit c'était toute limite à la liberté que certains voulaient effacer d'Internet, soit, un peu différemment, était invoquée l'inaptitude du droit à réglementer celui-ci. L'écho de cette vulgate s'est assourdi avec les années, et la vocation du droit à intervenir en matière d'Internet est désormais largement reconnue », A. Lepage ; *Libertés et droits fondamentaux à l'épreuve d'Internet*. Litec, p.3.

souveraineté ». Il a été dit qu'il existait dans le cyberspace « un vide juridique ». C'est dans le souci de répondre à cette inquiétude que Madame Isabelle Falque-Pierrotin a rendu un rapport le 16 juin 1996⁴⁴, dans le cadre d'une mission mandatée par le ministre chargé des télécommunications. Cette mission avait pour but de déterminer si l'arsenal juridique français était suffisant pour protéger un certain nombre de valeurs essentielles, notamment garantir l'ordre public au regard de la jeunesse et des consommateurs⁴⁵.

« A priori, les droits et mesures protectrices de l'internaute [...] ont vocation à s'appliquer à tous les internautes »⁴⁶. Une place doit toutefois être faite aux mineurs qui se justifie par les spécificités liées au statut juridique et à la vulnérabilité du mineur en général et de l'internaute mineur en particulier.

Internet s'est largement invité dans les foyers et les écoles. Qu'il s'agisse de navigation sur les millions de pages que peut compter le cyberspace (sites de jeux en lignes, pages personnelles de plus en plus connues sous l'appellation de weblogs ou blogs tout court), à la participation à des « chats », newsgroups. L'internaute en " culotte courte " est devenu une cible marketing majeure dans la stratégie directement commerciale ou non de nombreux responsables de sites⁴⁷.

L'expansion et la vulgarisation d'Internet ont fait du mineur un acteur aguerri du cyberspace. En tant qu'acteur du cyberspace, le mineur dispose de droits et d'obligations au même titre que tous les internautes. Une interrogation demeure cependant : du fait de sa vulnérabilité juridiquement avérée, doit-il bénéficier d'un aménagement de ses droits et obligations juridiques dans le cyberspace ?

Avant de poursuivre plus avant l'étude du mineur à travers ses droits et obligations dans le cyberspace, il convient de définir précisément ce que l'on entend par mineur même si cela peut paraître relever de l'évidence.

⁴⁴ Rapport de la mission interministérielle sur Internet, 16 mars-16 juin 1996, Isabelle Falque-Pierrotin, La Documentation Française, 1997.

⁴⁵ J. Louvier ; Le cadre juridique d'Internet. P.89

⁴⁶ Ibid. p.17.

⁴⁷ Droit et Nouvelles Technologies : Actualités. « Au centre des débats actuels : la protection des mineurs sur Internet » Guillaume Desgens-Pasanau (Juriste en droit des NTIC-Deloitte & Touche Juridique et Fiscal) 24 Juillet 2001.

http://www.droit-technologies.org/1_2asp?actu_id=450

« Le mineur est l'individu de l'un ou l'autre sexe qui n'a point encore l'âge de dix-huit ans accomplis »⁴⁸. Le mineur est une « Personne physique qui n'a pas atteint l'âge de la majorité légale (actuellement fixé à dix-huit ans) et que la loi en raison de son jeune âge place sous un régime de protection et le prive de la possibilité d'exercer elle-même ses droits (c'est-à-dire qui est frappée d'une incapacité d'exercice) »⁴⁹. Est-ce à dire que le mineur ne peut pas agir juridiquement sur Internet ou simplement que l'exercice de ses droits doit être encadré ?

Le mineur internaute demeure malgré sa vulnérabilité une personne juridique qui dispose de droits fondamentaux (**Titre 1**) générateurs d'obligations et de responsabilités (**Titre 2**) en droit commun et également dans le cyberspace.

⁴⁸ Art.388 du Code Civil

⁴⁹ Sous la direction de Rémy Cabrillac ; Dictionnaire du vocabulaire juridique. Litec

Il existe une subdivision dans la catégorie des mineurs : il existe la catégorie de l'infans qui est un « Jeune enfant qui n'est pas en mesure de comprendre la portée de ses actes »

Titre 1. LES DROITS ET LIBERTÉS FONDAMENTAUX DU MINEUR DANS LE CYBERESPACE.

Un droit fondamental est « une norme juridique, pouvant être énoncée dans une constitution (Loi fondamentale allemande) ou un traité international (Convention Européenne des Droits de l'Homme), et considérée comme intransgressible par une juridiction constitutionnelle ».

L'utilisation de la notion de « droits et libertés fondamentaux » est relativement récente⁵⁰. Cette notion connaît un succès sans faille ; cela s'explique certainement par le fait qu'elle transcende le clivage traditionnel entre droit privé et droit public.

L'adjectif fondamental a été utilisé pour la première fois par le Conseil Constitutionnel pour qualifier les droits et libertés dans une décision du 14 janvier 1982 relative aux nationalisations⁵¹. L'expression « droit fondamental » sera consacrée par la décision n° 89-269 DC du 22 janvier 1990 du Conseil Constitutionnel en matière de droit des étrangers.

Récemment la Charte des droits fondamentaux de l'Union Européenne du 18 décembre 2000 a contribué à la consécration de ces droits par l'emploi officiel de l'expression droits fondamentaux⁵².

Le caractère relativement récent de ces droits n'est pas, du point de vue d'Agathe Lepage, étranger au flou qui les caractérise⁵³.

⁵⁰ Voir M. Delmas-Marty, Introduction in Liberté et droits fondamentaux sous la direction de M Delmas-Marty et C Lucas de Leyssac, Points Essais 2002.p.9. Pour une large perspective historique voir, JL. Gazzanica, La dimension historique des libertés et droits fondamentaux sous la direction de R Cabrillac, M.A Frison Roche et Th. Revet. p.9 et suivant.

⁵¹ V Champeil-Desplats, La notion de droit "fondamental" et le droit constitutionnel français. D.1985, chronique, p.323.

⁵² A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet. P.12. – Voir également A. Pécheul, La charte des droits fondamentaux de l'Union européenne. RFDA.2001.P 688. – F. Benoît-Rohmer, La charte des droits fondamentaux de l'Union Européenne. D.2001 chronique. P.1423, Comm. Com. Electr ; février 2001 ; commentaire n°20 obs. A. Lepage et juin 2001 commentaire. n°55 obs. C. Caron.

Il n'existe pas de définition à proprement parler des libertés et droits fondamentaux. Il est le plus souvent procédé par énonciation des droits et libertés qui les caractérisent. La sensation de flou dont parle Agathe Lepage dans son ouvrage est certainement accentuée par une grande variété des droits et libertés fondamentaux. Elle opère deux types de répartitions.

Dans un premier temps elle distingue quatre groupes.

- Selon la considération de l'être (dignité de la personne humaine, respect du corps humain, vie privée et plus généralement droits de la personnalité, vie familiale, droits fondamentaux de l'enfant).
- Selon la considération du citoyen (droit à une nationalité, liberté politique et droit de vote, liberté d'aller et de venir, droit à la sûreté, liberté de religion, de pensée, de croyance, liberté d'expression, liberté d'association, liberté de créer).
- Selon la considération du justiciable (droit d'accès à la justice, droit à un tribunal, présomption d'innocence, droits de la défense en matière pénale, protection de la personne poursuivie en cas de modification de la législation pénale, principe de la légalité des délits et des peines, droits fondamentaux spécifiques au procès civil ou au procès administratif, droits des victimes, exécution des décisions de justice).
- Selon la considération de l'acteur économique et social (propriété, liberté contractuelle, liberté du commerce et de l'industrie, liberté du travail, droits sociaux, droit à la santé, droit au logement)⁵⁴.

Dans un second elle opère une répartition en deux grands groupes.

- Les libertés et droits fondamentaux à caractère général.
- Les libertés et droits fondamentaux dont le caractère spécifique est propre à certaines catégories de personnes (les étrangers, les détenus...etc.).

⁵³ Libertés et droits fondamentaux à l'épreuve d'Internet. P.12. « *Le caractère relativement récent de la catégorie des libertés et droits fondamentaux n'est sans doute pas étranger au fait qu'elle se trouve encore nimbée de quelque flou* »

⁵⁴ Classification retenue par l'ouvrage Libertés et droits fondamentaux sous la direction de R. Cabrillac, M-A. Frison-Roche et Th. Revet.

La première catégorie peut elle-même être subdivisée entre les droits substantiels d'une part (relatifs à la personne, l'esprit, l'action politique et sociale, la vie socio-économique et culturelle), et les garanties (réparties entre la légalité, l'accès à la justice et le procès équitable)⁵⁵.

Une autre classification met en exergue :

- les droits-libertés (droits de la personne humaine tels que la dignité de la personne, liberté individuelle, liberté d'association, liberté d'enseignement, liberté de conscience et d'opinion, liberté d'expression et de communication, droit de la propriété, liberté d'entreprendre, droits du travailleur, comme la liberté syndicale, le droit de grève et le droit à la participation) ;
- les droits participation (droit de vote) ;
- les droits de créance (droit à la protection sociale et à la sécurité matérielle, droit au respect de la vie familiale, droit à l'instruction et à la culture, droit à la solidarité nationale, droit à l'emploi) ;
- les droits-garantie (droit au juge, droits de la défense, droit à la sécurité juridique, application non rétroactive des lois pénales plus sévères et application rétroactive de la loi pénale plus douce, présomption d'innocence) ;
- le droit à l'égalité⁵⁶.

Dans cette étude, le choix d'une classification, ne va pas se faire par préférence ou au détriment d'une autre. Il va s'agir d'emprunter à chacune des classifications la matière et les éléments correspondant au sujet traité ici. Une double considération sera mise en avant : il faudra autant tenir compte de la nature et du statut du mineur que du cyberspace.

Il ne peut être question en l'espèce d'une quelconque étude du mineur dans le cyberspace sans qu'il n'ait été procédé à une analyse de la nature et de l'étendue de ses libertés et droits fondamentaux.

Il existe un sentiment courant chez les internautes qui leur fait penser que les données et les libertés économiques sont mieux protégées que les libertés individuelles et collectives dans le

⁵⁵ Libertés et droits fondamentaux sous la direction de M. Delmas-Marty et C. Lucas de Leyssac ; Points essais 2002.p.18 & s

⁵⁶ L. Favoreu et alii, Droit des libertés fondamentales, Dalloz 2002. 1ere édition.

cyberespace. La réglementation sur Internet protégerait en priorité les données économiques, mais ne défendrait qu'assez peu les libertés individuelles et collectives⁵⁷. Ce sentiment est renforcé par le fait que dans l'idée générale le commerce électronique est désormais le moteur du développement d'Internet⁵⁸. Qu'en est-il de la valeur ou de l'importance des droits et libertés fondamentaux du mineur ? De quelle nature sont les droits et libertés individuels du mineur (**Chapitre I**) ? Quelles en sont les limites dans l'exercice (**chapitre II**) ?

Le mineur en tant que personne physique doit prétendre, au même titre à la possession de droits liés à sa personne de même que des libertés individuelles propres à s'appliquer dans le cyberespace.

⁵⁷ D. Wolton, O. Jay, Internet. Petit manuel de survie, Flammarion 2000, p.136.

⁵⁸ « Le commerce électronique est fréquemment identifié à Internet même si d'autres réseaux en font partie... ».Eric A. Caprioli, Règlement des litiges internationaux et droit applicable dans le commerce électronique, Jurisclasseur Droit @ Litec2002, p.1.

Chapitre 1. LES DROITS INDIVIDUELS DU MINEUR DANS LE CYBERESPACE.

Le droit, et le code civil en particulier, insistent sur la notion de mineur, surtout quand elle considère un individu dans son incapacité⁵⁹. L'appréciation de la minorité n'est pas qu'arithmétique. La minorité peut être exceptionnellement écourtée (les cas d'émancipations de jeunes mineurs article 476 du code civil) ou rallongée (les minorités prolongées)⁶⁰. Par ailleurs, le critère du discernement joue un rôle important dans l'appréciation de la minorité et ne dépend pas que d'une appréciation mathématique bien qu'il existe des âges légaux pris en considération pour la détermination de la volonté librement consentie des mineurs.

Bien que le critère de minorité soit déterminant pour un certain nombre d'activités du mineur dans le cyberespace, la dimension juridique de l'internaute mineur ne se résout par ce seul critère. « [...] Les droits et mesures protectrices de l'internaute [...] ont vocation à s'appliquer à tous les internautes »⁶¹. L'une des matières qui souffre le plus de la diffusion d'informations sur Internet est la vie privée dans une acception globale. L'enfant dès sa naissance est un être humain qui a droit au respect de sa vie privée dans tous ses aspects. Cette vie privée peut être mise à mal par le biais de la collecte et de la diffusion des données personnelles dans le cyberespace. Les données personnelles peuvent être vues comme le « carburant » permettant au cyberespace de prospérer et de poursuivre son évolution.

Définition des données personnelles.

L'article (2,a) de la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, définit les données à caractère personnel ou données personnelles⁶², comme « toute information concernant une personne physique identifiée ou identifiable (personne

⁵⁹ Jean Carbonnier, Droit civil Tome 2, La famille, l'enfant, le couple, Thémis Droit privé 21^e édition 2002, p.79.

⁶⁰ Institutions atypiques relevant du droit de l'assistance éducative, du droit du divorce (art. 295 code civil), la dépendance financière à l'égard de ses parents (art.2011 du code civil).

⁶¹ A. Lepage, Droits et libertés fondamentaux à l'épreuve d'Internet. Page 17.

⁶² Dans la loi du 6 janvier 1978, dite Loi Informatiques et Libertés il y est fait référence comme données nominatives. La notion de données personnelles semble plus large, quoique la différence ne soit pas réellement significative.

concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Ainsi, sont considérées comme des données personnelles le nom patronymique, le numéro de sécurité sociale, l'immatriculation du véhicule, un numéro de téléphone, un numéro de carte bancaire, une adresse email...⁶³. Seules sont protégées les personnes physiques, à condition qu'elles soient identifiées ou identifiables. Internet facilite la diffusion des informations dont les données personnelles constituent une part importante. Grâce aux données personnelles, il est possible de suivre une personne à la trace quelle que soit sa localisation géographique. Ces éléments ont relancé la question de la protection des données personnelles. Le fonctionnement des services d'Internet s'appuie pour une part importante sur l'utilisation de données personnelles de toutes sortes. Ces données personnelles ont un rôle incontournable dans le service de messagerie, les moteurs de recherche, le commerce en ligne, etc.

Du fait de la rapidité des échanges, de l'interactivité et des immenses possibilités de reproduction de l'information offertes par Internet, force est de constater que se révèlent simultanément des risques d'atteintes à la vie privée des personnes. Le recueil, la mémorisation et le transfert aisés d'informations personnelles sur Internet, favorisent leur diffusion et leur exploitation et rendent les personnes physiques concernées directement ou non identifiables par recoupement de données⁶⁴. S'agissant de la diffusion des informations personnelles, le danger est d'autant plus grand que même les non internautes peuvent être concernés par une diffusion de leurs données personnelles sur la Toile.

La question de la protection des données personnelles à l'égard des mineurs révèle plusieurs difficultés. D'une part ils sont directement concernés par la diffusion de leurs propres données personnelles volontairement ou non fournies. D'autre part ils peuvent impliquer des tiers (membres de leurs familles ou autres) dont ils auront sciemment fourni les données personnelles.

⁶³ Ce que la loi Informatique et libertés « donnée nominative » porte le nom de « donnée à caractère personnel » dans les instruments de l'OCDE, du Conseil de l'Europe et de la directive communautaire. C'est la traduction littérale des termes anglais « personal data ». http://www.dit.presse.fr/infolib/french/arti_pitrat.htm

⁶⁴ Internet, les jeunes et la protection des données personnelles et de la vie privée. www.cnil.fr/juniors/fiches/fiches1.pdf

§1. Les données personnelles du mineur dans le cyberspace.

La circulation des données personnelles sur Internet est une question sensible, le facteur de la minorité du détenteur ou du fournisseur des données rajoute de la gravité à la question. Le mineur appartient à une catégorie de personnes très protégées. Toute information le concernant doit être manipulée sous certaines conditions⁶⁵ et avec beaucoup de précautions. Les données personnelles obéissent à un régime juridique spécifique dans le cyberspace, les protections qui découlent de ce régime juridique spécifique sont accrues lorsqu'il s'agit de données impliquant un mineur.

A. Le régime juridique des données personnelles dans le cyberspace.

La question des données personnelles crée un pont entre les libertés et droits fondamentaux et le commerce électronique. Le commerce électronique étant considéré comme le moteur de l'essor d'Internet⁶⁶, c'est dans ce domaine que se sont cristallisées les inquiétudes liées à la collecte et à l'utilisation des données personnelles dans le cyberspace.

La référence aux données personnelles du mineur suppose deux catégories de données personnelles: d'une part les données personnelles propres au mineur et l'identifiant directement, d'autre part les données familiales susceptibles d'identifier individuellement un membre de la famille ou la famille dans sa globalité. C'est la représentation des données directes ou indirectes. Ces données concernent aussi bien les majeurs de la famille (au premier rang desquels les parents), que les autres mineurs de la famille.

S'agissant des données concernées : il peut s'agir de l'adresse du domicile familial, d'adresses e-mails des membres de la famille, de toute forme de numéro identifiant (téléphone mobile ou fixe), d'immatriculation (telle celle d'un véhicule), un numéro de sécurité sociale ou tout autre identifiant correspondant à une administration ou à un service de clientèle, adresse IP, etc.

⁶⁵ Notamment l'autorisation des parents ou des tuteurs légaux responsables du mineur concerné. Cette autorisation est préalable à toute manipulation et/ou diffusion.

⁶⁶« La société de l'information telle qu'elle est vue aux Etats-Unis n'a de sens que si elle génère un commerce et des valeurs commerciales. Ceci à la différence du concept de « société de l'information » notamment français actuel, qui sous-tend une vision plus humaniste, plus sociétale. [...] La vie privée tend à être considérée comme un obstacle injustifié qu'il convient d'éliminer ». M. Briat et Ch. M. Pitrat, « Urgent : Concepts à clarifier » http://www.dit.presse.fr/infolib/french/arti_pitrat.htm

Eu égard à l'interdépendance existant entre le traitement des données personnelles et le commerce électronique, il convient de s'interroger sur la nature juridique des données personnelles dans le cyberspace. Doit-on leur conférer une nature patrimoniale ou ne s'agit-il que d'information ?

1. Les données personnelles : une valeur commerciale.

Le cyberspace doit pour une part substantielle son existence et son dynamisme au commerce électronique. Cela semble justifier la tentation ou plutôt la tendance à conférer une valeur économique aux données personnelles circulant sur la Toile.

1-a. Valeur économique.

Dans le cyberspace comme dans le monde réel (par opposition au monde virtuel), le commerce électronique sous-tend une part substantielle des échanges effectués entre les internautes. Il est donc logique que le premier bénéficiaire de la collecte des données personnelles soit le commerce électronique. Pour cette raison « le commerce électronique est [...] souvent mis sur la sellette en raison de la menace qu'il fait planer sur les données personnelles⁶⁷ en favorisant des procédés dont l'objet est de recueillir des informations sur l'internaute qu'il en ait conscience ou non »⁶⁸. Ces informations recueillies auprès de l'internaute peuvent être utilisées à des fins commerciales. Derrière chaque internaute (et donc ses données personnelles), on entrevoit le consommateur qui pourrait faire l'objet d'un profilage marketing ciblé avec un mailing adapté.

La question qui se pose est celle de la valeur des données personnelles. Doit-on les considérer comme des biens commercialisables au même titre que les biens de consommation ?

La directive du 24 octobre 1995 sur le traitement des données à caractère personnel considère que la libre circulation des données, fait partie de la libre circulation des biens et services⁶⁹. Elle précise cependant qu'il s'agit de biens particuliers nécessitant une protection particulière. On retrouve des dispositions similaires dans le droit avec la loi du 6 janvier 1978 dans son

⁶⁷ L. Cadoux, et P. Tabatoni, Internet et protection de la vie privée : commentaires, printemps2000, p.57 et s

⁶⁸ A. Lepage. Libertés et droits fondamentaux à l'épreuve d'Internet ; Jurisclasseur Droit @ Litec2002, p.24.

⁶⁹ Directive 24.10.1995 n°95/46/CE du Parlement européen et du Conseil relative à la protection des données à caractère personnel et à la libre circulation de ces données, JO n°L.281, 23 novembre 1995.

dispositif informatique et libertés qui autorise la commercialisation des fichiers des entreprises. Aucune référence explicite n'est faite aux données personnelles, pas plus qu'il n'est déterminé la nature des fichiers dits commercialisables.

Les données personnelles deviennent des biens marchands, échangés, achetés, loués dans le cadre d'un marché lucratif en pleine expansion, et parfois à l'insu des personnes concernées. La valeur économique d'un site ou d'un portail, d'un fond de commerce électronique, est de plus en plus dépendante de la valeur reconnue aux données personnelles des internautes qui lui sont affiliés (clients, membres, intervenants, prospects)⁷⁰.

L'importance économique des données personnelles est encore plus marquée aux Etats-Unis; d'où l'idée rependue que les Etats-Unis ne font pas de la protection des données personnelles sur Internet leur priorité. Il y a de leur part une volonté de réguler Internet au minimum pour laisser place aux forces du marché. Cette position limite la portée de la protection des droits des consommateurs sur le plan international⁷¹. Le fait est qu'ils ont une approche pragmatique de la question ; l'intervention de l'Etat fédéral et des Etats fédérés n'est pas souhaitable *a priori*. La priorité est donnée à l'autorégulation par les acteurs eux-mêmes, et par les entreprises qui ont intérêt à établir un climat de confiance sur Internet. C'est là une vision pragmatique qui emprunte beaucoup à la gestion des relations économiques classiques⁷².

1-b. Objet patrimonial.

Le régime juridique de la protection des données à caractère personnel est induit par leur nature particulière. Malgré le fait qu'elles ne relèvent ni du statut des produits, ni de celui des services, on leur applique le même régime du point de vue de leur circulation⁷³.

⁷⁰ Jean Frayssinet, Internet et la protection juridique des données personnelles, Colloque International, Internet et le droit, Droit européen et comparé d'Internet, 25-26 septembre 2000

⁷¹ G. Chatillon, La protection des consommateurs et des PME ; Le commerce électronique : Quelles protections ? Actes du colloque 19-20 novembre 2001, Le droit international d'Internet, p.388.

⁷² « La société de l'information telle qu'elle est vue aux Etats-Unis n'a de sens que si elle génère un commerce et des valeurs commerciales. Ceci à la différence du concept « société de l'information » notamment français actuel, qui sous-tend une vision plus humaniste [...]. Pour concilier ces choix de société, il est fait appel à des règles de commerce international basées essentiellement sur l'élimination de tout obstacle à la libre circulation de biens et de services. Dans cette approche l'information est un bien qui perd sa spécificité et auquel on applique le principe de libre commerce. La vie privée tend à être comme un obstacle injustifié qu'il convient d'éliminer. Cette vision est en général partagée par les organisations internationales dont l'objectif est la création de zone de libre échange ». M. Briat et Ch. M. Pitrat, Urgent : Concepts à clarifier.

http://www.dit.presse.fr/infolib/french/arti_pitrat.htm

⁷³ M.-P Fenoll-Trousseau et G. Haas, Internet et protection des données personnelles, Droit@Litec édition2000, p.5

La Directive du 24 octobre 1995 sur le traitement des données à caractère personnel énonce en son article premier que « les données personnelles sont des biens informationnels ayant une valeur marchande, qui doivent circuler librement sur le territoire de l'Union dans le cadre d'un marché unique pour éviter des disparités économiques et concurrentielles, tout en faisant l'objet d'une protection des droits et libertés fondamentaux de la personne »⁷⁴. « Les données personnelles peuvent être considérées comme des biens commercialisables, de consommation⁷⁵ ».

Il est reconnu une véritable valeur marchande aux données à caractère personnel ; cependant leur nature particulièrement sensible nécessite un mécanisme de protection afin de ne pas laisser à l'entière discrétion des acteurs économiques la gestion de ce « marché » exponentiel des données personnelles.

Olivier Iteanu s'inspirant de faits jugés par le tribunal correctionnel et la Cour d'appel⁷⁶ nous présente un scénario où la vie privée (par le biais des données personnelles) fait l'objet d'une marchandisation⁷⁷. Il est question d'un journaliste d'investigation qui s'étant donné pour mission de dénoncer le fait que des marchands peu scrupuleux ayant collecté des données personnelles sous la foi parfois de fausses promesses, les monnaient. Ce cas de figure induit une valeur patrimoniale aux données personnelles collectées⁷⁸ dans une optique informative.

Les personnes sont-elles propriétaires des données qui les concernent ? C'est la question que pose le rapport rendu au Ministre de la fonction publique et de la réforme de l'Etat⁷⁹. Selon ce rapport, « si un droit de propriété doit être reconnu sur les données personnelles, ce droit de

⁷⁴ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. JOCE n° L 281 du 23/11/1995 p. 0031 - 0050

⁷⁵ Erika Orengo, DESS Droit de l'informatique et du multimédia sous la direction de J. Huet 2001-2002, La protection des personnes dans le cadre des flux transfrontières de données personnelles.

⁷⁶ Jugement du tribunal correctionnel de Paris 13^e chambre prononcé le 13 février 2002, Antoine C. /ministère public, T., et de l'arrêt de la cour d'appel de Paris, rendu le 30 octobre 2002 dans cette même affaire.

⁷⁷ Olivier Iteanu, Tous cybercriminels. La fin d'Internet ? Jacques-Marie Laffont Editeur 2004, p.136

⁷⁸ Le propos de ces affaires concernait au premier chef l'intrusion d'un individu dans un système de sécurité par une faille de sécurité. La dénonciation de la marchandisation de la vie privée n'en était que l'objet.

⁷⁹ P. Truche, J-P. Faugère et P. Flichy, Administration électronique et protection des données personnelles, Livre Blanc, coll. des rapports officiels, Rapport au Ministre de la fonction publique et de la réforme de l'Etat, La documentation française, p.75

propriété devra plutôt être conféré à la personne qui est concernée par les données qu'au détenteur de la base de données »⁸⁰.

Pour qu'il y ait un véritable droit de propriété, la libre disposition du bien est nécessaire. Or selon que l'on considère la personne concernée ou le détenteur des données personnelles comme le bénéficiaire d'un droit de propriété sur lesdites données, la libre disposition de ces données varie. Cet aspect devant faire l'objet d'une analyse dans la suite de cette étude, on se contentera d'énoncer l'interdépendance de principe qui existe entre le détenteur et la personne concernée par les données personnelles s'agissant de la libre disposition et donc du traitement de ces données.

En France, la commercialisation des fichiers des entreprises est autorisée par le dispositif Informatique et libertés mis en place par la loi 1978, texte créateur de la CNIL autorité administrative indépendante dont la mission est de veiller au respect des dispositions de la loi portant notamment sur la cession et le traitement des données. Aucune référence explicite n'est faite aux données personnelles. Pas plus qu'il n'est déterminé la nature des fichiers dits commercialisables. Cette commercialisation doit cependant respecter un certains nombres de règles que nous étudierons en *infra*.

D'autres interrogations portant sur la valeur patrimoniale des données personnelles sont apparues s'agissant notamment du domaine de l'entreprise⁸¹. Deux start-up Toysmart.com et Boo.com avaient envisagé en leur temps, pour éponger leurs pertes, de jouir en les cédant, de la valeur patrimoniale de leurs fichiers clients.

Cette approche patrimoniale des données personnelles sera également observée lors de la fusion Vivendi Seagram Canal plus. Le fichier de cinq millions d'abonnés à Canal Plus

⁸⁰ Il s'agit ainsi d'une exception au principe selon lequel l'information appartient à celui qui en a réalisé la collecte ou qui en assure la formulation.

⁸¹Cynthia Chassigneux, Doctorat en droit Université Panthéon-Assas en cotutelle avec l'Université de Montréal, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, « *Quel est le statut juridique des données personnelles que le commerçant électronique détient dans ses fichiers clients. Doivent-elles ou non être intégrées dans le patrimoine de l'entreprise. Peuvent-elles être cédées en cas de faillite avec les actifs de la société ? Telles sont les questions qui ont pu se poser au regard des affaires Toysmart.com et Boo.com par exemple. Ces sociétés ont été remarquées tant pour leur succès que leur retour. Ces start-up d'hier ont envisagé vendre leurs fichiers clients pour minimiser leurs pertes, les données contenues dans les fichiers constituant une véritable mine d'or* », Paris 3.07.2003, p.64 §111

intéressait tout particulièrement Vivendi. Mais l'intervention de la CNIL et du CSA a permis à Canal Plus de conserver la maîtrise de ce fichier⁸².

Pour conclure cette analyse, on peut considérer que « les données personnelles sont des biens informationnels, ayant une valeur marchande, qui doivent circuler librement sur le territoire de l'Union dans le cadre d'un marché unique pour éviter des disparités économiques et concurrentielles, tout en faisant l'objet d'une protection des droits et libertés fondamentaux de la personne, en particulier, mais pas seulement, de la vie privée »⁸³.

2. Les données personnelles, information à caractère personnel.

Dans l'esprit des pionniers, Internet devait être un immense espace de liberté, sans contrainte, sans frontière, sans police d'aucune sorte. La nécessité de partager l'information fut un des éléments générateurs d'Internet. « A ses débuts, Internet servait d'ailleurs principalement à échanger des informations et du savoir⁸⁴ ».

Le thème de la protection des droits et libertés des personnes, en particulier celui de la vie privée est apparu le premier au tournant des années 70-80. Cela a donné lieu en Europe à une vague de législations spécifiques sur la protection des données personnelles afin d'encadrer leur gestion à travers les systèmes informatiques et les fichiers de toutes tailles⁸⁵.

La constitution de fichiers ne représentait pas (tout au moins au début) une grande menace pour les libertés individuelles. Ceci s'explique par le fait que n'était concerné qu'un nombre limité de personnes (la communauté des chercheurs, un cercle défini par une activité commune et des personnes facilement identifiables).

En France, l'administration sera l'un des plus grands gestionnaires de fichiers, le but avoué étant une meilleure administration du service public.

⁸² E.Orengo, La protection des personnes dans le cadre des flux transfrontières de données personnelles, DESS droit de l'informatique et du multimédia sous la direction de Monsieur J. Huet, 2001-2002, p.9.

⁸³ Jean Frayssinet, Internet et la protection juridique des données personnelles, Colloque international Internet et le droit, 25-26 septembre 2000, p.6

⁸⁴ M.P. Fenoll-Trousseau et G. Haas, Internet et protection des données personnelles, Litec, p.1.

⁸⁵ Jean Frayssinet, La protection des données personnelles est-elle assurée sur Internet ? p.435-443

Acte du colloque Paris 19 et 20 novembre 2001, Université Paris I Panthéon Sorbonne et l'Association ARPEGE, Le droit international d'Internet sous la direction de Georges Chatillon, Bruylant Bruxelles 2002, p.435

2-a. Les données personnelles électroniques et le service public.

L'administration en France dans un souci d'amélioration des services aux administrés, a constitué de grands fichiers. La première vague d'informatisation des administrations intervient entre les années 1960 et 1970. Cette informatisation visait principalement une meilleure productivité. Il y avait néanmoins en arrière pensée la volonté d'une meilleure connaissance de la population, de même qu'un meilleur contrôle de celle-ci. La considération pour la vie privée n'était pas encore au centre des préoccupations. Il s'en est suivi une constitution de grands fichiers bâtis autour d'identifiants massifs⁸⁶.

Cet effort de l'administration française intervient alors même qu'Internet est naissant et, n'est pas encore étendu en dehors des cercles des chercheurs et des militaires.

Il convient de définir le type de données personnelles qui sont concernées ici. Il s'agit de tout identifiant chiffré ou non qui renvoie à l'identité de la personne et rien qu'à elle. Toute personne, tout administré accumule tout le long de son existence de nombreux identifiants ou matricules dont le but est de permettre une gestion plus aisée des dossiers. Il est question ici de l'administration centrale qui rassemble en son sein de nombreuses administrations et services ayant chacun un mode d'identification propre : au sein de l'administration sociale, la sécurité sociale avec le numéro de sécurité sociale, la caisse d'allocations familiales et son numéro d'allocataire, etc. Le service public de l'éducation ou un étudiant acquiert un identifiant national qu'il gardera tout au long de son cursus.

Les identifiants uniques renvoyant directement à l'identité de la personne peuvent également donner des indications sur la situation de la personne, ou d'autres informations sur la personne (à l'instar du numéro de sécurité sociale qui donne votre année et votre mois de naissance votre statut de ressortissant étranger ou français, indique votre sexe). Dans d'autres cas les indications sont plus subtiles mais revêtent toutes des informations complémentaires et sensibles sur la personne, informations qui en définitive permettent l'identification d'un individu.

⁸⁶ P. Truche, J-P. Faugère et P. Flichy, Livre blanc ; Administration électronique et protection des données personnelles, Rapport au ministre de la fonction publique et de la réforme de l'Etat, La documentation française 2002, p. 19.

Les données personnelles rassemblées par les différents services publics n'ont aucune valeur marchande. Elles ne peuvent être légalement commercialisables, ni faire l'objet de cession. *A priori*, ces fichiers ne devraient même pas faire l'objet de croisements entre les différentes administrations sauf cas exceptionnel. Le danger est que par un jeu de croisement des informations, il soit possible d'établir un profil très détaillé de l'administré. Dans la même idée, ces grands fichiers administratifs ne connaîtront en principe jamais de destin international.

Ces fichiers ont une valeur informative ; ils ont pour vocation de contribuer à un traitement personnalisé et plus rapide de chaque administré. Une affaire Safari⁸⁷ fut révélée par Philippe Boucher dans un article intitulé « Safari ou la chasse aux Français »⁸⁸. Dans cet article il accuse le pouvoir politique d'organiser la « chasse aux Français » par un croisement des fichiers administratifs à partir du seul numéro de sécurité sociale. A la suite de cette affaire, une commission fut créée à la demande du Premier ministre. Elle devait proposer des mesures tendant à garantir le respect des libertés individuelles et publiques face au développement de l'informatique. Ces travaux seront précurseurs de la loi de 1978⁸⁹.

L'avènement d'Internet a introduit dans ce domaine comme dans d'autres une certaine dose d'insécurité. Ce fut notamment le cas avec l'avènement de l'administration en ligne. Désormais tout administré peut dans une certaine mesure accomplir un certain nombre d'actes administratifs en ligne, gérer ses dossiers en ligne. Cela suppose une identification systématique en ligne qui laisse des traces pouvant être détournées ou exploitées par des personnes malveillantes en ligne avec des problèmes d'usurpation d'identité.

Les auteurs du Livre Blanc sur l'« *Administration électronique et protection des données personnelles* »⁹⁰, dans leur volonté de décrire la valeur marchande des données personnelles, vont examiner la question par rapport au droit de propriété sur les données personnelles.

⁸⁷ Système informatisé pour les fichiers administratifs et le répertoire des individus. Projet gouvernemental visant à interconnecter les fichiers administratifs à partir d'un identifiant unique, le numéro de sécurité sociale.

⁸⁸ Ph. Boucher, Safari ou la chasse aux Français », Le Monde 21 mars 1974.

⁸⁹ M-P. Fenoll-Trousseau, G. Haas, Internet et la protection des données personnelles, p.11.

⁹⁰ Livre blanc « Administration électronique et protection des données personnelles » remis le 26 février 2002, par MM. Pierre Truche, Jean-Paul Faugère et Patrice Flichy au ministre de la fonction publique et de la réforme de l'Etat, <http://www.ssi.gouv.fr/fr/actualites/raptruche.pdf>

De leur point de vue, si un droit de propriété devait être reconnu sur les données personnelles, le bénéficiaire devrait-en être la personne concernée. Ce faisant il s'agirait alors d'une exception au principe selon lequel : l'information appartient à celui qui en réalise la collecte ou qui en assure la formulation soit le détenteur des fichiers. Il manque dans ce cas un élément de libre disposition du bien tant pour la personne concernée par les données personnelles que pour le détenteur des dites données⁹¹ ; élément déterminant le droit de propriété sur les données personnelles.

Si l'utilisation par l'administration des données personnelles n'a pas de vocation économique, il existe d'autres entités, elles privées, qui bien qu'elles aient également comme objectif le service aux usagers, le font dans une optique mercantile et/ou informative.

2-b. Les données personnelles à vocation informative.

Le régime juridique et la protection des données personnelles nous renvoient aux droits et libertés fondamentaux. « Il ne s'agit pas tant de protéger les données elles-mêmes mais bien d'avantage de protéger les droits et libertés fondamentales des individus dont les données font l'objet de traitements »⁹².

2.b'. Les fichiers informatiques pour les besoins du fonctionnement d'une entreprise.

L'essor économique galopant de certains secteurs produit des entreprises surdimensionnées. Leur mode d'organisation (selon leur importance) s'appuie généralement sur des filiales nationales voire internationales. Elles mettent sur pied des partenariats avec d'autres entreprises, ou font appel à des sous-traitances. Pour le besoin de l'étude, nous allons nous intéresser aux entreprises de services.

De nombreuses sociétés transfèrent périodiquement des fichiers afin notamment de délocaliser certains services, analyser les fichiers clients, centraliser les données sur les serveurs de la maison mère, envoyer des données à une filiale, etc.

⁹¹ Ibid. p.75

⁹² Pierre Bischoff (administrateur à la commission européenne. Direction générale XIII « Télécommunication, marché de l'information et valorisation de la recherche), L'Union Européenne et la protection des données. La société de l'information à l'épreuve des droits de l'homme, Revue du Marché Commun et de l'Union Européenne n°421, septembre 1998, p.538.

Du fait de la mondialisation des échanges et du fonctionnement des sociétés multinationales, les transferts internationaux d'informations personnelles sont devenus des éléments indissociables de la réalité économique et sociale des entreprises.

La constitution de bases de données mondiales de gestion du personnel dans les multinationales, la centralisation de fonctions d'assistance ou de maintenance informatique en leur sein, l'hébergement de sites Web par des prestataires établis à l'étranger ne sont que quelques exemples courants de projets générant des transferts internationaux de données⁹³. Les entreprises concernées ont toutes une vocation économique qui pourrait laisser penser que les données concernées n'ont qu'une valeur économique ; cependant et du fait que ces transferts sont indispensables à une bonne gestion administrative de ces entreprises, la vocation informative se greffe à celle économique : il s'agit de données hybrides.

2.b". Les données personnelles à vocation purement informative.

Les moteurs de recherche sur Internet doivent nous permettre d'effectuer des recherches dans le cyberspace. Ils « scannent » tout le réseau Internet. Cette recherche est fonction de mots clés que nous aurons préalablement déterminés.

Le référencement sur Internet est le mode de diffusion le plus fréquent de données, de produits et de services. Il s'effectue grâce à des outils de recherche. Les outils de recherche sont de deux sortes :

- Des outils humains comme les annuaires⁹⁴, les guides ou les répertoires, qui apparaissent comme des répertoires de sites classés par thèmes et construits manuellement sur demande du titulaire du site par des systèmes de déclaration volontaire.
- Des outils automatiques ou moteurs de recherche, qui sont fondés sur des programmes de navigation appelés « robots » qui parcourent les pages Web et leurs liens de

⁹³Georges de la LOYERE, Commissaire, Quand les données personnelles traversent les frontières de l'Europe, 30 mai 2005 - Tribune

<http://www.cnil.fr/index.php?id=1830&news%5Buid%5D=263&cHash=12264f4391>

⁹⁴Peuvent notamment être concernés les annuaires des chercheurs. En 1995 la CNIL a été saisie de 17 demandes d'avis relatifs à la mise sur Internet d'annuaires professionnels. Le but (louable à l'origine) était de favoriser les échanges à l'intérieur de la communauté des chercheurs. Il s'agissait donc au départ d'une vocation purement informative. Le problème s'est posé à cause de leur diffusion sur le Web compte tenu de la facilité de navigation ou de la reprise aisée des pages par quiconque ; Libération , 9 juillet 1996, Catherine Maussion, Première intrusion de la Cnil sur Internet, p.13.

manière continue en indexant de façon automatique l'information trouvée, à partir de mots clés, contenus soit dans l'adresse URL d'un document HTML, soit dans le titre d'un site, ou même selon l'indice de popularité des sites⁹⁵.

La valeur informative des données personnelles a une grande importance dans le domaine de la liberté d'information et d'expression⁹⁶. Sa valeur n'est plus à démontrer pour la liberté de la presse ; cela est vrai autant pour les auteurs de cette presse que pour ses lecteurs. Grâce aux données personnelles (essentiellement nominatives), l'accès à l'information est simplifié et permet une multiplication exponentielle du volume et des sources données.

Les journalistes travaillent en liaison directe sur une échelle planétaire avec les serveurs des agences de presse, les bases de données publiques, les archives informatisées des autres organes et des grandes institutions. Cette diversification des sources constitue une garantie de pluralisme et de fiabilité de l'information⁹⁷.

Internet a quasiment dépossédé les journalistes professionnels de leur statut de privilégiés par rapport à l'accès et à la diffusion de l'information. Tout internaute peut être l'auteur d'un article qu'il pourra diffuser sur sa page personnelle, sur un site personnel ou sur un site public. Par ailleurs, l'internaute se trouve pour ainsi dire à égalité d'accès à l'information avec les organes de presse, il peut interroger les mêmes sources dans les mêmes conditions⁹⁸. Il suffit pour cela de maîtriser Internet et l'utilisation des moteurs de recherches. Cela est vrai même si l'internaute ne vise pas un but journalistique par ces recherches. Les données personnelles ainsi visées concernent au premier chef le nom et les informations directement liées à la personne (nom, adresse ...).

Un domaine illustre assez bien cette question : l'administration publique. Les progrès intervenus dans le domaine informatique depuis vingt ans ont bouleversés la donne, notamment la pratique de la numérisation. La numérisation des documents publics et leur diffusion sur les réseaux ont accéléré la levée des dernières barrières en matière de liberté

⁹⁵Murielle Cahen propose de nombreuses informations juridiques concernant directement Internet. Article : « La protection des outils de référencement : l'articulation entre contrefaçon et concurrence déloyale » http://www.murielle-cahen.com/p_referencement.asp

⁹⁶ Guy Braibant, Données personnelles et société de l'information, collection des rapports officiels, Rapport au premier ministre, La documentation française, Paris 1998, p.14.

⁹⁷ Ibid.

⁹⁸ Ibid.

d'accès aux documents administratifs. Les renseignements de tous ordres, les rapports publics, les textes juridiques⁹⁹, sont devenus directement accessibles en ligne¹⁰⁰.

Les sites éducatifs pour tous et pour les jeunes en particulier (scolaires, lycéens et étudiants) ont vocation informative, bien que leur consultation ne constitue pas l'essentiel de la navigation des mineurs (quoi qu'en pensent les parents)¹⁰¹. Les adultes ont tendance à voir dans Internet une gigantesque base de données capable d'apporter un savoir encyclopédique à leurs enfants. Selon Annette Dumesnil, « *Internet est un outil merveilleux d'aide aux devoirs mais ce n'est pas que cela* »¹⁰². Les recherches documentaires en vue de travail scolaire peuvent avoir comme mot clef ou base de recherche une donnée personnelle (le plus souvent un nom).

Dans un autre contexte tout aussi informatif quoique plus ludique, les mineurs et les adolescents en particulier ont souvent un engouement pour les stars. Ils sont intéressés par tout ce qui se rapporte à ces personnalités. Ils recherchent donc souvent des informations sur Internet ce en passant par des moteurs de recherche. Ces derniers scannent tout le Web avec le mot clef (le nom ou le pseudonyme de la star) et ressortent tous documents écrits, sonores ou imagés se rapportant à la personne visée sans considération de la légitimité de ces informations au regard du droit à la vie privée de tout un chacun¹⁰³.

La valeur informative des données personnelles peut être d'une utilité médicale, et concerner un aspect privé de la vie du mineur, on entre là dans le domaine des données personnelles particulièrement sensibles.

⁹⁹ Tous ces documents sont de véritables creusets de données personnelles.

¹⁰⁰ Guy Braibant, Préc., p.14-15.

¹⁰¹ Selon un site canadien, 65% des parents pensent que leurs enfants utilisent essentiellement la Toile pour leurs travaux scolaires, alors que 56% des jeunes citent le courriel comme étant leur activité préférée ; La protection de la vie privée et les jeunes, Réseau éducation-Médias

www.éducation-medias-ca/français/enjeux/vie_privée_enjeu.cfm

¹⁰² Annette Dumesnil poursuit en disant : « *A la différence de la télé, où ils sont passifs, les jeunes internautes y sont sans cesse invités à réagir, à être interactif. Qu'y a-t-il de plus éducatif que de participer à un site de critiques de cinéma ?* » Le Nouvel Observateur, 22 novembre 2001 ; Votre enf@nt et internet, S. Arteta, M. Lemonier, S. Noucher et C. Soula.

¹⁰³ La chanteuse Lorie a eu connaissance d'un site litigieux en effectuant sur le nom de « Lorie » à l'aide du moteur de recherche voila.fr exploité par la société Wanadoo Portails ; TGI de Paris, Ordonnance de référé 12 mai 2003, Mlle Laure Pester dite Lorie c/ M. Géraume Schweitzer, Légipresse n°205, octobre 2003, commentaire Laurence Tellier-Loniewski (avocat au barreau de Paris, Cabinet Alain Bensoussan), p.150 et s.

2-c. Les données sensibles du mineur : les données médicales.

La collecte des données médicales doit être faite en respect de la vie privée du mineur comme c'est le cas dans toutes les collectes de données personnelles. Cette collecte doit respecter le tronc commun des principes d'une collecte légitime de données personnelles : droit à l'information préalable¹⁰⁴, droit d'accès direct et indirect¹⁰⁵, droit de curiosité, droit de communication, droit de rectification¹⁰⁶, droit d'opposition¹⁰⁷, droit à l'oubli. Certaines de ces exigences sont renforcées en considération du caractère sensible des données concernées.

Le patient ou dans le cas du mineur son représentant légal, doit être préalablement informé sur la nature des données et doit donner son consentement écrit. La collecte est ciblée ; elle ne peut englober la totalité des données présentes dans le dossier du patient. Il doit être informé de la finalité de la collecte, des modalités d'anonymisation indispensables pour le traitement des données médicales. Le patient dispose d'un double droit d'accès (direct ou indirect):

- sur demande directe de son représentant légal,
- par l'intermédiaire d'un professionnel de santé,
- sur sa demande ou sur celle du responsable de son traitement¹⁰⁸.

Il va de soi que le mineur ou son représentant légal doit connaître le destinataire des données et le responsable de la base de données. Le médecin collecteur doit être indépendant du promoteur de la récolte des données ; il ne doit pas être rémunéré sauf à être dédommagé de ses frais réels et du temps qu'il aura consacré à la collecte¹⁰⁹. S'agissant de son droit de rectification, le patient et même son tuteur légal ne peuvent le faire eux-mêmes ; seul y est habilité le responsable du traitement qui n'est pas nécessairement son médecin traitant. Le patient a enfin, un droit de suppression ou d'interdiction.

¹⁰⁴ Article 27 Loi 1978 : Les personnes concernées par les données qui vont être traitées doivent bénéficier au préalable d'un certain nombre d'information : caractère obligatoire ou facultatif des réponses, conséquences à leur égard, les destinataires des informations, droit d'accès et de rectification.

¹⁰⁵ Loi 1978 art.34 et 35

¹⁰⁶ Id, art.36

¹⁰⁷ Id, art.26

¹⁰⁸ Les données médicales sont régies par la directive 95/46 et l'article 458 du code pénal relatif au secret médical, Thibaut Verbiest et Etienne Wery (Avocats aux Barreaux de Paris et de Bruxelles, Cabinet ULYS, membres Eurojuris), 16 mars 2005, Le dossier médical informatisé : la délicate protection des données personnelles, voire les sites Sixi Soins Infirmiers et Informatiques et Droit et Nouvelles Technologies respectivement :

http://www.sixi.be/Ledossier-medical-informatise-la-delicate-protection-des-donnees-personnelles_a245.html

http://www.droit-technologie.org/1_2.asp?actu_id=1048&motcle=donn%E9es+medicales&mode=motamot

¹⁰⁹ Système de récolte de données médicales anonymes auprès de médecins généraliste, 8 mai 2004, Bulletin du conseil national n°104, p.5 (Belgique).

La collecte entre un patient et son médecin dans l'optique des soins ne pose pas de problèmes, ce sont les exploitations ultérieures qui nécessitent un contrôle¹¹⁰. Les données médicales sont régies par les articles 40-01 à 40-10 et 40-11 à 40-15 de la loi de 1978¹¹¹.

La collecte des données personnelles médicales se fait souvent et de plus en plus par le biais de leur numérisation. Cela rentre dans une perspective de gestion de la santé d'un patient par le biais d'Internet. Une consultation en ligne est alors possible en composant un code secret. Trois difficultés en découlent : l'identification des personnes qui consultent le dossier, la sécurisation et l'intégrité des données médicales du patient et le droit de ce dernier face à cette intrusion¹¹².

Le droit à l'information, la valeur informative des données personnelles peut tout de même conduire par un traitement déloyal des données personnelles à la violation de la vie privée de la personne concernée¹¹³.

B. Le traitement des données personnelles du mineur.

Le traitement des données personnelles fait l'objet de nombreux débats et études. L'existence de fichiers regroupant des données personnelles n'a pas lieu d'être si aucun usage n'en est fait. C'est l'usage des données personnelles qui est générateur de danger pour les droits des personnes concernées.

¹¹⁰ Ibid.

¹¹¹ Les données médicales sont régies par la directive 95/46 et l'article 458 du code pénal relatif au secret médical, Thibaut Verbiest et Etienne Wery, op. cit. Voir les sites Sixi Soins Infirmiers et Informatiques et Droit et Nouvelles Technologies respectivement :

http://www.sixi.be/Ledossier-medical-informatise-la-delicate-protection-des-donnees-personnelles_a245.html

http://www.droit-technologie.org/1_2.asp?actu_id=1048&motcle=donn%E9es+medicales&mode=motamot

L'article 6 de la Convention 108 mentionne les données médicales parmi les catégories particulières de données qui ne peuvent être traitées automatiquement « à moins que le droit Internet ne prévoit des garanties appropriées ». La CNIL les assimile souvent à des données sensibles et veille à la mise en place de réseaux sécurisés de transmission des données et de mécanismes renforcés de confidentialité et de protection des droits des personnes, EDUCNET. Veille juridique, février 2004, La notion des données personnelles- c/ Les données sensibles. – CNIL, Délibération n°85-080 du 22 octobre 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 18 novembre 1985.

<http://www.educnet.education.fr/juri/vieprivee/donneesC.htm>

¹¹² Thibaut Verbiest et Etienne Wery, op. cit.

http://www.sixi.be/Ledossier-medical-informatise-la-delicate-protection-des-donnees-personnelles_a245.html

http://www.droit-technologie.org/1_2.asp?actu_id=1048&motcle=donn%E9es+medicales&mode=motamot

¹¹³ Les juges ont récemment fait prévaloir le droit au respect de la vie privée sur le droit à l'information. TGI Paris, 3^e chambre, 3^e section 29 mai 2002

Par traitement des données personnelles il faut entendre traitement automatisé. C'est l'ensemble des opérations réalisées par des moyens automatiques relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction d'informations nominatives ; ainsi que toutes les opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communication d'informations nominatives¹¹⁴.

Les données nominatives faisant l'objet d'un traitement automatisé sont soumises à toutes les dispositions de la loi de 1978. La loi établit une distinction entre les traitements du secteur public et ceux du secteur privé. Les premiers doivent faire l'objet d'une autorisation préalable¹¹⁵ tandis que les seconds doivent simplement être déclarés¹¹⁶.

La Loi informatique et libertés¹¹⁷ a créé un cadre légal pour le traitement des données à caractère personnel en France. Elle pose deux catégories de règles à respecter. La première catégorie vise à protéger le droit des personnes et prévoit sept prérogatives en faveur des personnes fichées¹¹⁸.

- Droit à l'information préalable¹¹⁹.
- Droit d'accès direct et indirect¹²⁰.
- Droit de curiosité.
- Droit de communication.
- Droit de rectification¹²¹.
- Droit d'opposition¹²².
- Droit à l'oubli.

¹¹⁴ M-P. Fenoll-Trousseau, G. Haas, Internet et protection des données personnelles, p.14.

¹¹⁵ Loi n° 78-17, 6 janvier 1978 article 15

¹¹⁶ Id, article 16

¹¹⁷ Loi n°78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés : JO 7 janvier.

¹¹⁸ La directive du 24 octobre 1995 sur le traitement des données personnelles énonce des principes similaires ; en son article 10, droit d'information préalable, droit d'accès aux données en son article 12, droit de contestation et de modification, d'opposition en son article 14, principe de loyauté du traitement, du respect de sa finalité, conservation nécessaire à la réalisation de la finalité en son article 6. Une nouveauté est à noter cependant par rapport à la loi de 1978, le principe de la nécessité du consentement de la personne pour le traitement des données est consacré à l'article 7 de la directive. Principe assorti cependant d'un certain nombre d'exceptions.

¹¹⁹ Article 27 Loi 1978 : Les personnes concernées par les données qui vont être traitées doivent bénéficier au préalable d'un certain nombre d'information : caractère obligatoire ou facultatif des réponses, conséquences à leur égard, les destinataires des informations, droit d'accès et de rectification.

¹²⁰ Loi 1978 art.34 et 35

¹²¹ Id, art.36

¹²² Id, art.26

La deuxième catégorie est constituée de principes encadrant la collecte, le traitement et la conservation des données personnelles. Il s'agit de :

- La finalité du traitement : le traitement doit répondre à une finalité particulière, dûment déterminée.
- La loyauté : l'article 25 de la loi de 1978 dispose que « la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».
- L'obligation de sécurité.
- La protection des données dites sensibles.

Le traitement des données personnelles représente un danger pour les personnes d'un double point de vue ; lors de leur collecte et selon l'usage qui en fait notamment dans le cas de transferts.

1. La collecte des données personnelles des mineurs et auprès des mineurs.

« Au hasard de leurs pérégrinations sur le Web, les internautes sont souvent appelés à se dessaisir d'informations les concernant »¹²³.

La collecte des données personnelles n'est pas en elle-même illicite. La loi 1978 n'interdit pas la création de fichiers nominatifs, elle en régleme simplement les modalités et les utilisations¹²⁴. Seule la collecte d'informations par un moyen frauduleux, déloyal, illicite ou malgré l'opposition légitime de la personne visée est condamnée par le code pénal français en son article 226-17 à 22.

La collecte de données personnelles sur Internet présente les plus grands risques pour les utilisateurs car l'évolution technique rend la collecte plus facile et rentable¹²⁵. Il existe plusieurs types de données personnelles pouvant être collectées sur Internet. Les données

¹²³ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, Droit@Litec2002, p.24.

¹²⁴ M-P. Fenoll-Trousseau, G. Haas, Internet et protection des données personnelles, Litec 2000, p.11.

¹²⁵ Erika Orengo, La protection des personnes dans le cadre des flux transfrontières de données personnelles, DESS droit de l'informatique sous la direction de J Huet 2000-2001, p.9 ; M-P. Fenoll-Trousseau, G. Haas, Internet et protection des données personnelles, Litec2000, p.2.

volontairement livrées par la personne concernée, les données de connexion et les données de navigation¹²⁶ inconsciemment semées par la personne concernée.

La collecte de données personnelles sur Internet représente encore plus de risque pour les personnes lorsqu'il s'agit de mineurs. Le danger est double : lorsque sont collectées les données personnelles du mineur, et lorsque des données concernant d'autres personnes sont recueillies auprès du mineur.

Jean Frayssinet dit que «... *l'internaute, de manière directe ou indirecte, visible ou invisible, volontaire ou involontaire livre, comme le Petit Poucet semait des petits cailloux, des données directement ou indirectement personnelles ou des traces, qui donnent lieu à un fichage traditionnel...* »¹²⁷. Il existe deux moyens de procéder à la collecte de ces données : de manière directe ou indirecte.

1-a. La collecte directe.

La collecte de données personnelles à des fins commerciales ou non, vise la constitution de fichiers nominatifs ou les individus sont classés selon des critères plus ou moins objectifs.

Les enfants sont souvent de meilleurs internautes que les adultes ou du moins des internautes plus assidus. Faute de maturité et d'expérience civique ils constituent des cibles idéales¹²⁸ dans la collecte des données personnelles quel que soit le but de cette collecte.

Dans l'absolu, les internautes ont conscience de devoir se dépouiller d'informations personnelles lorsqu'ils sont appelés à remplir un formulaire en ligne. Des sondages américains font apparaître que 41% des internautes renonçant à livrer des informations personnelles préfèrent se déconnecter tandis que 40% choisissent de mentir¹²⁹. Mais cette

¹²⁶ Sophie Louveaux, Comment concilier le commerce électronique et la protection de la vie privée ? Droit des technologies de l'information. Regards prospectifs, sous la direction d'Etienne Montero, Cahier du centre de recherche informatique et droit, Bruylant. Bruxelles 1999, p.151-152.

¹²⁷ J. Frayssinet, Internet et la protection juridique des données personnelles, Colloque international. Internet et le droit, 26 septembre 2000.

¹²⁸ Internet, les jeunes et la protection des données personnelles et de la vie privée.

www.cnil.fr/juniors/fiches/fiches1.pdf/

¹²⁹ J. Boyer, Internet et la protection des données personnelles et de la vie privée : Cahier français, mars-avril 2000, p.74 et s., spéc. , p.75.

réaction est elle attribuable à tout internaute ou alors faut t-il y voir la marque d'internautes particulièrement avisés.

La collecte directe ne peut avoir lieu qu'avec le consentement¹³⁰ ou du moins la participation consentie de l'internaute. Mais, le fait est que tous les internautes ne sont pas égaux devant cette collecte, les mineurs étant considérés comme les plus vulnérables et les plus malléables.

La collecte des données personnelles auprès des mineurs entraîne une interrogation quant à la probité de certains sites Web dédiés aux enfants. Une enquête¹³¹ a montré en la matière que, alors que 8 sites sur 10 collectent des données personnelles, seuls 4 sites sur 10¹³² présentent une déclaration relative au respect de la vie privée. Lorsqu'elle apparaît, cette information légalement obligatoire est souvent incomplète¹³³.

D'entrée de jeu se pose la question de la validité de la collecte auprès des mineurs, qu'il s'agisse ou non de leurs données personnelles. En principe, le consentement du mineur n'a de valeur que s'il est corroboré par celui d'un parent ou du moins d'un majeur responsable.

De manière générale, l'internaute qui souhaite réaliser une transaction électronique livre de lui-même ses données personnelles afin de permettre la réalisation de la transaction. Il fournira par exemple son nom son adresse en vue de la livraison de biens commandés¹³⁴.

¹³⁰ Le principe de la nécessité du consentement est consacré à l'article 7 de la Directive du 24 octobre 1995 sur le traitement des données à caractère personnel. Il s'agit d'une nouveauté par rapport à la loi de 1978 qui posait simplement le principe d'un droit d'opposition. Il existe cependant des exceptions à ce principe de consentement. C'est le cas en matière de commerce électronique quand le traitement a lieu dans le cadre de l'exécution d'un contrat art. 7b ; le consentement n'est pas exigé lorsque le traitement répond à un intérêt légitime de son responsable ou d'un tiers qui aurait communication des données, dans la mesure où ne prévalent pas l'intérêt ou les droits fondamentaux de la personne concernée.

¹³¹ Enquête a été réalisée par l'université d'Anvers en Belgique et diligentée par le Monsieur le professeur Michel Walrave en 2005. Il n'est pas précisé si les sites (294 en tout) sont tous ou non belges. Cette enquête paraît en intégralité sur les sites suivants :

www.safeinternet.be

www.e-privacy.be

¹³² 82% des sites pour enfants collectent les données et seulement 39% présente une déclaration relative à la vie privée, 81% demandent le nom du visiteur, 87% demandent des coordonnées telles l'adresse e-mail, 54% demandent l'adresse du domicile, 32% demandent le numéro de téléphone, 19% demandent le numéro de GSM, 37% demandent les caractéristiques personnels exemple âge et pour 15% le sexe, pour 7% les passe-temps et pour 6% la nationalité et enfin pour 5% l'éducation scolaire, Enquête du professeur Michel Walrave préc.

¹³³ Etienne Wery, 7 novembre 2005, voire le Site Droit & Nouvelles technologies.

http://www.droit-technologie.org/1_2.asp?actu_id=1125

¹³⁴ Sophie Louveaux, comment concilier le commerce électronique et la protection de la vie privée ? Droits des technologies de l'information. Regards prospectifs, sous la direction d'Etienne Montero, Cahier du centre de recherche informatique et Droit, Bruylant Bruxelles 1999, p.152

Il existe diverses manières de collecter des données auprès des mineurs. Il est possible par le biais de formulaires, de jeux, de forum de discussion, de collecter directement des données personnelles auprès du mineur.

1.a'. La collecte par le biais des formulaires et jeux.

Les publicitaires collectent des informations en invitant les mineurs à remplir des formulaires pour pouvoir jouer sur le net et participer à des concours. Il semblerait que 59% des mineurs ciblés se disent prêts à donner leur nom et d'autres renseignements personnels pour courir la chance de gagner un prix à un concours : 52% donneraient leur adresse de courriel¹³⁵.

Les jeux et concours en ligne constituent une des raisons qui motivent les mineurs à passer beaucoup de temps sur la Toile. Certains sites ont une vocation éducative tandis que d'autres ont une vocation purement mercantile. D'un point de vue légal, les mineurs doivent être assistés dans toutes ces activités par un majeur responsable, qui doit valider leur consentement par le sien propre. C'est dans ce sens que l'association canadienne du marketing a amendé son code de déontologie pour y ajouter des clauses concernant la vente et la promotion auprès des mineurs de moins de treize ans¹³⁶. Ces directives insistent sur l'obligation de ne pas recueillir d'informations auprès des enfants sans le consentement exprès des parents.

Dans le même esprit, aux Etats-Unis, la Children Online Privacy Protection Act (COPPA) adopté par le Congrès en octobre 1998 et entrée en vigueur en avril 2000 énonce que, aucune information personnelle ne doit être recueillie en ligne auprès d'un enfant de moins de treize ans sans le consentement de ses parents ou d'un tuteur légal. Ce consentement doit être vérifiable, soit sous la forme d'un formulaire d'autorisation envoyé par courrier postal ou télécopie, ou directement par le biais d'un numéro de téléphone sans frais de la compagnie. Ce texte concerne les sites commerciaux basés aux Etats-Unis qui s'exposent à des amendes en cas de non respect.

La réalité est cependant loin de cet énoncé, tout au moins en ce qui concerne le Canada ; ces précautions ne sont pas toujours respectées par toutes les parties Le Réseau Education-Médias montre que 80% des jeunes sont seuls quand ils naviguent sur Internet et que la plupart des

¹³⁵ La protection de la vie privée et les jeunes, Réseau éducation-Médias.

www.education-medias.ca/francais/enjeux/vie-privée-enjeu.cfm

¹³⁶ Cet amendement est intervenu en avril 1999 et paru sur le site Réseau éducation-médias

parents ignorent tout des activités de leurs enfants en ligne. 65% d'entre eux pensent que leurs enfants utilisent essentiellement la Toile pour leurs travaux scolaires, alors que 56% des jeunes citent le courriel comme étant leur activité préférée ; 50% naviguent pour le plaisir ; 40% utilisent les messageries instantanées et 39% fréquentent des bavardoirs¹³⁷. Autant d'activités qui se prêtent à la divulgation même involontaire d'informations personnelles¹³⁸.

La collecte directe des données personnelles auprès des mineurs concerne autant le secteur public que le secteur privé. Le secteur public est concerné à une moindre échelle. Ceci s'explique en grande partie par le fait que les démarches administratives sont effectuées en majorité par des adultes. Nous allons tout de même envisager ce cas de figure.

Il existe plusieurs modes de collecte des données personnelles auprès des mineurs. Dans la catégorie des collectes consenties et donc directes, nous avons les formulaires de toutes natures complétés en ligne. Nous avons également les forums de discussions où la collecte quoique directe doit être nuancée.

Qu'en est-il de l'état du droit sur la collecte des données auprès des mineurs en France, en Europe et aux Etats-Unis ?

1.a". La réglementation de la collecte des données auprès des mineurs.

En France, aucun texte ne régleme de façon précise la problématique liée à la collecte des données personnelles des mineurs. L'article 488 du code civil (portant sur la majorité du mineur) et l'article 2 du code de commerce modifié par la loi du 5 juillet 1974 (qui énonce que « le mineur même émancipé ne peut être commerçant ». Cette incapacité l'empêcherait d'engager son patrimoine mais aussi de prendre des décisions concernant sa personne). Une lecture combinée de ces deux articles permettrait-elle de conclure dans le domaine de la collecte des données personnelles qu'une telle collecte auprès des mineurs serait illégale ?

La loi de 1978 garantit à tous trois droits : information, accès et opposition. Ces dispositions encadrent la protection des données personnelles des individus en général et elles

¹³⁷ Forum de discussion

¹³⁸ www.education-medias.ca/français/enjeux/vie-privée_enjeu.cfm

n'appréhendent pas suffisamment les problématiques liées à l'usage d'Internet par des mineurs selon un constat de la CNIL.

La loi du 6 janvier 1978 pose dans son article 40-6, un principe en matière de fichiers ayant pour fin la recherche dans le domaine de la santé. En vertu de ce texte, ce sont les « titulaires de l'autorité parentale » qui exercent les droits prévus au bénéfice de toute personne mineure fichée : droit à l'information, droit d'opposition, d'accès et de rectification des données la concernant.

Une recommandation de la CNIL du 1^{er} avril 1980 relative aux modalités du droit d'accès¹³⁹, semble poser un principe plus général en indiquant que, « s'agissant d'un droit strictement personnel, celui-ci ne peut être exercé que par son titulaire et le mandat ne peut être utilisé, selon les règles du droit commun que pour les mineurs et incapables majeurs¹⁴⁰.

La CNIL a déjà eu à se prononcer sur un cas de collecte de données auprès de mineurs sous la forme d'une recommandation en date du 22 octobre 1985. Saisie d'une plainte concernant la diffusion d'un questionnaire auprès des élèves d'un collège, la CNIL avait considéré que cette enquête, auprès d'enfants mineurs, aurait du être précédée d'une demande d'accord écrit des parents. Depuis, la CNIL estime que l'accord écrit des parents est nécessaire pour la diffusion d'une photo d'enfant sur Internet, ainsi que pour la cession des coordonnées d'un enfant mineur en matière de marketing¹⁴¹.

Dans la recommandation du 22 octobre 1985, la CNIL précise qu'un mineur ne peut être soumis à des tests ou épreuves à caractère psychotechnique ou psychologique sans l'accord écrit de la personne qui en assure la responsabilité légale. Cela va plus loin ; en 1997 lors de l'examen des traitements d'informations nominatives mis en œuvre dans le cadre d'un site Internet ministériel, la commission a demandé que la rubrique « courrier électronique », destinée à recevoir des courriers en provenance de jeunes, comporte une mention très explicite afin de pas inciter ces derniers à donner leur nom de famille et l'adresse de leur domicile. En revanche les jeunes peuvent être encouragés à indiquer s'ils le souhaitent leur

¹³⁹ Délibération n°80-010 1^{er} avril portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés

¹⁴⁰ <http://www.>

¹⁴¹ http://www.clic-droit.com/web/editorial/dossier.php?dossier_id=7

prénom, leur pseudonyme, l'indication de leur commune et pays de résidence, leur classe (niveau)¹⁴².

La déclaration des traitements de données personnelles mise en œuvre dans le cadre d'un site Internet doit systématiquement indiquer si le site est particulièrement destiné aux mineurs¹⁴³. Selon l'article 27 de la Loi de 1978, les titulaires du site ont l'obligation d'informer les internautes lors de la collecte des données du caractère obligatoire ou facultatif des réponses qu'ils sont invités à fournir, des personnes ou des organismes destinataires des informations, de l'existence d'un droit d'accès aux informations qui les concernent et du lieu où il s'exerce. La CNIL conclut son rapport en disant que la collecte d'information auprès des mineurs concernant l'entourage familial, le mode de vie des parents, leur statut social professionnel, doit être considérée comme excessive et déloyale. Les jeux et loteries proposés aux enfants ne doivent pas conduire à céder à des tiers les données ainsi recueillies, sauf accord exprès des parents.

Les recommandations de la CNIL n'ont aucune valeur contraignante en matière de collecte de données personnelles auprès des mineurs, et elles ne sont relayées par aucun texte légal ayant valeur contraignante. De plus, elles ne proposent en aucun moment la mise en place d'un régime d'autorisation préalable à la collecte des données auprès des mineurs¹⁴⁴. Cette loi a créé un site junior pour sensibiliser et apprendre aux enfants à surfer sans dévoiler des données sur leur vie privée.

A la question de savoir si en France la collecte de données personnelles auprès des mineurs est possible la réponse est oui mais en respectant une double condition :

- Recueillir le consentement préalable des parents à qui l'on doit donner les moyens de s'opposer à la collecte.
- Fournir une information claire aux mineurs.

¹⁴² Rapport de la CNIL du 12 juin 2001, Internet et la collecte des données personnelles auprès des mineurs, Cécile Alvergnat.

¹⁴³ Rubrique III du formulaire simplifié et électronique de déclaration.

¹⁴⁴ Indragandhi Balassoupramaniane, Le journal du barreau volume 33 n°19 15 novembre 2001.
<http://www.barreau.qc.ca/journal/Frameset.asp?article=/journal/vol33/no19/droitcompare.html>

Il est cependant admis que le webmestre d'un site auquel un jeune est connecté puisse collecter l'adresse électronique et l'âge du mineur pour lui envoyer une lettre d'information. Le recueil de toute autre information est considéré comme non conforme à une telle finalité.

En Europe, le Conseil de l'Union européenne a rendu une recommandation en date du 24 septembre 1998 concernant « le développement de la compétitivité de l'industrie européenne des services audiovisuels et d'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de protection des mineurs et de la dignité humaine ». Il s'agit là d'un acte juridique non contraignant qui n'aborde pas la protection des mineurs à l'égard de la collecte et de la diffusion de leurs données personnelles¹⁴⁵.

Aux Etats-Unis, en mars 1998 la Federal Trade Commission (FTC) du département du commerce américain publiait les résultats d'une enquête portant sur les données recueillies par les sites de commerce. Selon cette étude, 89% des sites qui s'adressent aux enfants récoltent des informations personnelles sur leurs jeunes visiteurs (nom, âge, adresse, centre d'intérêts, numéro de sécurité sociale, etc....) et sur leurs parents. Plus encore, ces sites conditionnent leur accès aux mineurs par un recueil d'information. 54% de ces sites informent sur l'utilisation ultérieure des données recueillies ; 12% offrent un droit d'accès et de modification et seulement 1% réclament un accord parental préalablement à toute collecte¹⁴⁶.

Une étude datant de janvier-février 2000 auprès de 1001 parents d'internautes âgés de huit à dix-sept ans et de 304 enfants de dix à dix-sept ans. Cette étude révèle que, avec la promesse d'un cadeau 65% des jeunes sont prêts à donner des informations sur leurs boutiques favorites et 54% prêts à livrer des précisions sur les marques préférées de leurs parents.

Ces résultats ont amené la FTC à proposer la mise en place d'une législation spécifique sur la question. C'est ainsi que le Children's Online Privacy Protection Act (COPPA) a vu le jour le 21 avril 2000.

- Tout site est obligé de requérir une autorisation parentale avant une demande de renseignements personnels auprès d'un enfant de moins de treize ans. Les

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

informations recueillies doivent être accessibles et les parents peuvent obtenir leur suppression en indiquant qu'ils révoquent leur accord.

- Il y a une obligation à l'encontre des responsables de sites. Obligation d'afficher clairement la politique de recueil des données, de prévenir les parents des enfants si leur politique change ou de fournir un contact avec une adresse courriel, une adresse postale et un numéro de téléphone.

Certains sites à l'instar d'eCrush ont décidé d'interdire l'accès à leur service aux mineurs de moins de treize ans ; Hotmail, Yahoo et Disney.com ont quant à eux pris l'initiative de demander aux parents une autorisation sous forme de numéro de carte bancaire afin de s'assurer l'authenticité des autorisations recueillies.

Les Etats-Unis sont le pays le plus à la pointe en matière de la réglementation de la collecte de données personnelles auprès des mineurs. C'est l'un des premiers pays à s'être doté d'une législation sur Internet et les mineurs.

1-b. La collecte indirecte.

« Il existe plusieurs types de données personnelles pouvant être collectées lors de l'utilisation d'Internet : les données livrées par la personne concernée elle-même, les données de connexion et les données de navigation »¹⁴⁷. Si la personne navigue sur Internet sans livrer elle-même ses données personnelles, elle laissera nécessairement des traces. Il est donc nécessaire de mettre sur pied une protection des internautes (notamment les plus vulnérables) afin qu'ils ne soient pas suivis à leur insu grâce aux traces électroniques qu'ils laissent¹⁴⁸.

Comme l'intitulé l'indique, la collecte indirecte des données auprès des mineurs s'effectue de manière indirecte. Elle s'opère de plusieurs manières ; une collecte directe peut devenir indirecte dans un processus de traitement des données. Les données de connexion et de navigation sont un des moyens pour collecter indirectement des données. La collecte indirecte est également possible dans les forums de discussion et par le biais de captations d'adresse email.

¹⁴⁷ Sous la direction de Etienne Montero, Droit des technologies de l'information. Regards prospectifs ; Cahier du centre de recherche informatique et droit, Bruylant Bruxelles 1999 p.151-152.

¹⁴⁸ M-P. Fenoll-Trousseau, G. Haas, Internet et protection des données personnelles, p.2

La collecte indirecte de données, réalisées à l'insu des intéressés, s'effectue essentiellement à partir de cession de données.

1.b'. La collecte indirecte sur les forums de discussion.

L'internaute mineur est souvent amené à se dessaisir volontairement d'informations personnelles le concernant lui ou son entourage familial. Un danger réel découle de l'usage qui peut être fait de leurs données personnelles et dont ils n'ont pas connaissance, ou dont-ils n'ont pas conscience¹⁴⁹. C'est le cas par exemple pour les données qui sont cédées dans les forums de discussion.

La collecte indirecte de données sur les forums de discussion peut être le fait de producteurs de sites Internet par le biais de fichier « log »¹⁵⁰.

La CNIL, rappelant aux responsables de ces instruments de discussion la réglementation en matière de protection des données personnelles, a recommandé que les utilisateurs de forums soient informés de l'interdiction d'utiliser les informations qu'ils auront révélées à d'autres fins que celles ayant justifiées leur communication¹⁵¹.

L'absence de mention d'interdiction de collecte sur des sites ne suffit pas à assurer le caractère licite et loyal de la collecte des mès. La CNIL recommande à tous les sites d'indiquer clairement aux tiers « qu'une donnée diffusée sur Internet, dans un annuaire ou un espace de discussion, ne peut pas être utilisée à d'autres fins que celles qui ont justifiées sa diffusion, sauf à s'assurer préalablement du consentement de la personne concernée ». La commission s'est également interrogée sur le point de savoir « s'il ne conviendrait pas de s'accorder sur une interdiction pure et simple de l'utilisation à des fins de prospection commerciale de mès collectés à partir de forum de discussion non commerciaux¹⁵² ».

¹⁴⁹ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, Litec, page 24

¹⁵⁰ Ce sont des fichiers regroupant les données relatives aux consultations effectuées par les internautes permettant la détection d'intrusion ainsi que l'estimation de la fréquentation du site Internet.

Erika Orengo, La protection des personnes dans le cadre des flux transfrontières de données personnelles, DESS Droit de l'informatique et du multimédia sous la direction de J Huet.

¹⁵¹ CNIL, Rapport d'activité 1996, La Documentation Française, p.92

¹⁵² Les conditions de collecte des données. <http://www.educnet.education.fr/juri/vieprivee/collecteA.htm>

Le problème juridique qui se pose ici est celui du principe de finalité. Il s'agit conformément à la directive 95/46 du 24 octobre 1995, de respecter la finalité des espaces de discussions et des listes de diffusion. Une personne qui a eu recours à la messagerie électronique pour s'exprimer dans un espace de discussion déterminé et pour un sujet précis, ou qui s'est inscrite dans une liste de diffusion pour partager des informations avec un groupe d'interlocuteurs intéressés par un sujet commun n'a par hypothèse pas consenti, même implicitement à la cession de ses informations personnelles à d'autres fins.

Ce qui fait défaut dans ce type de collecte indirecte, c'est l'absence de consentement de la personne intéressée. Conformément aux articles 10 et 11 de la directive 95/46, une obligation d'information pèse sur le collecteur de données, cette obligation doit être accomplie au moment de la collecte des données ou, si une cession à un tiers est envisagée, au plus tard, lors de leur première transmission à des tiers¹⁵³. Ces normes ne sont pas assorties de sanctions et n'interdisent pas formellement la collecte indirecte de données.

Les mineurs sont de grands utilisateurs de forums de discussions¹⁵⁴ ; ils se retrouvent souvent sur des forums « communautaires » ou des chats. Ils y ont parfois des relations pouvant sortir du cadre du cyberspace, pour ce faire ils peuvent dans certaines circonstances être amenés à échanger leurs coordonnées personnelles afin de poursuivre le contact en dehors des forums. Il en résulte de nombreux risques dont il sera question dans des développements à venir.

Le principe de la finalité de la collecte n'est pas très bien respecté dans les forums la menace est potentiellement accrue par la nature des relations que le mineur noue sur la Toile et qui pourraient lui être préjudiciables. On pense notamment aux prédateurs de toutes natures qui pourraient se servir des informations données par le mineur pour lui nuire. Le mineur n'a pas toujours conscience que, son interlocuteur sous de faux prétextes et de faux profils peut lui soutirer des informations personnelles sur lui ou son entourage familial à des fins délictuelles.

¹⁵³ La véritable portée du problème : la collecte des emails dans les espaces publics d'Internet
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/d99_048c.pdf

¹⁵⁴ 4.5% des six millions d'internautes recensés en France ont moins de quinze ans ; 63 millions d'internautes aux Etats-Unis en 1999, avec 1.25 millions d'internautes âgés de 9 à 17 ans qui possèdent la connexion à domicile et qui avouent y passer environ deux heures par jour ; Cécile Alvergnat, Rapport de la CNIL du 12 juin 2001, rédacteurs, Fatima Hamdi et Jean-Paul Macker, Internet et la collecte de données personnelles auprès des mineurs , www.cnil.fr

1.b". La collecte indirecte par le biais des traces électroniques.

i. Les cookies.

Le « cookie » est un petit fichier qui sera téléchargé en fin de connexion par le serveur sur le micro-ordinateur de l'internaute. Il enregistre le parcours de navigation effectué, parcours qu'il est susceptible de relire lors de la connexion suivante afin d'optimiser la navigation.

On distingue les cookies de session et les cookies rémanents. Les cookies de session ne contiennent pas de date d'expiration et sont automatiquement détruits lorsque l'internaute ferme la session ouverte ou une page sur Internet. Les cookies rémanents contiennent eux, une date d'expiration fixée par leur auteur et sont destinés à permettre au serveur Web d'accéder aux informations qu'il contient jusqu'à l'échéance de ce terme.

Les cookies peuvent contenir des informations fournies par l'internaute lors de ses visites (date de naissance, achats...). Ils peuvent enregistrer des données à l'insu de l'internaute comme les caractéristiques de la machine qu'il utilise (processeur, système d'exploitation, logiciels ...) ¹⁵⁵.

Dans des sites qui comportent 40 000 pages comme celui de Microsoft, cela peut être d'une aide certaine, mais on voit facilement les dérives que cela peut entraîner avec la constitution de bases de données et la mise en place de logiciels d'analyse de comportements permettant la constitution de profils.

L'inscription sur le disque dur de l'internaute que nécessite les cookies pourrait permettre d'invoquer certaines dispositions du code pénal notamment l'article 323 alinéa premier, qui punit de deux ans d'emprisonnement et de 30 000€ d'amendes « *le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* » ¹⁵⁶. Par ailleurs, les principes posés par la loi informatique et libertés restent applicables. Les utilisateurs doivent être informés de la création des "cookies" et ils peuvent

¹⁵⁵ Julien Hans, Cookies et vie privée : le Conseil de l'Union Européenne adopte une position commune, 18 février 2002

¹⁵⁶ Code pénal, chapitre III Des atteintes aux systèmes de traitement automatisé de données, art. 323-1 ordonnance n°2000-916 du 19 septembre 2000 article 3, Journal Officiel du 22 septembre 2000 entrée en vigueur le 1^{er} janvier 2002 ; Loi n°2004-575 du 21 juin 2004 article 451 du Journal Officiel du 22 juin 2004.

s'y opposer en désactivant cette fonction dans leur navigateur. La CNIL précise que les internautes doivent pouvoir en connaître la teneur de manière intelligible¹⁵⁷.

Alors que la CNIL n'adhérait pas totalement aux dispositions contenues dans la directive du 15 décembre 1997 concernant les traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, les dispositions de la Directive 2002/58/CE semblent être plus en adéquation avec les recommandations de la CNIL¹⁵⁸. La directive Vie privée et communication électronique du 12 juillet 2002¹⁵⁹ a pour objet, entre autre la réglementation des cookies. En son article 5 § 3, la directive pose le principe selon lequel l'internaute doit être informé du traitement et qu'il a le droit de le refuser.

L'auteur Jean Frayssinet énonce au sujet de la collecte de données opérées par le biais de cookies que, ces données ne sont pas des données personnelles mais des données relatives à l'ordinateur, l'internaute restant anonyme. L'auteur atténue son propos en admettant que, en s'adressant à un ordinateur identifié on s'adresse néanmoins à une personne quoique non identifiée. La personne, le consommateur ne font qu'un avec la machine qui devient transparente. Il y a là un passage de l'information anonyme à l'information indirectement personnelle¹⁶⁰.

Les internautes mineurs sont plus vulnérables que les autres internautes devant la collecte indirecte des données par la technique des cookies. Leur vulnérabilité s'observe d'un double point de vue. D'une part les responsables de sites collectent à leur insu leurs données personnelles, d'autre part leurs parents ou tuteurs légaux peuvent exercer un contrôle détaillé de leur navigation sur Internet, par date et par heure grâce à l'historique automatiquement mise à jour par les cookies. La navigation du mineur fait l'objet d'un traçage ayant pour but du point de vue parental leur protection ; cette surveillance peut être déjouée par un mineur expérimenté qui aura pris la peine d'effacer ses traces au fur et à mesure¹⁶¹.

¹⁵⁷ Internautica ; Les données privées, 15 novembre 1999

http://www.internautica.tm.fr/rubriques/donnees_privées/donnees3.htm

¹⁵⁸ Patrick Hauss, Vie privée et communications électroniques : où en sommes nous ?

http://www.clic-droit.com/web/editorial/imprimer.php?art_id=149

¹⁵⁹ JOCE L.201, 31 juillet. 2002, p.0037-0047, voir P.-Y Gautier, le droit au respect de la « vie privée électronique » est en marche : Comm. Com. Electr. Octobre 2002, p.2 et 3.

¹⁶⁰ J. Frayssinet, Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs, Libertés individuelles à l'épreuve des NTIC, Lyon PU 2001, p.39

¹⁶¹ Stéphane Arteta, M. Lemonnier, S. Noucher et C. Soula, Votre enfant et Internet, Comment suivre sa trace ?, Le Nouvel Observateur, 22 novembre 2001.

ii. La collecte par les données de connexion.

Les données de connexion font partie des traces électroniques que l'on sème sur Internet. Les travaux sur ordinateur ont aussi une série d'effets secondaires. Chaque activité, même aussi simple que le fait d'écrire une lettre ou de copier un texte laisse plusieurs traces à partir desquelles il est possible de reconstruire l'historique de son activité sur un ordinateur et plus encore sur Internet. Le potentiel d'intrusion dans la vie privée par la manipulation des données personnelles est énorme¹⁶².

- Les logfiles (fichiers journal) sont les traces électroniques parmi les plus connues. Ils sont configurables, c'est-à-dire qu'ils permettent de choisir quelles informations doivent être collectées et dans quelles circonstances. Pour les contrôler techniquement, on peut leur définir une durée maximale ou une taille maximale.
- Il existe des logiciels de dernière génération « eavesdrop/wiretop logfiles » qui permettent de surveiller l'ensemble des activités exécutées, en stockant localement les données capturées ou en les envoyant discrètement (par exemple par courriel caché). Il permet également de capturer la saisie dans tout envoi ou réception de courriel par l'utilisateur, donc aussi des mots de passe qu'il aura introduit.

Chaque trace électronique contenant des données personnelles est une collecte de données au sens de la loi fédérale sur la protection des données en Suisse¹⁶³.

Quelle est la loi applicable en matière de traitement et, en l'occurrence de collecte des données personnelles dans l'Union Européenne ? Lorsque le responsable de traitement est établi sur le territoire de l'Union Européenne, il devra se soumettre à la directive 2002/58, telle que transposée par la loi nationale de son établissement. Lorsqu'il existe plusieurs responsables de traitement qui sont établis dans différents Etats membres, plusieurs lois nationales s'appliqueront concurremment. Cette solution est fournie par la Directive européenne. Néanmoins, certains pays ont transposé ce principe avec certaines divergences.

Par exemple, selon la loi grecque, la loi nationale s'applique dès lors qu'un traitement concerne des données de personnes établies en Grèce, même si le responsable de traitement

¹⁶² Traces électroniques et données personnelles, Berne mars 2004

http://www.edsb.ch/f/themen/sicherheit/technik/elektronische_spurenf.pdf

¹⁶³ Ibid.

n'y est pas établi. En Italie, la loi nationale s'applique dès que le traitement est réalisé sur le territoire italien. En Autriche, la loi nationale s'applique à toute utilisation de données dans le pays. En France, rien n'est prévu concernant l'application territoriale du fait que la loi est antérieure à la directive européenne, et n'a dès lors qu'un contexte national.

Différentes lois nationales peuvent s'appliquer concurremment du fait que les Etats membres n'ont pas adopté de critères communs dans le cadre de normes communes¹⁶⁴.

2. Le transfert des données personnelles des mineurs.

Les progrès technologiques des réseaux de télécommunication, permettent aux données personnelles de passer les frontières avec une grande facilité. Cette facilité a pour conséquence que les données concernant les citoyens d'un Etat membre sont souvent exploitées dans d'autres Etats membres de l'EU. Le flux d'échanges des données personnelles entre les Etats membres allant croissant, une réglementation concernant les transferts de données s'est avérée indispensable¹⁶⁵.

Les législations nationales relatives à la protection des données exigeaient jusqu'alors une "bonne gestion" des données de la part des organes gérant les données : les responsables de fichiers. Ces derniers ont l'obligation de gérer les données loyalement, dans des conditions sûres, et de les utiliser à des fins explicites et légitimes. Les législations nationales ont aussi garanti une série de droits aux personnes, tel le droit d'être informé lorsque des données personnelles sont traitées et de s'en voir communiquer la raison, le droit d'accéder aux données et, le cas échéant le droit de faire modifier ou supprimer ces données.

Bien que les législations nationales relatives à la protection des données visent à garantir les mêmes droits, certaines différences ont subsisté en pratique. Ces différences pouvaient potentiellement créer des obstacles à la libre circulation de l'information et constituer des fardeaux supplémentaires pour les opérateurs économiques et les citoyens tributaires de la circulation des données personnelles.

¹⁶⁴ IPR Helpdesk (financé par la Commission européenne, DG entreprises et industrielles sous le sixième programme cadre de RDT de l'Union Européenne), La protection des données à caractère personnel dans le cadre du commerce électronique. <http://www.ipr-helpdesk.org/docs.FR/personalData.html#N1004B>

¹⁶⁵ Protection des données dans l'Union Européenne, Europe direct, Dialogue avec les citoyens et les entreprises, p.3 http://europa.eu.int/comm/justice_home/fsj/privacy/guide/index_fr.htm

Les opérateurs avaient l'obligation de s'enregistrer ou d'être autorisés à gérer des données par des autorités de surveillance dans plusieurs États membres. Ces conditions répondaient à la nécessité de se conformer à des normes différentes, la possibilité d'être interdit de transfert de données vers d'autres États membres de l'Union européenne. Il existait même des hypothèses ou, certains États étaient dépourvus de législation en la matière. Pour toutes ces raisons, il était nécessaire de réguler cette question à l'échelle européenne, et les directives CE se sont inscrites dans cette perspective¹⁶⁶.

La collecte des données personnelles n'est pas un but en soi. Il ne s'agit pas simplement de constituer des bases de données. Le fait que ces données soient collectées dans le but d'être utilisées est une évidence qui de surcroît est légale. Le problème de la légalité et de la légitimité de ces collectes se pose à partir du moment où la finalité de cette utilisation n'est pas en adéquation avec celle qui avait été préalablement annoncée aux personnes concernées par la collecte des données. La question de la légitimité ou de la légalité est plus cruciale lorsque les titulaires des données n'ont pas été préalablement informés de la collecte de leurs données et donc inévitablement de l'utilisation de ces données.

2-a. Le transfert des données personnelles du mineur au sein de l'Union Européenne.

La cession nationale ou intracommunautaire. La protection accordée par la loi de 1978 ne s'applique qu'aux cas de cessions de fichiers sur le territoire français. Au sein de l'Union Européenne c'est la directive du 24 octobre 1995 qui s'applique.

2.a'. Le système de la loi informatique et liberté du 6 janvier 1978.

Le transfert et la cession de données personnelles sont autorisés en France par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après *Loi 1978* ou *Loi Informatique et Libertés*). Elle vise la protection des données personnelles face à l'informatisation grandissante de l'administration, mais aussi des entreprises privées. Elle vise aussi bien le secteur public que privé (article 14 *Loi 1978*) : le premier est soumis à un avis

¹⁶⁶ Ibid., p.3-4

préalable (article 15 *Loi 1978*) alors que le second doit simplement déclarer ses intentions (article 16 *Loi 1978*) à la Commission Nationale de l'Informatique et des Libertés (CNIL)¹⁶⁷.

Selon le système instauré par cette loi, à l'occasion de la déclaration faite auprès de la CNIL, il doit être précisé si les données sont destinées à être transférées à l'étranger. Si c'est le cas, l'article 24 de la loi stipule que ce transfert peut être soumis à une autorisation préalable¹⁶⁸.

La déclaration auprès de la Commission liberté consiste à établir l'engagement selon lequel le traitement satisfait aux exigences de la loi¹⁶⁹; la déclaration peut être faite par voie électronique. La CNIL délivre en retour un récépissé, le cas échéant par voie électronique. Dès réception du récépissé le traitement peut être mis en œuvre, mais sans aucune clause exonératoire de responsabilité.

Pour satisfaire aux exigences de la loi et faire l'objet d'une déclaration simplifiée, le traitement doit respecter les éléments suivants :

- Les finalités des traitements faisant l'objet de la déclaration.
- Les données à caractère personnel ou catégories de données à caractère personnel traitées.
- La ou les catégories de personnes concernées.
- Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées.
- La durée de conservation des données à caractère personnel¹⁷⁰.

Sauf à respecter les exigences de la loi, le transfert de données ne pose pas de réels problèmes sur le plan national qui ne puissent être résolus par le droit commun. La question des flux ne peut pas se cantonner dans la réalité des faits à une dimension nationale, Internet étant un outil transfrontalier. La CNIL avait commencé à proposer des solutions au cas par cas, pour les transferts de données en dehors des frontières françaises.

¹⁶⁷ Cynthia CHASSIGNEUX, *La protection des données personnelles en France*, Lex Electronica, vol. 6, n°2, hiver 2001 <http://www.lex-electronica.org/articles/v6-2/chassigneux.htm>

¹⁶⁸ Erika Orengo, *La protection des personnes dans le cadre des flux transfrontières de données personnelles*, DESS Droit de l'informatique et du multimédia sous la direction de J. Huet, 2001-2002, p.2

¹⁶⁹ Article 23 loi informatique et libertés, modifié par Loi n°2004-801 du 6 août 2004 art. 4 (JORF 7 août 2004).

¹⁷⁰ Article 24 de la loi 1978 modifié par Loi n°2004-801 du 6 août 2004 art.4 (JORF 7 août 2004)

C'est ainsi que, dans sa délibération « Fiat France n°89-18 du 11 juillet 1989¹⁷¹, la CNIL exige la conclusion d'un contrat de protection de données entre l'expéditeur et le destinataire, lorsque celui-ci est situé dans un pays n'offrant pas un niveau de protection adéquat équivalent à la loi de 1978¹⁷². Le droit européen n'ayant pas encore régi ce point entre les membres de la Communauté, les Etats par le biais de leurs organismes de protection des données devaient procéder au cas par cas.

Sur les flux transfrontaliers de données personnelles, le droit international public est limité. La communauté européenne a donc souhaité harmoniser le droit de ses Etats membres afin que la libre circulation des données personnelles dans le cadre du Marché commun ne connaisse pas d'entrave.

2.a". Le système de la directive du 24 octobre 1995¹⁷³.

La directive a mis en place au sein de l'Union Européenne un dispositif permettant que les données puissent librement circuler en son sein. Ce dispositif se situe dans la logique de la libre circulation des biens et services telle que posée par la directive 95/46/CE. La directive est basée sur les mêmes principes que la loi française du 6 janvier 1978. Elle a vocation à s'appliquer sur le territoire de l'Union européenne. Les flux transfrontaliers de données personnelles contribuent au développement économique et social. Dès lors, la liberté de circulation de l'information entre pays membres doit être développée : en conséquence doivent être évités les obstacles injustifiés à ce développement¹⁷⁴.

Les données personnelles sont des biens informationnels ayant une valeur marchande. Elles doivent pouvoir circuler librement sur le territoire de l'Union dans le cadre d'un marché unique, afin d'éviter des disparités économiques et concurrentielles. Dans cette dynamique, les pays membres de la Communauté européenne se devaient de résoudre le problème posé par la disparité existant entre les législations nationales. Dans un premier temps, ils ont adhéré

¹⁷¹ Lors de la délibération du 11 juillet 1989, la CNIL s'est prononcée sur la transmission d'information relatives à la gestion du personnel entre la France et l'Italie, par la société Fiat. L'Italie ne disposant d'aucune législation appropriée, la CNIL a demandé à la société Fiat-Turin de s'engager contractuellement avec la société Fiat-France à respecter les dispositions de la loi française et de la Convention du Conseil de l'Europe.

¹⁷² Erika Orengo, La protection des personnes dans le cadre des flux transfrontières de données personnelles, DESS Droit de l'informatique et du multimédia sous la direction de J. Huet, 2001-2002, p.2-3.

¹⁷³ Texte publié au Journal officiel des Communautés européennes n° L 281 du 23/11/1995 p. 0031 – 005.

¹⁷⁴ Les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980.

à la Convention 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Ce texte, de même que les lignes directrices du 23 septembre 1980 de l'OCDE inspireront la directive de 1995.

En l'état actuel du droit, le transfert de données personnelles ne pose pas au sein de l'Union européenne de problèmes juridiques majeurs. Même si la transposition dans certains pays membres dont la France ne s'est faite qu'assez tardivement¹⁷⁵, les internautes pouvaient se prévaloir devant leurs juridictions nationales de la directive 95/46/CE non encore transposée.

La Convention 108 du Conseil de l'Europe du 28 janvier 1981 énonce en son chapitre III que, les parties ne peuvent pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre partie ; des dérogations sont cependant prévues¹⁷⁶.

2-b. Le transfert vers les pays tiers.

Les ressources du droit international privé sont limitées, peu adaptées et difficiles à mettre en œuvre pour un internaute qui voudrait se défendre contre un usage abusif dans un pays étranger de ses données personnelles. Le risque est de voir émerger de véritables paradis virtuels de données personnelles similaires aux paradis fiscaux¹⁷⁷. C'est dans cet esprit que l'Union européenne a procédé à une étude au cas par cas de l'adéquation juridique des pays vers lesquels des transferts de données devaient être effectués.

2.b'. Les pays tiers à protection « adéquate »

L'article 25 §1 de la directive déclare que « *Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat* ».

¹⁷⁵ La transposition définitive de la France est intervenue avec la Loi n°2004-575 pour la Confiance dans l'économie numérique du 21 juin 2004 parue au JO du 22 juin 2004.

¹⁷⁶ Jean Frayssinet, Internet et la protection juridique des données personnelles, Colloque International, Internet et le droit, 26 sept. 2000.

¹⁷⁷ J. Frayssinet, op. cit.

Le caractère adéquat s'apprécie en tenant compte de la nature des données, des finalités du traitement, des pays, de leur législation, des règles professionnelles et de sécurisation¹⁷⁸. Cette appréciation devant se faire au cas par cas, le groupe institué par l'article 29 de la directive, dit groupe de protection des personnes à l'égard du traitement de données à caractère personnel a tenté de préciser la notion de protection adéquate dans un document du 24 juillet 1998¹⁷⁹.

Il est nécessaire que les Etats membres uniformisent l'appréciation qu'ils feront du caractère adéquat de la protection des pays tiers destinataires du transfert ; ce principe est posé par l'article 25-3 de la directive 1995. S'il survient une divergence d'avis entre les Etats membres, il revient à la Commission européenne d'apprécier la protection adéquate. Elle devra pour ce faire recueillir l'avis d'un comité prévu par la directive en son article 31. Dans l'hypothèse où la commission voudrait passer outre l'avis de ce comité, le Conseil des ministres devra trancher¹⁸⁰.

Le Conseil et le Parlement ont donné le pouvoir à la Commission de décider sur la base de l'article 25(6) de la directive 95/46/CE qu'un pays tiers offre un niveau de protection adéquat en raison de sa législation interne ou des engagements pris au niveau international. L'adoption d'une décision de la Commission, basée sur l'article 25(6) de la Directive comporte:

¹⁷⁸ Directive 24 oct. 1995, art. 25-2 « *Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives au transfert de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée des traitements envisagées, les pays d'origine et de destination finale, les règles de droit générales ou sectorielles en vigueur dans le pays tiers en cause, ainsi que les professionnelles et les mesures de sécurité qui y sont respectées* »

¹⁷⁹ Document disponible sur le site :

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/1998_fr.htm

Commission européenne, Direction générale Marché intérieur et services financiers, Libre circulation de l'information, protection des données et aspects internationaux s'y référant ; DG XV D/5004/98WP 13 ; Groupe de protection des personnes à l'égard du traitement des données à caractère personnel ; Travaux futurs sur les codes de conduite: Document de travail concernant la procédure d'examen des codes de conduite communautaires par le groupe de travail, Adopté le 10 septembre 1998.

¹⁸⁰ Directive 95/46 article 31 1). La Commission est assistée par un comité composé des représentants des Etats membres et présidé par le représentant de la Commission. 2). Le représentant de la Commission soumet au comité un projet de mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 148 paragraphe 2 du traité. Lors des votes au sein du comité, les voix des représentants des Etats membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote. La Commission arrête des mesures qui sont immédiatement applicables. Toutefois, si elles ne sont pas conformes à l'avis émis par le comité, ces mesures sont aussitôt communiquées par la Commission au Conseil. Dans ce cas: la Commission diffère l'application des mesures décidées par elle d'un délai de trois mois à compter de la date de la communication, le Conseil, statuant à la majorité qualifiée, peut prendre une décision différente dans le délai prévu au premier tiret.

- Une proposition de la Commission.
- Un avis du groupe de Commissaires nationaux de protection des données (Art. 29 Groupe de protection des données).
- Un avis du comité de gestion (Art. 31) émis par une majorité qualifiée des Etats membres.
- 30 jours de droit de regard du Parlement européen pour vérifier si la Commission a correctement utilisé ses pouvoirs d'exécution. Le Parlement européen peut, s'il le considère approprié, émettre une recommandation.
- L'adoption de la décision par le Collège des Commissaires.

L'effet d'une telle décision est que, les données personnelles peuvent circuler au départ des vingt-sept Etats membres de l'UE et des trois Etats membres de l'EEE (Norvège, Liechtenstein et Islande) vers un pays tiers sans qu'aucune garantie supplémentaire ne soit nécessaire. Deux conditions sont requises pour que la protection d'un pays tiers soit considérée adéquate :

- Le pays doit avoir adopté des principes fondamentaux semblables à ceux de la directive. Cela suppose que le principe de finalité gouverne les traitements de données ainsi que celui de la transparence. Les personnes doivent être informées de l'identité du responsable du traitement et de ses finalités. Elles doivent aussi bénéficier du droit d'accès, d'opposition et de rectification. La sécurité et la confidentialité des données doivent également être assurées. Il est important que le pays tiers conditionne (de même que le pays européen d'où les données ont été au préalable transférées) le transfert des données, à la même exigence que la directive : à savoir un niveau de protection adéquate¹⁸¹.
- Le principe posé par la directive de 1995 est que les transferts de données sont interdits vers les pays tiers à l'Union européenne si ils ne se prévalent pas d'une réglementation équivalente en matière de protection des données personnelles. Dans l'autre sens, pour les données personnelles provenant d'un Etat tiers et traitées dans l'Union, les citoyens de ces Etats se voient appliquer le droit du pays d'accueil à condition qu'il soit conforme à la directive¹⁸².

¹⁸¹ Erika Orengo, op. cit.

¹⁸² Jean Frayssinet, Internet et la protection juridique des données personnelles, Colloque international, Internet et le droit, 26 septembre 2000.

Ces dispositions de la directive n'ont pas très bien été accueillies par les Etats tiers. Ils y ont vu une forme d'impérialisme ou d'exportation du droit européen en vue d'imposer aux Etats tiers de s'aligner sur lui¹⁸³. Une application stricte des dispositions de la directive laissait planer une menace sur les échanges de l'Union européenne avec le reste du monde. Une liste noire risquait d'émerger d'une application stricte de la loi, contraignant ainsi l'Union européenne à prendre des mesures pour empêcher tout transfert de données vers le pays en cause. Cela se serait apparenté à un boycott qui ne pouvait qu'entraîner des conséquences économiques et politiques négatives.

En vue d'adoucir cette position, il a été prévu à l'article 25 de la directive que, la commission est en mesure d'engager « au moment opportun », des négociations avec les pays tiers afin que ceux-ci garantissent un niveau de protection adéquat. La commission a également la possibilité d'engager des négociations avec des pays n'assurant pas un niveau de protection adéquat afin que tout transfert de données ne soit pas rendu impossible.

A ce jour, la Commission européenne a reconnu comme adéquate la protection des législations suisse¹⁸⁴ et hongroise (la Hongrie étant devenue entre temps un Etat membre de l'Union européenne)¹⁸⁵. Depuis le 14 janvier 2002 le Canada a aussi été reconnu comme présentant un niveau de protection adéquat¹⁸⁶; de même que l'Argentine¹⁸⁷, Guernesey¹⁸⁸, l'Île de Man¹⁸⁹. Les principes de la « sphère de sécurité » publiés par le ministère du commerce des Etats-Unis et les données à caractère personnel contenues dans les dossiers des passagers ont été qualifiés comme répondant aux critères de protection adéquate. Cette qualification a cependant été refusée à l'Australie¹⁹⁰.

Le principe est l'interdiction de transfert de données vers les pays tiers dont la protection n'est pas adéquate; la directive du 24 octobre 1995 prévoit néanmoins des exceptions à cette interdiction dans son article 26 :

¹⁸³ Ibid.

¹⁸⁴ Décision 2000/518/Ce de la Commission du 26 juillet 2000 relative à la constatation du caractère adéquat de la protection des données personnelles en Suisse, JOCE L.218 du 25 août 2000.

¹⁸⁵ Décision 2000/519/Ce de la Commission du 26 juillet 2000 relative à la constatation du caractère adéquat de la protection des données personnelles en Hongrie, JOCE L.218 du 25 août 2000.

¹⁸⁶ Décision de la Commission 2002/2/EC du 20.12.2001 - J.O. L 2/13 du 4.1.2002

¹⁸⁷ Décision de la Commission C (2003)1731 du 30 juin 2003 - JO L 168, 5.7.2003

¹⁸⁸ Décision de la Commission du 21 novembre 2003 sur la protection adéquate des données personnelles en Guernesey - J.O. L 308, 25.11.2003

¹⁸⁹ Décision de la Commission 2004/411/CE du 28.4.2004 constatant le niveau de protection adéquat des données à caractère personnel dans l'Île de Man

¹⁹⁰ Avis 3/2001 du 26 janvier 2001

« Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, peut être effectué, à condition que:

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé, ou

b) que le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, ou

c) que le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou

d) que le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou

e) que le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou

f) que le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier ».

Ces exceptions limitent la portée de la protection des données personnelles posée par la directive. Dans l'alinéa 2 de l'article on quitte la relation Etat membre et Etat tiers pour une relation Etat-entreprise¹⁹¹.

¹⁹¹ 2. Sans préjudice du paragraphe 1, un Etat membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées... »

Ces exceptions visent les cas où la personne concernée par le traitement (ou son tuteur légal s'agissant de mineur et conformément au droit commun) a donné son accord, si le transfert des données est nécessaire à une exécution contractuelle ou si le responsable du traitement offre des garanties suffisantes.

La détermination du responsable du traitement est capitale, tant pour l'exercice des droits des personnes concernées par le traitement des données personnelles que pour l'exercice des actions en responsabilité. L'intérêt réside notamment dans la désignation d'un responsable unique du traitement des données personnelles, dans la mesure où, cela simplifierait les formalités imposées par la directive. Sont notamment concernés les groupes internationaux qui utilisent des réseaux intranet transfrontaliers pour les besoins de leur gestion interne.

Si on suivait la directive à la lettre, une déclaration de traitement des données personnelles auprès de l'autorité de contrôle de leur pays respectif devrait être effectuée par les filiales. L'établissement d'une convention de flux transfrontières entre chaque société exportatrice de ces données et leur destinataire situé dans un pays n'assurant pas un niveau de protection adéquate serait également nécessaire¹⁹².

2.b". Les systèmes dérogatoires de transfert de données en l'absence de protection adéquate.

i. Le recours à un cadre contractuel pour assurer la protection des données personnelles

Parmi les dérogations établies par l'article 26 de la directive, il en existe une tenant au fait que le responsable du traitement puisse apporter une garantie suffisante de protection de la vie privée et des libertés et droits fondamentaux des personnes concernées. Ces garanties peuvent résulter de clauses contractuelles. La directive laisse la possibilité d'une contractualisation de la protection des données personnelles par les acteurs économiques. Cet assouplissement de la directive européenne peut être perçu comme un rapprochement¹⁹³. Dans cette perspective, on sépare le cadre des règles générales de celui des règles au cas par cas.

L'idée de recourir à des mécanismes contractuels pour assurer le respect des garanties accordées aux personnes avait déjà été imaginée par la Commission Nationale de

¹⁹² Erika Orengo, op. cit.

¹⁹³ Agathe Lepage, op. cit., p.32

l'Informatique et des Liberté¹⁹⁴. Cette approche économique de la protection des données personnelles des internautes se justifie par le fait que les flux transfrontaliers participent au développement du commerce international et au progrès économique. Les interdire reviendrait à freiner l'essor et les échanges économiques internationaux qui transitent par le Web.

Les dérogations prévues dans l'article 26 de la directive 95/46 ne devaient être que des exceptions répondant à des situations particulières¹⁹⁵. Elles ne devaient pas se substituer à la règle de principe. En pratique les clauses contractuelles prennent une importance croissante afin de contourner le dispositif de la directive à l'égard du transfert de données vers les pays jugé rigides.

Grâce au recours au contrat de protection des données, les garanties accordées aux personnes par le système français et européen suivent les données malgré le franchissement de frontières. La décision d'apprécier le caractère suffisant de ces garanties contractuelles revient en principe à l'Etat-membre plutôt qu'à la commission comme c'est le cas pour le « niveau de protection adéquate ». Elle conserve néanmoins un pouvoir de contrôle par rapport à l'application faite de l'article 26 § 2 de la directive¹⁹⁶. Chaque Etat membre doit informer la Commission et les autres Etats des autorisations qu'il accorde sur le fondement des garanties contractuelles. Les autres Etats peuvent manifester une opposition à cette décision s'ils estiment que les garanties contractuelles sont insuffisantes¹⁹⁷.

L'Union Européenne laisse aux entreprises qui échangent des données le soin de prévoir des mécanismes contractuels de protection des personnes. Les autorités européennes encadrent cependant cette faculté, puisqu'elles ont fixé un cadre contractuel précis que les entreprises, même si elles n'y sont pas obligées, ont intérêt à respecter afin de simplifier leurs opérations de transfert de données¹⁹⁸.

¹⁹⁴ Article 69 Loi 1978 énonce que, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat n'ayant pas une protection adéquate si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci.- Erika Orengo, préc., op. cit. p.9, La CNIL dans sa délibération 89-18 du 11 juillet 1980 Fiat – France proposait de pallier l'inadéquation de la législation italienne de protection des données à la loi française par un contrat entre l'expéditeur et le destinataire des données.

¹⁹⁵ Erika Orengo, préc., p.14.

¹⁹⁶ Ibid., p.15.

¹⁹⁷ Ibid.

¹⁹⁸ Ibid.

L'Union européenne n'est pas pour autant prête à laisser entre les mains des acteurs privés le contrôle de la protection des personnes. A elle seule la contractualisation ne saurait remplir ce rôle, elle doit être basée sur des principes généraux. Le Conseil d'Etat souligne la nécessité que ces clauses contractuelles soient accompagnées d'un dispositif législatif, il parle de « dynamisme de corégulation »¹⁹⁹.

En cas de non application du contrat portant sur la protection de données au cours d'un transfert de données, à quelle autorité revient-il de veiller au respect du contrat ? La mise en œuvre de la responsabilité contractuelle n'est pas automatique mais dépend du bon vouloir d'une des parties. Le recours à cette responsabilité contractuelle ne permet pas de sanction ni de contrainte générale. Les autorités nationales telles que la CNIL ont également la possibilité d'approuver des contrats de transfert dès lors qu'ils jugent le niveau de protection adéquat. L'exercice de cette faculté risque de nuire à l'uniformité des pratiques sur le territoire européen.

La Commission européenne a dans une décision du 27 décembre 2001 posé les clauses contractuelles types pour le transfert de données à caractère personnel vers les pays tiers²⁰⁰.

ii. Le compromis entre l'Union Européenne et les Etats-Unis : l'accord Safe Harbor

Il existe une idée préconçue à propos des Etats-Unis selon laquelle, ils ne se soucient pas de la protection des données personnelles notamment dans le cadre d'Internet. Ils préconiseraient à la place une politique du "laissez-faire" et d'autorégulation²⁰¹.

La protection des données personnelle en Europe a fait apparaître des rapports de force nouveaux qui ont obligé les Etats-Unis à se soucier du reste du monde. Le modèle américain renvoyait au gestionnaire des données, au maître du traitement, le soin d'assurer la protection des données. L'Etat fédéral n'a pas édicté de loi générale au profit de réglementations sectorielles.

¹⁹⁹ Conseil d'Etat, Internet et les réseaux numériques, p.211

²⁰⁰ JOCE 10 janvier 2002 décision de la commission 2002/16/CE du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnels vers les sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE.

http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_fr.htm

²⁰¹ J. Frayssinet, op. cit. – A. Lepage, op. cit. p.32-33.

Au regard de la sensibilité des internautes par rapport à la protection de leurs données personnelles (right to privacy), en raison de la multiplication de procès aux Etats-Unis (affaire double click ou geocities), et du développement du commerce électronique, les responsables de la gestion de données personnelles ont commencé par prendre des mesures pour préciser ou dégager leur responsabilité. Cela prend la forme de clauses précises contenues dans des pages spéciales exposant la « privacy policy » à laquelle l'internaute choisit d'adhérer ou non.

Il y a une pratique qui consiste en la création d'organismes privés délivrant un label aux portails ou sites d'entreprises s'engageant à respecter une charte contenant entre autre des règles de protection des données²⁰².

La question demeure entière s'agissant des flux de données personnelles entre les Etats-Unis et l'Union européenne. Autant les normes nationales ne peuvent s'appliquer en dehors de leurs frontières, autant les normes européennes ne peuvent s'imposer aux Etats-Unis et inversement.

L'accord "Safe harbor" est l'aboutissement de longues négociations entre l'Union européenne et les Etats-Unis. L'objectif est de contourner le principe posé par l'article 26 de la directive de 1995 pour parvenir à un rapprochement des conceptions européennes et américaines sur la protection des données. Cet accord a été conclu dans la logique de l'article 25-6 de la directive prévoyant des dérogations à l'interdiction de transfert de données vers les pays tiers n'ayant pas un niveau de protection adéquat. Il s'agissait de trouver un terrain commun entre deux conceptions très différentes de la protection des données personnelles. L'approche américaine laisse une grande place à l'autorégulation ; la régulation des comportements se fait *a posteriori* tandis qu'en Europe l'analyse juridique et la régulation se font *a priori*.

Aux termes des Accords Safe Harbor Principles²⁰³, une entreprise européenne pourra sans en demander d'autorisation à la commission européenne, céder ses fichiers à une entreprise américaine à condition que cette dernière garantisse un niveau de protection adéquat²⁰⁴. Il

²⁰² J. Frayssinet, Internet et la protection juridique des données personnelles, préc.

²⁰³ Safe Harbor principes cela veut dire littéralement « principe du port sûr », mais, et selon la traduction retenue il faut entendre par là « principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée ». Yves Poulet, Les safe harbor principes – une protection adéquate ? juricom.net 17 juin 2000. Texte présenté lors du colloque de l'IFCLA, Paris, 15 et 16 juin 2000. <http://www.juricom.net/uni/doc/20000617.htm>

²⁰⁴ Les entreprises américaines sont présumées offrir un niveau de protection adéquat et les flux transfrontières de données européennes à destination des Etats-Unis seraient ainsi facilités.

revient à la Federal Trade Commission de mettre en œuvre les garanties prévues. Elle est chargée d'accorder la possibilité à certaines organisations²⁰⁵ de décerner un label garantissant le respect du niveau de protection par l'entreprise²⁰⁶.

Le système américain que proposent les accords Safe Harbor repose sur une solution d'auto-réglementation plutôt que législative. Le *Department of Commerce* américain est à l'origine des *Safe Harbor Principles*. « *L'effectivité de ces principes dépend d'organes juridictionnels officiels, en particulier de la Federal Trade Commission* », ce qui plaiderait pour un "effective mix" (selon la qualification récemment retenue par les débats de l'OCDE²⁰⁷), qui est un système alliant les vertus de l'auto-réglementation et l'autorité de la puissance publique²⁰⁸.

En réaction à la Directive européenne et à ses exigences, le *Department of Commerce* américain en particulier la *National Information Agency* a rapidement affirmé que la volonté américaine était, (en ce qui concerne tout au moins le secteur privé) d'assurer une protection adéquate dans le cadre de codes de conduite et d'autres instruments d'autorégulation. Un premier texte qualifié d'« *Elements of Effective selfregulation for privacy Protection* » a été publié à ce propos en 1998. Suite aux négociations ininterrompues depuis 1998 entre la Commission européenne²⁰⁹ et les Etats-Unis, la position américaine a largement évolué. Le *Department of Commerce* du gouvernement américain a publié diverses versions des *Safe Harbor Principles* qui visent à assurer la protection des données à caractère personnel

²⁰⁵ Il s'agit d'organes labellisateurs tels que TRUST-e et BBB On line.

²⁰⁶ On ne parle plus de niveau de protection adéquat au niveau des Etats mais au niveau des entreprises.

²⁰⁷ Voir à ce propos les débats tenus lors de la conférence de suivi d'Ottawa sur le commerce électronique (Paris, novembre 1999). Sur la notion d'autorégulation, lire en particulier les travaux de la Fondation Bertelsman.

²⁰⁸ Yves Pouillet, Les safe harbor principles – Une protection adéquate ? *Juriscom.net* 17 juin 2000, préc.

²⁰⁹ Le Groupe dit de l'article 29 a émis dans le cadre de ces négociations et à propos des diverses versions du texte du *Safe Harbor* les opinions suivantes :

→ Avis 1/99 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain, DG MARKT 5093/98 WP. 15 ;

→ Avis 2/99 du 3 mai 1999 concernant la pertinence des "principes internationaux de la sphère de sécurité" publiés par le ministère du commerce des États-Unis le 19 avril 1999, DG MARKT 5047/99– WP. 19 ;

- Avis 4/99 du 7 juin 1999 concernant les questions souvent posées, devant être publiées par le ministère américain du commerce dans le cadre des principes proposés pour la "sphère de sécurité, DG MARKT 5139/00 – WP. 21 ;

→ Document de travail sur l'état actuel des discussions en cours entre la Commission européenne et le gouvernement américain du 7 juillet 1999 concernant les Principes internationaux de la « sphère de sécurité » relatifs à la protection de la vie privée, DG MARKT 5075/99 – WP. 23

→ Avis 7/99 du 3 décembre 1999 sur le niveau de protection des données garanti par les principes de la "sphère de sécurité" publiés avec les questions fréquemment posées (FAQ) et d'autres documents connexes les 15 et 16 novembre 1999 par le ministère du commerce américain, DG MARKT 5146/99 WP. 27.

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1999_fr.htm

transférées d'un Etat membre européen vers les Etats-Unis²¹⁰. Ces principes sont complétés par la réponse à des « QFP » (questions fréquemment posées) ou, selon la terminologie américaine, à des « FAQ » (*Frequently Asked Questions*), publiées par le Ministère du Commerce des Etats-Unis et fournissant des orientations pour la mise en œuvre de ces principes.

Le système mis en place par les Safe Harbor Principles n'est pas satisfaisant dans la mesure où il se base uniquement sur le principe de volontariat et n'assure pas un degré de protection adéquat dans la mesure où le principe de finalité du traitement n'y est pas pris en compte²¹¹.

Pour l'essentiel, les principes publiés et les FAQ réaffirment l'essentiel des « *Elements of Effective selfregulation for privacy Protection* » même si des progrès notables en ce qui concerne le contenu et l'« effectivité » (*enforcement*) des principes doivent être notés. On remarquera tout d'abord que les *Safe Harbor Principles* ne concernent pas les données « purement américaines », c'est-à-dire celles collectées auprès de citoyens américains aux Etats-Unis, et donc non protégées à l'origine par la Directive.

Il va de soi que l'uniformité des règles en vigueur quelle que soit l'origine des données eût été préférable plutôt que la soumission à des règles différentes, ce qui entraîne des risques de méconnaissance des règles du *Safe Harbor* au sein des organisations américaines²¹².

²¹⁰ On note que les *Safe Harbor Principles* ne concernent pas les données purement « américaines », c'est-à-dire non protégées à l'origine par la Directive. Ce point est important. On déplorera avec nombre d'auteurs américains que les principes y repris ne puissent être invoqués par des citoyens américains mais, plus grave, on s'interrogera sur l'effectivité des principes dans la mesure où les entreprises américaines devront soumettre les données d'origine européenne à d'autres règles que celles habituellement suivies. Il va de soi que l'uniformité des règles en vigueur, quelle que soit l'origine, eût été préférable et non la soumission à des règles différentes, ce qui entraîne des risques de méconnaissance des règles du *Safe Harbor* au sein des organisations américaines. Un exemple est la question de la définition des données sensibles singulièrement élargie par les *Safe Harbor Principles* par rapport à la définition américaine classique. Spontanément, un employeur américain ne rangera pas comme donnée sensible l'opinion syndicale ou la donnée d'origine ethnique de son employé.

²¹¹ Julien Faurel, La labellisation des sites Internet, DESS Droit du multimédia et de l'informatique sous la direction de Gaël Kostic, Université Paris II – Assas 2000-2001, p.5.
www.u-paris2.fr/dess-dmi/rep_travaux/16_julienfaurel.pdf

²¹² Un exemple est la définition des données sensibles reprises par le *Safe Harbor*. Cette définition, même si elle ne satisfait pas le prescrit européen, est bien plus large que celle communément admise aux Etats-Unis : ainsi la race est une donnée sensible au sens du *Safe Harbor* et non de la législation américaine. On peut donc craindre qu'un employeur américain ne range pas spontanément la race comme donnée sensible. En d'autres termes, le fait que le *Safe Harbor* soit une législation d'exception laisse craindre une moindre effectivité des règles y contenues ; Yves Pouillet art. préc., Les Safe harbor principles.- Une protection adéquate ?

L'adhésion à ces principes est totalement volontaire. Cependant, pour que les organisations obtiennent et conservent la reconnaissance du fait qu'elles assurent un niveau de protection adéquat pour le transfert de données de l'Union européenne vers les Etats-Unis conformément à la présente décision, elles doivent souscrire à ces principes. Pour ce faire elles doivent divulguer leurs règles de confidentialité ce qui relève de la compétence de la Commission fédérale du commerce en vertu des dispositions de la section 5 du « *Federal Trade Commission Act* » qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce ou de tout autre organisme remplissant une mission analogue.

La « *Federal Trade Commission Act* » permet à la Commission fédérale du commerce d'obtenir des mesures de redressement par voie d'injonction en cas de pratiques déloyales ou frauduleuses. Elle permet la réparation des préjudices subis par les citoyens des Etats-Unis ou d'autres pays ce, dans l'exercice de ses fonctions officielles de contrôle dans son domaine de compétence. La FTC a en outre montré qu'elle était disposée à étudier les plaintes indépendamment de la nationalité ou du pays de résidence du plaignant²¹³. Les conclusions d'Yves Poulet sont mitigées s'agissant de la portée des Safe Harbor Principles²¹⁴.

²¹³ Yves Poulet art. préc.

²¹⁴ « Sans nier que les Safe Harbor Principles présentent une solution audacieuse et, dans un certain sens, pleine de promesses, nous émettons des réserves à propos de l'adéquation de la protection que pourraient apporter des Safe Harbor Principles et la déclaration par un organisme public ou privé de leur respect. Ces réserves sont motivées comme suit : 1) L'étendue du champ d'application reste floue et sujette à interprétation ; 2) Les principes du Safe Harbor ne concernent que les données couvertes par la Directive et non l'ensemble des données traitées par les organisations américaines. Ils introduisent dès lors, pour les données européennes, un régime d'exception qui risque d'être mal connu et peu respecté dans les faits ; 3) Les principes du Safe Harbor méconnaissent le principe de la finalité déterminée et légitime. Cette méconnaissance introduit des risques quant aux conditions d'application des autres principes ; 4) Les principes du Safe Harbor donnent au droit d'accès une portée trop relative et laissent dès lors aux organisations la possibilité d'échapper trop facilement à leur devoir de transparence ; 5) L'application des principes du Safe Harbor repose sur la « jurisprudence » ou l'intervention de multiples organes d'autoréglementation dont aucune autorité officielle ne garantit l'unité d'interprétation. En particulier, la compétence de la F.T.C. est trop indirecte en la matière pour la garantir ; 6) L'effectivité du respect des Safe Harbor Principles repose sur des mécanismes compliqués dont la qualité de certains est peu évidente. En particulier, l'auto certification par l'organisation elle-même est certes entourée de garanties quant aux possibilités de contestation de la conformité auprès d'autorités indépendantes, mais la qualité d'indépendance de ces autorités est peu définie et la manière dont les organisations sont soumises à ces organisations, non précisée 7) De manière générale, l'approche américaine repose sur l'intervention des institutions privées « d'Alternative Dispute Resolution » dont on ne peut que constater qu'elles sont au début de leur existence, que leur fonctionnement est dès lors peu éprouvé et, enfin, que leur pouvoir d'investigation est mal précisé. 8) En définitive, on regrette que le Safe Harbor laisse en définitive la personne concernée démunie. C'est à elle de vérifier la situation de conformité ou non de l'organisme américain qui traite des données, c'est à elle de trouver et saisir l'autorité indépendante de contrôle apte à étudier son cas, c'est à elle de proposer les arguments de sa demande. A ce propos, une aide et un support des organisations américaines militantes des droits de l'Homme ou de défense des libertés eussent été utiles mais leur intervention n'est pas envisagée et elle risque d'être rare et peu probable, ces organisations étant créées au départ pour la défense des citoyens américains et non européens. Ibid.

§2. Le droit à la vie privée du mineur dans le cyberspace.

La Déclaration Universelle des Droits de l'homme : « *Nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domaine ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». L'article 9 du code civil et l'article 8 de la Convention Européenne des Droits de l'homme et du citoyen posent le même principe quoique en des termes légèrement différents.

Définition de la vie privée. La vie privée « *correspond à l'intimité de la personne, cela regroupe sa vie sentimentale, conjugale, familiale, ses relations amicales, son état de santé, sa vie quotidienne à son domicile, ses loisirs, sa correspondance. Cet ensemble est protégé par le droit au respect de la vie privée, qui est un droit de la personnalité, c'est-à-dire dont toute personne bénéficie. Les atteintes à cette intimité peuvent donc faire l'objet de sanctions civiles et pénales*²¹⁵ ».

Les aspects de la vie privée du mineur qui sont le plus mis à mal dans le cyberspace sont : son droit à l'image et son droit à une correspondance privée.

A. L'image du mineur.

A la différence du droit au respect de la vie privée, qui a été expressément consacré par le législateur, le droit à l'image n'a pas de support légal. Sa reconnaissance a été l'œuvre d'une jurisprudence abondante, qui a greffé le droit à l'image sur l'article 9 du code civil²¹⁶. De l'avis de certains auteurs, l'expression «droit à l'image» serait une simple tournure de langage permettant de rassembler sous les notions de droit d'image les différents aspects juridiques qui gravitent autour d'un support technique de la représentation de réalités matérielles ou personnelles²¹⁷. Il n'est pas rare qu'une atteinte à la vie privée puisse être faite

²¹⁵ Code civil, art. 9 et Code pénal art.226-1 et s.- Définition extraite du Dictionnaire du vocabulaire juridique sous la direction de Rémy Cabrillac, Ed, Litec, p.387.

²¹⁶ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc, p.105.

²¹⁷ Céline Halpern, Le droit à l'image, Ed. De Vecchi 2003, P.7.

par le biais d'une image ; soit par elle-même, soit par les propos qui l'accompagnent²¹⁸. L'évolution technologique à laquelle nous devons Internet et l'avènement des appareils de photographies numériques a accentué la question du droit à l'image. Surtout en ce qui concerne sa reproduction et sa diffusion. Il est désormais assez aisé pour toute personne disposant d'un minimum de connaissances informatiques et en numérisation des photographies de pouvoir diffuser des images qui peuvent être porteuses d'atteintes à la vie privée des personnes.

Le mineur comme toute autre personne a droit au respect de son image, les dispositions nécessaires à la protection de ce droit doivent simplement être adaptées aux particularités juridiques du mineur et du cyberspace.

1. L'autorisation de diffusion de l'image du mineur.

Que ce soit sur Internet ou par un autre moyen, la diffusion de la photographie d'une personne est soumise à son autorisation, celle de son tuteur légal ou de ses ayants droits²¹⁹. La chambre criminelle de la cour de cassation a rappelé cette exigence. « *La fixation de l'image d'une personne, vivante ou morte, sans autorisation préalable de la personne ayant pouvoir de la donner est prohibée* »²²⁰ ce, quels que soient sa notoriété et son âge²²¹.

La capture en elle-même de l'image d'une personne n'est pas interdite, sauf intrusion dans la vie privée de la personne²²². Il faut respecter un certain nombre de mesures tenant d'une part, à l'autorisation de la reproduction ou la diffusion de l'image par la personne concernée et d'autre part à la finalité de l'utilisation de cette image.

²¹⁸ B. Beigner, L'honneur et le droit, LGDJ, préface J.Foyer, p.65 et s., G. Loiseau, L'autonomie du droit à l'image, Legicom n°20, 1999/4, p.71 et s.

²¹⁹ CA. Paris 14 mai 1975 : Dalloz 1976, J. 291 note Lindon ; CA. Versailles 21 mars 2002, sommaire. 2374 obs. Caron, Légipresse juillet-août 2002, n°193.III.137.

²²⁰ Céline Halpern, Droit et Internet, Editions de Vecchi 2003, p.87.

²²¹ Ibid.

²²² l'article 226-1 du code pénal punit « le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui [...], en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé » on peut en déduire qu'à contrario, si il n'est pas porté atteinte à la vie privée d'autrui par la prise d'une photographie dans un lieu public, la capture d'une image n'est pas prohibée.

1.a. Les détenteurs du droit d'autorisation

La reproduction de l'image des personnes est devenue une pratique courante, sinon indispensable dans de nombreux domaines comme l'éducation nationale, la recherche, qu'elle serve à illustrer un journal d'école ou de laboratoire, un site Internet²²³.

L'avènement de la numérisation a entraîné une mutation du droit de l'image. La numérisation de la photographie d'un individu nécessite un double accord : celui de la personne concernée, et celui de l'auteur de la photographie²²⁴.

Pour diffuser l'image d'un mineur sur Internet, il est nécessaire d'obtenir avant la diffusion l'autorisation des deux parents. A défaut d'autorisation le responsable du site s'expose à un an d'emprisonnement et 45 000€ d'amende ainsi qu'à une condamnation à des dommages et intérêts pour l'atteinte portée à ce droit.

Bien que les parents ou tuteurs légaux soient ceux habilités à donner leur autorisation pour la diffusion de l'image d'un mineur, ce dernier doit dans certaines circonstances ajouter son consentement à celui de ses parents dès lors qu'il est capable de discernement²²⁵.

Si les images sont prises dans des lieux publics, l'autorisation sera requise uniquement si l'enfant est reconnaissable et isolé sur la photo²²⁶. Par exemple, pour une photo prise dans une cour d'école ou celle d'un groupe d'enfants dans une excursion, l'autorisation ne sera pas nécessaire si la photographie ne permet pas de reconnaître l'enfant en particulier.

La liberté de communication des informations autorise la publication d'images de personnes impliquées dans un évènement, sous la seule réserve du respect de la dignité de la personne humaine²²⁷.

²²³ CA. Paris 6 novembre 2002 : CCE mars 2003, commentaire. n°32, note Lepage ; CA. Paris 15 mai 2001 : CCE novembre 2001, commentaire. n°118, note Lepage.

²²⁴ On étudiera ce point dans les droits d'auteur.

²²⁵ Céline Halpern, *Droit et Internet*, préc., p. 87. – A. Lepage, *Libertés et droits fondamentaux à l'épreuve d'Internet*, préc., p.41.

²²⁶ C. Halpern, préc., p.55.

²²⁷ Cour de Cassation, Civ. I, 20 février 2001. – Cass. 1ere civ. 12 juillet 2001, D.2002, p.1380 note C. Bigot et sommaire p.2298, obs. L. Marino, *Comm. com. Electr.*, novembre 2001, commentaire. n°117, obs. A. Lepage.

1.b. La forme de l'autorisation.

L'autorisation doit être expresse et préalable à la diffusion de l'image du mineur. Le fait que certaines photographies se trouvent sur des sites Internet ne permet pas pour autant de s'en saisir afin de les reproduire librement, et ce faisant se dispenser de l'autorisation de la personne concernée ou de ses représentants légaux²²⁸.

Il est recommandé de recourir à l'autorisation écrite sans forme particulière²²⁹. Il est néanmoins admis dans certaines espèces qu'il peut y avoir présomption d'autorisation, un consentement implicite ou encore un accord tacite²³⁰. L'existence d'un consentement implicite résultant des circonstances de la prise de vue est également parfois consacrée par les juges²³¹. En tout état de cause, l'accord ne vaut que pour le contexte de publication très particulier ayant permis d'apprécier un consentement tacite. On peut s'interroger sur le fait de savoir si la présomption d'autorisation, le consentement implicite à la diffusion de l'image du mineur concerne le mineur ou ses parents. Pour retenir « l'existence d'un consentement implicite résultant des circonstances de la prise de vue » des parents, il faudrait qu'ils aient été présents lors de la prise de vue.

Outre la nécessité d'une autorisation expresse, écrite et préalable des parents en vue de la diffusion de l'image d'un mineur, la finalité de l'utilisation de l'image doit être conforme à celle qui avait conditionnée son autorisation.

1.c. La preuve de l'autorisation.

En matière de vie privée, la charge de la preuve pèse sur la personne qui se prévaut de l'autorisation²³², c'est-à-dire, le plus souvent, l'auteur de la publication. Ainsi la Cour d'appel d'Aix-en-Provence, rappelant que « *le droit à l'image est un droit de la personnalité qui*

²²⁸ TGI Paris, Ch. Presse 12 décembre 2000, Comm. com. électr. 2001, commentaire A. Lepage ; JCP E 2002, p.75, obs., C. Vivant.

²²⁹ C. Halpern, Le droit à l'image, préc., p.41.- CA. Versailles 21 mars 2002, D. 2002, sommaire. 2374, obs. Caron.

²³⁰ Le droit à l'image, février 2004 <http://www.educnet.education.fr/juri/vieprivée/image.htm>

²³¹ CA Bordeaux, 10 févr. 2003: JCP 2003. IV. 2991. Ainsi, la cour d'appel de Bordeaux estime, à propos de la photographie d'un individu aux prises avec un chien de combat, cliché pris au cours d'un entretien avec le journaliste, que cette circonstance rend évident le fait que l'éleveur ne pouvait pas ignorer l'utilisation qui allait nécessairement être faite de cette photographie, à des fins d'information et d'actualité, de sorte qu'il convenait de considérer qu'il avait implicitement donné son consentement à sa diffusion

²³² F. Terré, La vie privée, in La protection de la vie privée dans la société de l'information, sous la direction de P. Tabatoni, PUF, 2002, p. 142

permet à chacun de s'opposer à la diffusion de son image sans son autorisation », prend soin d'ajouter qu'il « *va de soi qu'il appartient à celui qui publie l'image ou l'exploite commercialement de justifier de l'autorisation et non pas au "photographié" d'établir que l'autorisation qu'il a consentie était limitée ou restreinte à un domaine particulier* »²³³.

1.d. La finalité visée dans l'autorisation.

Dans la plupart des cas, une autorisation de diffusion ou de reproduction de l'image (notamment sur Internet) est accordée en fonction d'une utilisation bien précise. Chacun a droit en donnant son autorisation de choisir, ou de se déterminer par rapport au support qu'il estime adapté pour la diffusion de son image²³⁴.

La cour de cassation a rappelé que l'autorisation de reproduction d'une image a une portée stricte. Il faut entendre par là que le droit à la vie privée, le droit à l'image, n'est pas respecté lorsque la publication d'une photographie ne se conforme pas à « *la finalité visée dans l'autorisation donnée par l'intéressé* »²³⁵. C'est ainsi que l'autorisation donnée pour la publication de la photographie de l'enfant dans le journal de l'école ne vaut pas pour sa diffusion sur un site Internet fût-il scolaire²³⁶.

Le principe de la finalité de l'autorisation a été strictement appliqué dans un litige ayant opposé des parents à une école Montessori. Les parents avaient subordonné l'autorisation de publier l'image de leur enfant à l'obtention d'une copie du support²³⁷.

1.e. Le délai de l'autorisation.

L'autorisation consentie par les parents ou tuteurs légaux du mineur doit être utilisée dans un délai raisonnable. Une prolongation peut être prévue dans l'autorisation elle-même²³⁸.

²³³ CA Aix-en-Provence, 30 nov. 2001; CCE janv. 2003, commentaire. n° 11, note Lepage

²³⁴ Le droit à l'image, février 2004 : <http://www.educnet.education.fr/juri/vieprivée/image.htm>; - TGI. Paris 17^e ch. 7 juillet 2003, Légipresse décembre 2003, n°207.III.196.

²³⁵ Cass. 1^{ere} civ. 30 mai 2000 : Bull. civ. I n°167. C'est ainsi que l'autorisation donnée pour la publication de la photographie de l'enfant dans le journal de l'école ne vaut pas pour sa diffusion sur un site Internet fût-il scolaire.

²³⁶ Le droit à l'image, Ibid.

²³⁷ CA. Paris 14 février 2002, D.20 février 2002, J.2004.

²³⁸ C. Halpern, Droit et Internet, préc.

2. Le droit à l'image et la particularité d'Internet : la webcam.

Les techniques de diffusion et de reproduction de l'image sur Internet connaissent une évolution très rapide. De la conversion de l'image d'un support papier vers l'informatique par le biais de scanner, on est passé à la technologie de numérisation. Cette technologie a favorisé la diffusion sur Internet d'images pour quiconque dispose d'un appareil de photographie numérique et d'une connexion Internet²³⁹. La Webcam correspond au mode de fonctionnement d'Internet (puisque que conçue pour son usage exclusif), elle est le moyen par excellence de transmission en temps réel de l'image sur Internet. Avec la particularité de la Webcam, le droit à l'image dans le cyberspace ne se trouve pas simplifié. Il se pose à nouveau des questions qui semblaient résolues, s'agissant de la légitimité de la diffusion des images des mineurs.

2.a. Définition et origine.

Une Webcam est une « petite caméra numérique, branchée sur un ordinateur, qui permet de diffuser régulièrement et en temps réel sur le Web des images vidéo quelle qu'en soit la provenance et de réaliser des visioconférences sur Internet »²⁴⁰.

Depuis plusieurs années, des internautes désireux de rendre leur vie publique dévoilent une partie de leur vie privée sur Internet en filmant leurs faits et gestes quotidiens. Apparu aux Etats-Unis au milieu des années 1990, c'est en 1993 qu'a été créé le premier site Internet avec une Webcam qui consistait en un gros plan sur une cafetière dans une université²⁴¹.

L'année 1996 marquera l'entrée d'une Webcam dans le domicile d'un particulier, lorsque Jennifer Ringley installe une Webcam à son domicile. Ce phénomène né aux Etats-Unis va s'étendre à l'Europe où des internautes se mettent à leur tour à dévoiler leur vie sur Internet. Il

²³⁹ Christian GUILLAUME, professeur en BTS audiovisuel ; Les appareils de photo numériques utilisent des capteurs CCD similaires à ceux des caméscopes, et enregistrent les images sur des supports numériques, généralement de type "mémoires Flash", de la taille d'une carte de crédit. Très utiles pour reproduire des photos sur l'ordinateur ou pour les diffuser sur un Intranet ou Internet, ils autorisent généralement une meilleure définition que les photos argentiques scannées, tout en utilisant beaucoup moins de place mémoire. <http://www.apeg.info/articles/Choix%20appareils%20de%20photo%20num.htm>

²⁴⁰ www.net-dico.com/

²⁴¹ Selon le site Internet, Lire et écrire en histoire, géographie, éducation civique à l'école primaire ; « la légende d'internet veut que la Webcam fut inventée par les chercheurs de l'université de Cambridge qui souhaitaient savoir s'il restait du café dans la cafetière sans avoir à se déplacer. Depuis, ces appareils photos diffusant leurs images sur le Web permettent de voir en direct ».

http://www.tice-hg.net/stages/lire_ecrire.htm#Lire%20à%20partir%20de%20photos%20/%20webcams

existe actuellement en France un millier de sites répertoriés dans l'annuaire français des Webcams. Il y en a des dizaines de milliers aux Etats-Unis, depuis l'expérience d'origine, en 1996²⁴².

En très peu de temps, la Webcam s'est complètement banalisée. Ce gadget high-tech réalise le vieux désir de communiquer en ajoutant l'image animée à la voix. Il met à la portée de tous la visioconférence²⁴³.

2.b. Le statut juridique de la Webcam.

Parler de statut juridique de la Webcam est susceptible de faire polémique. Il n'en demeure pas moins que son existence et son utilisation posent de nombreux problèmes juridiques liés notamment à la question du droit à l'image.

La Webcam est un périphérique de l'ordinateur dont le statut juridique n'a pas encore été défini. Mais, par extension il semble logique que le droit régissant le droit à l'image trouve à s'appliquer en la matière. Cela peut être justifié par la caractéristique de la Webcam qui consiste à prendre des images qui pourront être diffusées de manière instantanée vers le cyberspace. La question se pose notamment pour des tiers dont il a été fait usage sans leur autorisation et de manière préjudiciable de l'image.

2.c. L'autorisation de diffusion et de reproduction de l'image par la Webcam.

La Webcam est sortie des logis pour se banaliser. Elle influe pour ceux qui en font usage sur tous les aspects de leur vie ; au travail avec la télésurveillance qui pose on s'en doute un problème juridique par rapport aux droits des salariés. Récemment il a été question d'une Webcam dans une crèche permettant aux parents de pouvoir garder un œil sur leur enfant²⁴⁴.

²⁴² Le Monde, 5 juillet 2001, p.8, Sylvie Chayette, Grâce aux webcams, des « Loft Story » en miniature se jouaient déjà sur le Net. - Emission du 05 Juillet 2001 ; On achève bien Loft Story émission résumée par écrit et retransmise sur le site qui suit :

http://www.franceculture.com/chaines/france-culture2/emissions/revuepresse/fiche.php?diffusion_id=2193

A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc, p.98.

²⁴³ Fabien Navel, L'image numérique – La Webcam.

http://www.france5.fr/SCIENCES_NATURE/W00133/1/62478.CFM

²⁴⁴ France 5. Les maternelles ; Dossier : Surveiller les enfants à tout prix : Webcams dans les crèches ; A Issy-les-Moulineaux, une directrice de crèche désireuse de faciliter la communication avec certains parents malentendants a doté deux ordinateurs de la crèche de webcams, Ce sujet de Sophie Pasquier à été diffusé dans l'émission Les maternelles du 17 avril 2003 (9h-10h30)

<http://www.france5.fr/maternelles/parents/W00315/5/87165.cfm>

Une heure par jour, tous les parents d'enfants de la crèche peuvent se connecter sur le Net grâce à un code sécurisé et voir leur enfant évoluer en temps réel en leur absence à la crèche. D'autres séances sont retransmises en différé. Aucun parent d'Issy-les-Moulineaux n'a protesté contre cette "cybercrèche"²⁴⁵.

Nulle part il n'est question du consentement explicite des parents quant à la reproduction de l'image de leurs enfants mineurs sur un site Internet. Cette autorisation implicite peut être déduite de l'absence de contestation de leur part quant à ce procédé, ou encore du fait qu'ils se connectent eux même au site de la "cybercrèche". On peut également déduire qu'une autorisation n'était pas nécessaire étant donné que le site Internet avait une audience restreinte aux seuls parents ; pour preuve l'existence d'un code sécurisé dont ils disposent pour se connecter à la "cybercrèche".

L'utilisation de la Webcam par les mineurs évolue presque aussi vite que ces derniers se familiarisent aux évolutions constantes d'Internet. Les mineurs pour lesquels la rencontre avec autrui est primordiale sur la Toile éprouvent un engouement pour la Webcam qui leur permet d'allier le son à l'image. Au-delà de ce tableau engageant de l'outil "suprême" de communication avec autrui, le problème reste entier s'agissant de la légalité de la diffusion des images d'autrui ainsi récoltées.

La véritable question est de savoir quand et sous quelle forme doit intervenir l'autorisation parentale de la diffusion des images du mineur issue de la Webcam. On sait que la Webcam est connectée au réseau Internet et que, lorsqu'elle est mise en marche sa diffusion est continue et en temps réel. Les parents doivent-ils donner leur autorisation une fois pour toute lorsque la Webcam est installée sur l'ordinateur ? Dans cette hypothèse à qui doivent-ils l'adresser et sous quelle forme ? L'autorisation doit-elle au contraire intervenir à chaque connexion de la Webcam ? Ce qui techniquement se révèle contraignant mais aussi irréaliste, une majorité d'internautes mineurs n'étant pas accompagné d'un adulte pendant leur navigation sur Internet.

En pratique l'autorisation parentale aurait du mal à être mise en œuvre. Dans les cas de diffusion et de reproduction d'image précédemment étudiés, l'autorisation devait être

²⁴⁵ Ibid.

expresse, écrite et préalable pour pouvoir être prouvée²⁴⁶. L'autorisation devait respecter un certain délai et correspondre à une finalité. Or s'agissant de la Webcam, même si l'autorisation était expresse et écrite à qui s'adresserait-elle ? S'il est vrai que le mineur va s'en servir dans ses communications avec son entourage connecté, il peut également s'en servir dans des forums de discussion où ses interlocuteurs ne sont pas préalablement déterminés. L'autorisation doit être préalable. Comment apprécier cette antériorité selon quel repère temporel ? Une autorisation avant chaque connexion serait très contraignante et pourrait être porteuse de violation du droit à la vie privée du mineur.

Parlant de vie privée, doit-on en réalité considérer les communications du mineur faites par le biais de la Webcam comme de la correspondance privée ? C'est ainsi qu'on a pu noter une place croissante de la Webcam dans les communications entre parents et enfants séparés pour diverses raisons. Cela est le cas notamment lors de la séparation de couples ayant des enfants. Pour pallier aux droits de visites insuffisants, aux confrontations houleuses entre parents à chaque désir de communication avec l'enfant, pour pallier tout simplement à l'absence du parent au quotidien. Une pratique s'est instaurée, qui n'a pas encore été consacrée par la jurisprudence ou la législation : l'utilisation de la Webcam en complément du droit de visite du parent absent²⁴⁷. Cette solution n'est pas la panacée du point de vue des droits de l'enfant ou du parent absent²⁴⁸. La Webcam présente l'avantage sur la correspondance privée (par le biais du courrier électronique ou de la messagerie Internet) de ne pas exclure les enfants ne sachant pas écrire. Les très jeunes enfants peuvent communiquer avec le parent absent. Une collaboration du parent présent sera nécessaire pour établir la connexion qu'un très jeune enfant ne saurait faire. La Webcam permet d'instaurer un contact visuel et oral permettant au parent absent de garder un lien tenu avec son enfant.

²⁴⁶ Cf. paragraphe précédent.

²⁴⁷ Libération 13-14 janvier 2001, Blandine Grosjean, Fabrice Rousselot, Quand la Toile rapièce les liens familiaux, p.2-4. Dans certaines familles « éclatées » les enfants disposent dans leur chambre d'une Webcam pour communiquer avec le parent qui est absent. Murielle Laroque-Ruelle, présidente de l'association des avocats de la famille est arrivé à négocier un accord (faute de mieux) avec l'ex-mari d'une de ses clientes afin qu'elle ait la possibilité de « voir » ses enfants enlevés par leur père au Liban via Internet. Dans un autre cas, après la séparation, la mère s'est installée avec son enfant de 2 ans aux Etats-Unis. Devant le juge des affaires familiales, la mère pour pouvoir recevoir l'autorisation d'emmener l'enfant a consenti à un rendez-vous hebdomadaire par Webcam entre le père et l'enfant qui ne savait encore ni lire ni écrire. Mais du fait du retard de la législation en la matière cela n'a pas été mentionné dans le jugement.

²⁴⁸ Article préc ; Erik Purasson, le président du Children's Rights Council (Conseil pour le droit des enfants) du New Jersey aux Etats-Unis, craint que l'on glisse vers une confusion entre un « cyber parent » et un véritable parent

La Webcam peut être affiliée à de nombreuses matières juridiques. Le droit à l'image est à prendre à considération étant entendu que la Webcam a pour fonction de véhiculer des images. La mise en œuvre de ce droit nécessitera des adaptations spécifiques dans le cas de la Webcam. Par ailleurs, les communications faites par le biais de la Webcam s'apparentent dans un sens à de la correspondance. Il s'agit de communications dont la nature publique ou privée sera à déterminer au cas par cas. Le caractère privé ou public sera retenu selon que les destinataires des images seront déterminés, déterminables ou non. On se réfère plus à une communication (privée ou publique) qu'à une correspondance, appellation qui dans son acception première se détermine par des écrits.

B. La correspondance privée du mineur dans le cyberspace.

La notion de correspondance est analysée par la doctrine comme : une communication personnelle, temporelle, susceptible d'interactivité, et adressée à des personnes déterminées et individualisées²⁴⁹. L'article 9 du code civil pose un principe général de la vie privée comme mentionné dans le paragraphe précédent. La Convention européenne des Droits de l'homme et des libertés fondamentales, de même que la Déclaration des droits de l'homme de 1948 apportent des précisions sur la définition de la correspondance privée²⁵⁰.

1. Le droit commun : le droit à la correspondance privée du mineur.

Il n'existe pas de définition légale de la correspondance privée²⁵¹. La circulaire du 17 février 1988 relative aux services télématiques²⁵² a tout de même essayé de préciser cette notion : « Il

²⁴⁹Virginie Peltier, Le secret des correspondances, PU Aix-Marseille, 1999, p. 217, n°256 et s. ; Lamy droit de l'informatique, 1997, n° 1676.

²⁵⁰ Article 8 de la Convention européenne des Droits de l'homme et des libertés fondamentales : “ *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ”. Article 12 de la Déclaration Universelle des droits de l'homme de 1948. “ *Nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur ou sa réputation* ”.

²⁵¹ Jacques Louvier, Le cadre juridique d'Internet, p.91.- LEN et correspondance privée : mise au point de MM. Ollier et Dionis du Séjour, 05 avril 2004.

http://padawan.info/fr/len/len_et_correspondance_privée_mise_au_point_de_mm_ollier_et_dionis_du_sejour.html

²⁵² Circulaire prise en application de l'article 43 de la loi 86-1067 du 30 septembre 1986 relative à la liberté de communication, concernant le régime déclaratif applicable à certains services de communication audiovisuelle <http://www.foruminternet.org/texte/documents/reglements/lire.phtml?id=25>

y a correspondance privée lorsqu'un message est exclusivement destiné à une ou plusieurs personnes physiques ou morales déterminées et individualisées »²⁵³.

Le principe du secret des correspondances est très ancien. Il a été mis en œuvre dès l'origine pour les lettres et les objets acheminés par la Poste²⁵⁴.

Internet présente la particularité s'agissant de correspondance de faire coexister deux régimes : celui de la correspondance privée et celui de la communication audiovisuelle. La nuance juridique réside dans le fait que la correspondance privée permet l'échange d'informations sans contrôle à l'exemple des communications téléphoniques ou des correspondances par voie postale. Tout filtrage revenant à violer le secret des correspondances²⁵⁵. Ce n'est pas le cas pour la communication audiovisuelle qui doit se soumettre à certaines conditions et peut faire l'objet de contrôle et de sanctions *a priori* et/ou *a posteriori*.

L'absence de définition en droit français du courrier pousse certains auteurs à faire des mises en garde sur de possibles confusions entre les notions de correspondance privée et électronique. Le premier alinéa de l'article 1er de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications dispose que « *le secret des correspondances émises par la voie des télécommunications est garanti par la loi* ». Cette définition est au mot près celle énoncée dans la directive du 12 juillet 2002²⁵⁶.

Selon la définition de la correspondance privée posée par la circulaire du 17 février 1988, il y a correspondance privée « lorsque le message est exclusivement destiné à une ou (plusieurs) personne physique ou morale, déterminée et individualisée ». En matière de courrier électronique, le destinataire est individualisé par une adresse e-mail²⁵⁷. Avant même que la jurisprudence ne se soit prononcée sur ce point, la doctrine considérait déjà que, l'envoi d'un

²⁵³ Circulaire du 17 février 1988 prise en application de l'article 43 de la Loi du 30 septembre 1986 sur la communication audiovisuelle. Cette définition de la correspondance privée est faite par opposition à la communication audiovisuelle.

²⁵⁴ M.-P. Fenoll-Trousseau, G. Haas, Internet et protection des données personnelles, Litec 2000, p.62

²⁵⁵ Christiane Feral-Schul, Le droit à l'épreuve d'Internet-Cyberdroit, Dalloz Dunod, 2^e édition, Introduction, p.6.

²⁵⁶ LEN et correspondance privée : mise au point de MM. Ollier et Dionis du Séjour, 05 avril 2004.

http://padawan.info/fr/len/len_et_correspondance_privée_mise_au_point_de_mm_ollier_et_dionis_du_sejour.html

²⁵⁷ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.36.

e-mail à une personne déterminée relevait de la correspondance privée²⁵⁸. Le tribunal correctionnel de Paris a rendu en date du 2 novembre 2000, la première décision qui a été prononcée en ce sens²⁵⁹. Cette décision sera suivie par une jurisprudence constante en la matière²⁶⁰.

Le Tribunal de Grande Instance de Paris, dans une ordonnance du 27 janvier 2003 a jugé que les courriers électroniques sont des correspondances privées bénéficiant du secret des correspondances²⁶¹. Le secret des correspondances est un principe qui découle de celui de la vie privée tel que posé par l'article 9 du code civil²⁶². Le respect du secret des correspondances émises par voie de télécommunication est garanti par la loi du 10 juillet 1991. Cette loi fait suite à la jurisprudence posée par les arrêts de la Cour européenne des droits de l'Homme *Kruslin* et *Huvig* du 24 avril 1990²⁶³.

La Convention internationale des droits de l'enfant, adoptée par l'Assemblée Générale de l'ONU le 20 novembre 1989 et entrée en vigueur le 2 septembre 1990 énonce des principes régissant la correspondance privée du mineur, en son article 16 tel que suit :

«1) Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. 2) L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

^{258 258} P.-Y. Gautier, l'e-mail in clés pour le siècle, Université Panthéon-Assas-Paris II, D.2000, p.369 et s., spéc., p.376. – L. Rapp, Le courrier électronique (e-mail), PUF 1998, collection « Que sais-je ? », p.89 et s. – S. Damartin, L'ordinateur, l'employeur et le salarié, Droit social, juin 2000, p.580 et s.

²⁵⁹ Tribunal correctionnel 17^e ch. 2 novembre 2000 : jurisdata n°2000-139077 ; D. 2000 inf. rap., p.286 ; Comm. com. électr. Janv. 2001, p.11. – L.Rapp. Secret des correspondances et courriers électr. : D.2000 n°41, p.III.

²⁶⁰ Arrêt Nikon : Cass. Soc. 2 octobre 2001 : D.2001, jurisprudence p.3148, - note P.Y Gautier, D.2001, sommaire., p.2296, obs., C. Caron ; Comm. Com. électr. Nov. 2001, commentaire. n°120, obs. A. Lepage, JCP E 2001, p.1918, note C. Puigelier ; JCP E 2002, p.73, obs. M. Vivant et J.M. Bruguière ; RTD civ., p.72, obs. J. Hauser ; Dr.soc. novembre 2001, p.915 et s., note J.E. Ray ; TPS 2001, commentaire. n°384, note P.Y. Verkind ; Droit et patrimoine 2002, n°101, p.112, note G. Loiseau.

²⁶¹ Rédaction Net-Iris veille juridique professionnelle, actualité 04/2003, Le secret des correspondances dont bénéficient les e-mails fait échec à une demande d'identification d'un expéditeur.

<http://www.net-iris.com>

Le même article apparaît dans le site clic-droit

http://www.clic-droit.com/web/editorial/imprimer.php?art_id=189

²⁶² Jacques Louvier, Le cadre juridique d'Internet, p.92

²⁶³ CEDH 24 avril 1990 (2 arrêts), *Kruslin*, D. 1990, 353, note J. Pradel, *époux Huvig*, série A, n° 176 ; à propos des écoutes téléphoniques

Le mineur a droit au respect de sa correspondance privée, ce qui englobe la correspondance électronique privée du mineur telle qu'elle peut se présenter dans le cyberspace. Ce droit à la correspondance électronique privée s'oppose aussi bien aux ingérences publiques que privées. La question s'est posée à propos des ingérences privées que pouvait souffrir la correspondance électronique privée du mineur. Les immixtions privées visées sont généralement d'origine familiale et plus précisément parentale. Les parents ont la responsabilité de veiller au bien être, et à la sécurité du mineur. Pour ce faire, ils doivent faire preuve de vigilance et mettre en œuvre une certaine surveillance du mineur. Cette surveillance peut prendre la forme d'une immixtion (légitime ou non) dans les correspondances adressées au mineur. S'agissant de correspondances ordinaires, les codes des postes et télécommunications prévoient que ces dernières, lorsqu'elles sont recommandées avec valeur déclarée, ou adressées « poste restante » à des mineurs non émancipés âgés de moins de dix-huit ans, ne peuvent leur être remises que sur présentation d'une autorisation écrite d'un parent ou tuteur légal²⁶⁴. Si on a pu aligner le droit au secret des correspondances électroniques au respect des correspondances privées tel que déterminé par le droit à la vie privée, peut-on concevoir que la tutelle des mineurs décrite ci-dessus en matière de correspondance ordinaire s'applique également au cyberspace ? En l'espèce, une autorisation préalable des parents ou tuteurs légaux pour la réception de courrier électronique semble en pratique irréalisable. A quel niveau devrait intervenir cette autorisation parentale ? A la création d'une adresse électronique, ou alors à chaque réception de courrier ? Par ailleurs sous quelle forme devrait-elle être présentée et qui serait habilité à en contrôler l'effectivité et la recevabilité ?

Que regroupe la définition de courrier électronique ? On a vu dans la définition du courrier électronique que cela concernait l'envoi d'un e-mail à une ou plusieurs personnes déterminées dans le cadre ou non d'une « mailing-list ». La multiplicité des destinataires ne suffit pas à enlever à un « courriel » la qualité de correspondance privée et la protection juridique qui en découle. Peut-on considérer comme une correspondance électronique privée la conversation qu'un mineur a dans un forum de discussion, dans un chat, du seul fait que les destinataires de ses messages sont restreints et déterminables par une communauté d'intérêt ?

²⁶⁴ Mise en œuvre de la convention internationale des droits de l'enfant en France et action gouvernementale en faveur de la situation des enfants dans le monde : <http://www.social.gouv.fr/htm/actu/convention/4g.htm>

Le droit à la correspondance privée du mineur a pris une nouvelle ampleur dans la vie familiale. C'est un élément qui contribue au maintien des liens familiaux notamment en cas d'éloignement géographique. Les communications électroniques jouent désormais un rôle prépondérant dans l'organisation des familles séparées de manière formelle ou non entre les enfants et leur parent absent. C'est une donnée qui d'une certaine manière a été imposée par les enfants adeptes au quotidien de ce mode de communication. Ils ne sont plus otages de l'animosité de leurs parents. Ils peuvent continuer sur un mode plus simple et direct que le courrier "normal" à garder un contact avec le parent absent. L'avènement et la banalisation des téléphones mobiles y contribuent également. La différence avec Internet étant le moindre coût. Une fois le matériel et l'abonnement réglés, la connexion est illimitée. Les juges aux affaires familiales n'ont pas encore formellement pris en compte cet élément dans les règlements portant sur les conflits de garde subséquents aux séparations²⁶⁵. Un seul arrêt prononcé le 19 mai 1999 par la Cour d'appel de Paris fait référence au rôle que peut avoir Internet (via les communications électroniques) entre le parent absent et son enfant²⁶⁶. Il est admis que les correspondances électroniques du mineur ne puissent souffrir d'aucune immixtion. Lorsque le message électronique est une correspondance au sens du droit pénal, il est interdit à quiconque de l'intercepter, de le détourner, de le divulguer, ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions²⁶⁷. En second lieu, le juge civil (ainsi que le juge social) accorde protection aux correspondances privées, chaque fois que ces dernières relèvent de l'exercice ou du secret de la vie privée, et dans toutes les situations, donc notamment avant leur transmission et après leur réception. La protection interdit essentiellement la prise de connaissance du contenu de la correspondance²⁶⁸.

Est-ce à dire que le droit à la correspondance privée des mineurs dans le cyberspace est absolu ? Nul droit n'est absolu. La législation française semble avoir pris le parti de prévoir dans certaines hypothèses outre une immixtion légale dans la correspondance électronique du mineur, une immixtion parentale également.

²⁶⁵ Une magistrate parisienne raconte que : « La première fois qu'un père m'en a parlé [d'Internet], j'ai trouvé ça génial. La mère était ok. C'était en 1997 ou 1998, mais je n'ai pas osé le notifier dans le jugement » ; Libération : L'évènement, samedi 13 et dimanche 14 janvier 2001, Quand la Toile rapièce les liens familiaux, Blandine Grosjean, p.2.

²⁶⁶ Cour d'appel de Paris

²⁶⁷ L'article 432-9 du code pénal incrimine par ailleurs spécifiquement le fait, pour un opérateur de communications électroniques, "agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu".

²⁶⁸ Cass., soc., 2 oct. 2001, Bull. 2001, V, n° 291, p. 233 et la divulgation de cette correspondance lorsqu'elle concerne la vie privée d'un tiers (ex. Cass. Civ. 1ère, 26 oct. 1965, Bull. n° 570) ou de toute personne physique

2. La remise en question par la Loi pour la Confiance dans l'Economie Numérique de la détermination du courrier électronique comme correspondance privée.

Il semblait acquis que le courrier électronique s'assimilait au courrier postal et bénéficiait pareillement du respect de la correspondance privée. La Loi pour la Confiance dans l'Economie numérique remet en question ce postulat. La notion de correspondance est analysée par la doctrine comme une communication personnelle, temporelle, susceptible d'interactivité, et adressée à des personnes déterminées et individualisées²⁶⁹.

La protection semble s'appliquer à toute information répondant à ces critères, durant la période de sa transmission. Inversement, un message électronique ne répondant pas à ces critères sera sans doute qualifié de communication privée par voie électronique (avec la seule protection du droit civil) ou de communication au public par voie électronique (cas notamment d'une publicité de contenu intemporel, et envoyée à des personnes non individualisées, sans possibilité d'instaurer de dialogue)²⁷⁰.

Les interrogations sur la qualification de correspondance privée du courrier électronique sont nées dans un premier temps des "listes de diffusion". Devrait-on qualifier de correspondance privée un courrier adressé à un groupe de personnes ? Dans l'affirmative quelle est la différence avec une communication publique en ligne. En effet, il n'est pas possible d'affirmer que l'expéditeur d'un message à une liste de discussion entendait l'envoyer à des personnes "déterminées ou individualisées"²⁷¹. D'où une interrogation sur la nature juridique d'une liste de diffusion.

La nature juridique d'une liste de diffusion (mailing-list) dépendra, comme toute activité sur Internet, de sa nature intrinsèque. Il y a plusieurs types de listes : les listes périodiques électroniques, modérées ou non, avec abonnement sur cooptation, avec archives publiques et/ou passerelle vers les news, avec identification forte de l'émetteur ou non...

²⁶⁹ Virginie Peltier, Le secret des correspondances, PU Aix-Marseille, 1999, p. 217, n°256 et s. ; Lamy droit de l'informatique, 1997, n° 1676.S

²⁷⁰ 25 octobre 2004 ; Modérateur Estelle De Marco et Serge Aumont , FAQ de la liste droit-net: Communication électronique : publique ou privée ? : Quelle est la nature juridique d'un message électronique?
http://listes.cru.fr/droit-net/fom?_recurse=1&file=6#file_34

²⁷¹ IRIS-MEDIATION, F.A.Q Conseils juridiques : <http://www.iris.sgdg.org/mediation/faqs/faq-conseil.html>

Chaque spécificité de la liste doit être prise en compte. Selon une jurisprudence allant dans le même sens que la circulaire définissant la correspondance privée, l'envoi d'une lettre "aux seuls membres d'un groupement liés par une communauté d'intérêts ne constitue pas une distribution publique"²⁷². "L'élément de publicité est caractérisé par la diffusion de cet écrit à un seul ou à des tiers dudit groupement"²⁷³. Une liste de diffusion sera souvent considérée comme privée, si chaque message diffusé émane de l'un des membres, pour n'être lu que par les autres membres, sous réserve de savoir la manière dont ces membres participent à la liste. Par contre, si les messages sont archivés sur un serveur, accessibles aux non-inscrits sur la liste en question, alors la communication ainsi réalisée doit être considérée comme étant publique²⁷⁴. Les mineurs aiment à se regrouper en communauté, les fondements de ces communautés sont aussi nombreux que divers. Il peut s'agir de communauté autour de préférences musicales, ou de fans clubs ; il peut s'agir de communauté autour de modes de vie comme pour les gothiques par exemples, etc. Dans un premier temps ces communautés se constituent souvent à partir de forums publics de discussion. Au fil des conversations, certains interlocuteurs se rapprochent au point de prolonger parfois leurs communications en dehors de la Toile. C'est ainsi que peuvent également se créer des mailings listes. L'enjeu étant de savoir quand qualifier ces listes de publiques ou privées. La question ne se pose pas véritablement pour les mailings listes qui sont établies à partir de carnets d'adresses privés. Par contre, pour le cas de figure mentionner plus haut, la confusion peut exister. Une mailing liste établie à partir de contacts dans un forum de discussion public peut-elle être privée au motif qu'il s'agit d'une communauté restreinte et identifiable conçue dans le cadre d'une communauté publique plus large ?

Il faut distinguer selon le type de liste et, selon les modalités de fonctionnement de la liste concernée. Si la mailing liste ne s'adresse qu'à certaines personnes bien définies et identifiables, c'est de la correspondance privée. Considérée comme une « extension du courrier électronique »²⁷⁵, la liste de diffusion relève a priori de la communication non publique²⁷⁶. La communauté d'intérêt entre les destinataires est un facteur qui permet de définir comme correspondance privée un courrier électronique envoyé à une liste de

²⁷² C.Cass., Chambre criminelle, 18 mai 1954

²⁷³ Crim 15 juillet 1981

²⁷⁴ 30 avril 2002, Modérateur Estelle De Marco et Serge Aumont ; FAQ de la liste droit-net : Communication électronique : publique ou privée ? Quelle-est la nature juridique d'une liste de diffusion?

http://listes.cru.fr/droit-net/fom?recurse=1&file=6#file_34

²⁷⁵ B. Ader, La loi de 1881 à l'épreuve d'internet : LÉgipresse, juin 1997, II-65, spéc., p.66.

²⁷⁶ C. Debbasch, H. Isar, X. Agostinelli, Droit de la communication, Dalloz 2002, 1ere éd, n°919. – J.-F. Chassaing, Internet et le droit pénal : D. 1996, chronique. p.329, n°1.

diffusion²⁷⁷. *A contrario*, une liste de diffusion peut être ouverte et de ce fait, son envoi a vocation à relever de la communication publique²⁷⁸. Dans l'hypothèse où il suffit sur simple demande d'être inscrit sur la liste, et que cette demande est systématiquement accordée, alors ce n'est plus de la correspondance privée mais de la communication publique ; la violation de la correspondance privée ne peut être retenue dans ce cas de figure²⁷⁹.

La correspondance privée et les forums de discussion. Les outils de discussion, accessibles à un nombre variable de personnes sont porteurs d'ambivalence. Cette ambivalence porte sur la distinction entre une correspondance privée et une communication publique. Dans les forums de discussion, sont rassemblées les contributions des participants²⁸⁰. En raison de l'absence d'une communauté d'intérêts liant entre eux les participants, la doctrine est encline à reconnaître l'appartenance des forums à la qualification de communication audiovisuelle²⁸¹. Il n'est cependant pas exclu que, du fait de l'organisation particulière d'un forum, (par exemple limitations de son accès à des personnes présentant une même qualité) ce dernier puisse ne pas relever de la qualification de communication publique²⁸². Les instruments de discussion se répartissent en trois catégories d'instruments :

- Publics (forum, IRC – Internet relay chat)
- Semi-publics (listes de diffusion)
- Privés (courrier électronique et ICQ- I seek you : « système de discussion par écrit synchrone avec sélection des partenaires sous la forme de listes de contacts »)²⁸³.

Bien que la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie des télécommunications garantisse en son article 1 alinéa premier le secret des

²⁷⁷ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.82.

²⁷⁸ L. Bochuberg, Internet et commerce électronique, Delmas 2001, 2^e éd., n°430. – L. Rapp, Le courrier électronique (E-mail), PUF 1998, coll. « Que sais-je ? », p.23. Une décision du TGI de Paris a considéré au sujet d'une liste de diffusion qu'il s'agissait d'un « lieu privé ouvert au public », TGI Paris, 1^{er} ch., 1^{er} sect., 12 déc. 2001 : Comm. com. électr. Juin 2002, commentaire. n°92, obs. A. Lepage.

²⁷⁹ Ibid.

²⁸⁰ A. Lepage, op.cit, p.80.

²⁸¹ P. Auvret, L'application du droit de la presse au réseau Internet : JCP G 1999, I, 108, n°11. – C. Debbasch, H. Isar, X. Agostinelli, Droit de la communication, Dalloz 2002, 1^{er} éd, n°920. – TGI Paris, 17^e ch. 26 mars 2002 : Comm. com. électr. Mai 2002, commentaire. n°78, obs. A. Lepage.

²⁸² A. Lepage, op. cit, p.82.

²⁸³ V. Beaudoin et J. Velkovska, Un univers relationnel sur Internet : forum et pages personnelles en Comprendre les usages d'Internet, sous la direction E. Guichard, Editions Rue D'Ulm, 2001, p.217 et s.

correspondances, une polémique est née de la définition des correspondances privées donnée par la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004²⁸⁴.

La loi 2004-575 du 21 juin 2004 dite LCEN, reprend les dispositions de l'article 2 de la loi n° 86-1067 du 30 septembre 1986 définissant une communication électronique : « *On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique* ».

Les parlementaires de l'opposition saisirent le Conseil constitutionnel en application de l'article 61 *alinéa* 2 de la Constitution²⁸⁵, en vue de faire censurer certaines dispositions de cette loi. Le texte de la saisine visait entre autre le non-respect du secret des correspondances par la voie électronique. Pour justifier cette saisine, ses auteurs ont fait valoir que le paragraphe IV du dernier *alinéa* de la loi ne faisait plus référence à la notion de correspondance privée²⁸⁶. Le passage incriminé définissait « *le courrier électronique [comme] tout message, sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère* ».

De l'avis des auteurs de la saisine, la suppression de la référence à la notion de correspondance privée aurait pour conséquence « *d'ouvrir la possibilité de contrôle indifférencié et sans limite préalable de l'ensemble des échanges réalisés à titre privé entre personnes identifiées* »²⁸⁷. Cette définition viendrait en contradiction de la circulaire du 17 février 1988, prise en application de la loi du 30 septembre 1986 et qui donne la définition de la correspondance privée à laquelle on se référait jusqu'alors. La conséquence en serait de créer un nouveau régime du courrier électronique, distinct à la fois de la communication publique en ligne et de la correspondance privée.

²⁸⁴ LOI 2004-575 du 21 juin 2004 Loi du pour la confiance dans l'économie numérique Texte de loi publié au Journal officiel de la République française n° 143 du 22 juin 2004, page 1168.

²⁸⁵ Art. 61.1) Les lois organiques, avant leur promulgation, et les règlements des assemblées parlementaires, avant leur mise en application, doivent être soumis au Conseil Constitutionnel qui se prononce sur leur conformité à la Constitution. 2) Aux mêmes fins, les lois peuvent être déferées au Conseil Constitutionnel, avant leur promulgation, par le Président de la République, le Premier Ministre, le Président de l'Assemblée Nationale, le Président du Sénat ou soixante députés ou soixante sénateurs.

²⁸⁶ Thèse de Jean-Pierre Mignard, Cybercriminalité et cyber-répression entre désordre et harmonisation mondiale, Université Paris I Panthéon Sorbonne, p.329.

²⁸⁷ Ibid. Le Conseil constitutionnel a été saisi de cette requête des parlementaires le 18 mai 2004. La saisine du Conseil constitutionnel s'appuie également sur la violation des articles 2 garantissant le droit à la vie privée et 11 consacrant la liberté de communication de la déclaration de 1789 de même que sur la violation.

Le Conseil constitutionnel a répondu brièvement dans une décision du 10 juin 2004²⁸⁸. Selon lui, la disposition décriée « se borne à définir un procédé technique ». De ce fait, le régime juridique de la correspondance privée n'est pas remis en cause. En cas de contestation il appartiendra à l'autorité juridictionnelle de se prononcer sur sa qualification. L'article 1^{er} de la loi du 10 juillet²⁸⁹ conserve sa vocation à s'appliquer quel que soit le procédé technique par lequel la correspondance privée est émise. Cette précision rassure quant à la reconnaissance du courrier électronique comme correspondance privée, bénéficiant de ce fait d'une protection appropriée. Le régime juridique de la correspondance privée électronique étant ainsi conforté, les mineurs pourront opposer à tous, le droit au respect de leur correspondance électronique privée contre toute ingérence privée ou publique. Ce droit dont ils peuvent valablement se prévaloir dans le cyberspace doit être respecté et protégé. Le mineur dispose de droits dans le cyberspace qui supposent une protection accrue de tous les intervenants du cyberspace. Il peut également user dans le cyberspace de libertés rattachées à sa personne : ses libertés individuelles.

²⁸⁸ Décision n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique
<http://www.conseil-constitutionnel.fr/decision/2004/2004496/2004496dc.htm>

²⁸⁹ « Le secret des correspondances émises par la voie de des télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seules cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci »

Chapitre 2. LES LIBERTÉS INDIVIDUELLES DU MINEUR DANS LE CYBERESPACE.

Le cyberspace est entendu comme le lieu par excellence d'application et de respect des libertés individuelles de tous les internautes. Le mineur internaute doit être en mesure de faire sans entraves, usage de ses libertés individuelles dans le cyberspace sauf à respecter les libertés d'autrui, de même que la législation du territoire dans lequel il se trouve. Les libertés individuelles dont le mineur est le plus susceptible de faire usage dans le cyberspace sont : la liberté d'expression et la liberté créatrice autrement dit le droit d'auteur. Ces libertés doivent s'appliquer dans le cadre de réglementations définies. Ces réglementations visant le double objectif de faire respecter au mineur les libertés d'autrui et d'assurer leurs protections.

La liberté d'expression n'est pas sans limite. Le mineur dispose sur la Toile de plusieurs outils lui permettant de diffuser son expression, ou celle d'autrui. Le mineur grâce à sa liberté d'expression peut faire œuvre créatrice dans le cyberspace. Ses créations faites ou diffusées dans le cyberspace sont régies par le droit d'auteur. Il s'agira ici d'analyser la liberté d'expression du mineur et son droit d'auteur en considération du statut juridique spécifique des mineurs.

§1. La liberté d'expression du mineur dans le cyberspace.

La liberté d'expression et d'opinion est universellement consacrée comme un droit fondamental de tout individu dans toute société démocratique. Il faut considérer l'individu dans son acception générale. La liberté d'expression bénéficie autant à ceux qui diffusent l'information qu'à ceux qui la reçoivent. De nombreux textes nationaux et internationaux consacrent la liberté d'expression. La Constitution française de 1958 la consacre, dans son préambule ; ce faisant elle reprend la Déclaration des droits de l'homme et du citoyen de

1789²⁹⁰. Cette même année, la Constitution américaine de 1776 fut amendée pour la première fois, et la liberté d'expression consacrée par le premier amendement qui lui confère une portée quasi absolue²⁹¹. La Déclaration universelle des droits de l'homme du 10 décembre 1948²⁹², consacre également cette liberté. Un texte consacre spécifiquement la liberté d'expression de l'enfant ; il s'agit de la Convention internationale des droits de l'enfant²⁹³ du 20 novembre 1989.

De l'avis de certains auteurs, il n'existe pas une mais plusieurs libertés d'expression²⁹⁴. La liberté d'expression peut se manifester par l'écrit, le son, l'image, etc. La liberté d'expression peut se manifester par le biais de différents types de communications électroniques. S'agissant de la liberté d'opinion, il est courant de l'associer au droit de la presse régit par la loi de 1881. Différents courants s'affrontent sur le fait de savoir si la liberté d'expression est absolue ou si elle doit souffrir des limites établies par la loi. Pour appréhender la nature et les implications de la liberté d'expression du mineur dans le cyberspace, il va falloir dans un premier temps étudier ses manifestations dans le cyberspace avant d'en étudier les limites.

A. Les manifestations de la liberté d'expression des mineurs dans le cyberspace.

La liberté d'expression du mineur trouve à s'appliquer quand il échange de la correspondance (privée ou non), lorsqu'il intervient dans des forums de discussion, lorsqu'il écrit et édite des contenus dans des pages personnelles ou tout autre support de la Toile. La nature particulière du cyberspace induit une imbrication entre les sphères publiques et privées, ce qui ne cesse de poser des problèmes du point de vue de la régulation. Le cyberspace un espace public qui

²⁹⁰ Article 11 « *La liberté de communication des pensées et opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* »

²⁹¹ « *Le Congrès ne pourra faire aucune loi ... restreignant la liberté de la parole et de la presse* »

²⁹² « *Tout individu a droit à la liberté d'expression et d'opinion, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit*
L'exercice de ce droit ne peut faire l'objet que de seules restrictions qui sont prescrites par la loi et qui sont nécessaires»

²⁹³ Article 13 « *L'enfant a droit à la liberté d'expression, ce droit comprend la liberté de rechercher, de recevoir, de répandre des informations et des idées de toutes espèces, sans considération de frontière, sous une forme orale, écrite, imprimée ou artistique, ou par tout moyen du choix de l'enfant* ».

²⁹⁴ Christiane Feral-Shuhl, *Le droit à l'épreuve d'Internet*, 2^e édition Dalloz-Dunod, p.86-87.

dans le temps une somme de plusieurs relations « privées » ; cette configuration du cyberespace fait qu'il recherche en permanence son équilibre²⁹⁵.

1. La liberté d'expression du mineur dans un espace public.

La liberté d'expression est plus facile à mesurer et à contrôler dans un espace public. La tâche se révèle malaisée dans un espace privé puisque cela suppose une violation de la vie privée du mineur se caractérisant par la violation du secret de sa correspondance. Il convient dans un premier temps de s'intéresser aux modes d'expression publique du mineur sur le Web. La liberté d'expression du mineur s'entend ici comme de la communication en ligne, de la communication audiovisuelle²⁹⁶ par opposition à la communication privée sous-entendue dans un espace privé.

1-a. Les communications privées du mineur dans des espaces publics.

Le rôle des mineurs, a fortement évolué en matière de communication publique grâce à Internet²⁹⁷. Cela s'explique par le fait qu'Internet favorise l'auto publication dans des proportions jusque là inégalées. La frontière entre auteur et destinataire est brouillée²⁹⁸, chacun peut prétendre alternativement et/ou simultanément à l'une ou l'autre des deux qualités²⁹⁹. Cela se vérifie aisément pour les pages personnelles où les mineurs sont indifféremment auteur et/ou lecteur.

1.a'. Les pages ou les sites personnels.

Les pages personnelles sont l'un des modes phares de manifestation de la liberté d'expression. Les jeunes internautes sont de plus en plus nombreux à se construire des pages personnelles sur le Web. Ces pages personnelles créées pour répondre à des motivations diverses peuvent

²⁹⁵ Céline Halpern, Droit et Internet, Guide juridique et pratique, Editions de Vecchi, p.5.

²⁹⁶ L'article 7 du projet de loi sur la société de l'information prévoyait d'insérer à l'article 2 de la loi n° 86-1067 du 30 septembre 1986 une définition de la communication en ligne comme étant « toute communication audiovisuelle transmise sur demande individuelle formulée par un procédé de télécommunication » ; la communication audiovisuelle est définie à l'article 2, alinéa 2 de la loi du 30 septembre 1986 comme « toute mise à disposition du public ou de catégories de public, par un procédé de télécommunications, de signes, de signaux, d'écrits, d'images, de son ou de messages de toute nature qui n'ont pas le caractère de correspondance privée » ; la circulaire du 17 février 1998, prise en application de l'article 43 de la loi du 30 septembre 1986, précise qu' « il y a communication audiovisuelle lorsque le message est destiné à un ensemble d'individus indifférenciés, sans que son contenu soit fonction de considérations fondées sur la personne »

²⁹⁷ J. Huet, La diversité culturelle sur le net, in Le droit de l'informatique au tournant du millénaire, sous la direction de X Linant de Bellefonds, Publibook 2001, p.247 et s., spéc., p.250.

²⁹⁸ J. Gautrand, L'empire des écrans, Le pré aux clercs 2002, p.73 et 74.

²⁹⁹ A. Finkielkraut, P. Soriano, Fatale liberté, Internet. L'inquiétante extase, Mille et Une nuits 2001, p.31 et s.

être consacrées à un hobby (collection, fan club...), à un thème précis sur lequel les adolescents souhaitent échanger avec des internautes affichant un intérêt similaire au leur. L'échange vise un partage de leurs expériences respectives, l'échange d'astuces, etc. On a pu voir des mineurs échanger sur des choses aussi diverses que la sexualité, le divorce des parents, les familles recomposées, le suicide, des exercices de classes, des jeux, films, etc.

Au-delà du besoin de s'exprimer librement, l'ambition est de créer de véritables communautés, reconnaissables par des codes déterminés. Dans l'hypothèse des pages ou des sites personnels basiques, les visiteurs viennent prendre connaissance des informations ou des avis sur un sujet présenté par l'auteur. Ils n'ont pas nécessairement l'opportunité d'interagir avec les autres visiteurs ou même avec le webmestre qui se confond souvent avec l'auteur ; ce cas de figure a tendance à se marginaliser. En réalité, ces sites sont dans presque leur totalité accompagnés de forums de discussion ou chats, qui permettent d'interagir sur les sujets traités par l'auteur et même d'entamer des discussions liées au thème traité ou correspondant à l'esprit de la page personnelle.

Les "ados" tentent de reconstituer avec des « internautes du bout du monde des tribus analogues à celles des cours de récréation »³⁰⁰. Ces pages sont une continuité des conversations des cours de récréations, l'avantage étant que l'audience est plus large et que le mineur peut s'abriter derrière un relatif anonymat (utilisation de pseudo) pour s'épancher sans crainte de se voir reconnaître.

Comme son nom l'indique, la page personnelle du mineur est une expression personnelle de ce dernier sur ce qui lui tient à cœur, cette page se décline le plus souvent sous les trois modes d'expression qu'offre Internet : l'écrit, l'image et le son ; les deux premiers étant les plus fréquemment utilisés. Par l'écrit le mineur reçoit et émet des messages instantanés ou non en direction des visiteurs interactifs de son site personnel. Par l'image, il illustre ses propos, soit en se mettant lui-même en scène dans une espèce de journal sur Internet (avec la Webcam et un microphone comme outils principaux) ; il peut également illustrer de photographies ou de vidéographies les sujets à la Une dans son site. Le son est souvent couplé avec l'image, mais à l'ère du téléchargement numérique et d'échange de musique, il peut se suffire à lui-même.

³⁰⁰ Télérama N° 2565-10 mars 1999, Claire Cardan, Les ados tissent leur Toile, p.88.

Loin des billets d'humeur sur des faits et phénomènes de société, le mineur peut avoir le désir de diffuser une expression plus personnelle et plus intime : son journal intime.

1.a". Le blog ou weblog

Le blog³⁰¹ ou weblog regroupe plusieurs réalités. Le concept *blog* est assez vague et englobe de ce fait plusieurs usages. Son succès est dû en grande partie à la facilité de publication qu'il promet, à la grande liberté éditoriale qu'il permet et à l'interactivité avec le lectorat. La majorité des blogs s'utilisent à des fins d'autoreprésentation quel qu'en soit l'objectif, c'est ce qui a pu provoquer des réactions fustigeant l'égoïsme que le blog véhiculerait.

Le blog peut être un journal intime, un carnet de bord dans lequel l'auteur inscrit au jour le jour ses pensées les plus intimes sur tous les sujets possibles. Ce type d'écrits avait pour vocation première de rester personnels, de n'être lus par aucune autre personne que son auteur. C'est pour cette raison qu'il représente l'essence même de la liberté d'expression puisque, aucune censure n'est *a priori* possible. Le blog semble bouleverser cet état de fait. Il faut toutefois relativiser le bouleversement dont aurait été porteur le cyberespace s'agissant de la diffusion des journaux intimes.

Le journal intime n'a pas attendu l'avènement d'Internet pour sortir de sa sphère intime afin d'être publiquement diffusé. C'est ainsi qu'un des journaux intimes le plus célèbre a été publié après la seconde guerre mondiale : "*Le journal d'Anne Frank*"³⁰². Il n'a pas été publié à l'initiative de son auteur cependant³⁰³. Il existe dans la littérature d'autres exemples de publication de journaux intimes. Il est vrai que comme en toute chose, le cyberespace est un facteur amplificateur de phénomènes préexistants.

³⁰¹ Un blog ou blogue (aphérèse de *web log*) est un site Web constitué par la réunion d'un ensemble de *billets* triés par ordre chronologique. Chaque billet (appelé aussi *note* ou *article*) est, à l'image d'un journal de bord ou d'un journal intime, un ajout au blog ; le *blogueur* (tenant du blog) y porte un texte, souvent enrichi d'hyperliens et d'éléments multimédias et sur lequel chaque lecteur peut généralement apporter des commentaires.

<http://fr.wikipedia.org/wiki/Blog>

³⁰² Le journal d'Anne Frank, La première édition française du Journal d'Anne Franck a paru en 1950 aux éditions Calmann-Lévy, avec une préface de Daniel-Rops

³⁰³ Il s'agissait du journal écrit par une adolescente allemande et de confession juive pendant la seconde guerre. Ce journal ne fut pas publié de son propre chef mais plutôt à l'initiative de son père alors qu'elle-même était décédée

On a pu noter récemment la pratique croissante de diffusion de journaux intimes en ligne³⁰⁴ et accessibles à tous. Cette pratique fédère autour d'elle de véritables communautés³⁰⁵. Une condition incontournable à cette communauté est l'anonymat³⁰⁶, bien que de plus en plus de personnes n'hésitent pas à diffuser nommément leur journal intime. L'expression est libre mais pas absolue et n'engage que son auteur³⁰⁷. Le mineur qui s'est joint à cette mouvance, a par ce biais la possibilité de rendre sa vie privée publique sans que cela ne soit préjudiciable à son identité réelle quant il utilise un pseudonyme. Il peut s'exprimer assez librement du fait de cet anonymat ; mais comme on l'a noté ses propos peuvent engager sa responsabilité, et les administrateurs se réservent un droit de censure sur les contenus. Ce faisant les administrateurs répondent à une obligation de résultat qui n'est pourtant pas exigée par la loi. Ils interviennent en amont de la loi.

Les journaux intimes des mineurs sont souvent des témoignages en appelant d'autres. Le mineur, dans un cri de détresse parfois, révèle des faits, des sentiments qu'il ne peut partager ou exprimer avec son entourage immédiat. Les blogs tenus par des adolescents sont très nombreux en France³⁰⁸.

³⁰⁴ Ph. Lejeune, *Cher écran...Journal personnel, ordinateur, Internet*, Seuil 2000. – *Adde Le Monde des livres*, 12 janvier 2001, p.VI.

³⁰⁵ Il existe un site qui s'intitule *Journal intime.com* qui publie une charte du journal intime en ligne, il s'agit d'une véritable communauté virtuelle tournant autour du thème du journal intime. La communauté est composée par les membres du site : <http://www.journalintime.com/charte.html>

³⁰⁶ Dans tous les cas ici nous désirons tous rester anonymes et garder une certaine sphère de vie privée, même si certains diffusent leur vie privée à l'aide d'un journal sur le web. Ainsi nous vous demandons de respecter la vie privée et l'anonymat de chacun. Ne cherchez pas à tout prix de découvrir qui se cache derrière tel ou tel pseudo. Si vous faites partie de l'entourage proche ou que vous connaissez un membre qui écrit dans le site, merci de garder ceci pour vous et de ne pas l'exposer publiquement : <http://www.journalintime.com/charte.html>

³⁰⁷ En vous inscrivant vous reconnaissez que ni l'hébergeur de ce site ni son (ses) administrateur(s) ne sauraient être tenus pour responsable des propos que vous tenez dans les forums des journaux ou du site ainsi que ceux tenus dans les messages privés ou dans votre propre journal. Cependant les administrateurs du site s'engagent de par la loi française en vigueur à fournir les données techniques permettant de vous identifier (adresses IP et heures de connexion) aux autorités compétentes si celles-ci en font la demande. Les messages à caractère manifestement illicites pourront être censurés par le(s) administrateur(s).

³⁰⁸ Près de six millions de blogs sur skyblogs selon le site en 2006 et plus généralement sur le Web, voire http://fr.wikipedia.org/wiki/Weblog#Pr.C3.A9sentation_et_vari.C3.A9t.C3.A9_de_la_blogosph.C3.A8re

Dans un autre registre, et toujours sous l'appellation de weblogs³⁰⁹ : il y a des textes écrits par des anonymes sur les sujets les plus divers, souvent dans une perspective de critique sociale³¹⁰. Ce type de blogs a envahi le cyberspace où il est quasiment omniprésent. Les blogs ont connu un véritable essor entre 2004 et 2005. Leur avènement et leur succès sur la toile ont sonné le glas des « pages perso » dans la mesure où leurs raisons d'être se confondent. Le blog a deux dimensions qui peuvent se rejoindre : l'écrit et l'image. Dans le premier cas il s'agit de partager sa vision des choses sur des thèmes donnés et dans le second il s'agit de partager des images et/ou du son (photographies, vidéographies, musique avec son cercle d'amis et au-delà).

Du journal intime qui a renoncé à sa confidentialité à l'outil de communication institutionnel ou de libre expression au service des collectivités locales et des citoyens, les blogs sont devenus pour certains d'entre eux une source d'information alternative aux médias traditionnels³¹¹. Ils drainent les déçus des médias traditionnels. De l'avis d'un professeur de droit américain ils donnent toute sa portée au premier amendement de la constitution américaine garant d'une liberté d'expression quasi-absolue³¹².

Les weblogs sont aussi vieux qu'Internet même si ils ne portaient pas cette appellation à l'origine³¹³. Les weblogs actuels sont de vrais journaux auxquels tout le monde peut participer³¹⁴. On en trouve sur absolument tous les sujets. La guerre contre l'Irak, la littérature,

³⁰⁹ Le mot Weblog ou plus simplement « blog » désigne une sorte de journal intime publié sur le web. On dit aussi « carnet web » et « blogue » au Québec : <http://www.internenettes.fr/savoir/weblogs.html>
Le terme weblog est une contraction des termes Web – Toile et Log – journal, bloc-notes. Ce terme fut utilisé pour la première fois en décembre 1997 par John Barge, Peter Merholz réduira la contraction au terme blog en 1999 ; selon la commission générale de terminologie et de néologie le weblog est un journal ou un bloc-notes souvent personnel présentant en ordre chronologique de courts articles ou notes généralement accompagnés de liens vers d'autres sites, Avis public paru au Journal Officiel le 25 mai 2005 ; A la fin de l'année 2004 27% des internautes américains ont déclarés être des lecteurs de blogs , Blogs et droits, Olivier Sanviti et Patrick Vibert, <http://www.legalbiznet.com/cgi-bin/viewnews.cgi?category=1&id=1119961511>

³¹⁰ Libération, 19 mars 2002, p.30 ; Libération, 19 avril 2002.

³¹¹ Nicole Bondoïs et M. Nicolas Samarcq, Les Blogs, un service d'édition en ligne soumis aux mêmes règles que les sites Internet <http://www.droit-ntic.com/news/afficher.php?id=314>

³¹² A. Lepage, op. cit, p.63.

³¹³ Les Weblogs existent depuis décembre 1997, date à laquelle John Barger leur a donné ce nom. <http://www.robotwisdom.com> Mais il faut remonter plus loin dans l'histoire d'Internet pour retrouver leur véritable origine. Quand Internet a commencé, des tas de gens ont fait une page perso sur leur thème favori, à laquelle ils joignaient toujours une liste de liens vers des pages traitant du même thème. Le phénomène prenant de l'ampleur, on a vu se créer des répertoires par thèmes de tous ces sites, car de plus en plus de gens souhaitaient publier leurs contributions.

³¹⁴ De l'avis de A. Lepage ce sont des intermédiaires entre les pages personnelles et les webzines. Les webzines sont ou e-zines sont des magazines créés directement et exclusivement sur le net. « Dépourvus de toute affiliation avec une publication en papier, ils représentent la génération spontanée de la presse électronique et se

l'actualité, le dernier album d'un chanteur de rap, les nouvelles technologies, l'athéisme, ou la politique en Louisiane³¹⁵.

Au sens de la loi, le titulaire d'un blog est un éditeur de service de communication publique en ligne soumis aux dispositions de la loi sur la liberté de la presse, sur la communication audiovisuelle et la loi pour la Confiance dans l'Economie Numérique. A ce titre, il est tenu à l'obligation d'identification posée par l'article 6-III de la loi du 21 juin 2004. Il doit déclarer auprès de son hébergeur ses nom, prénom, domicile et numéro de téléphone. Cependant, au titre l'obligation d'identification, le blogueur non professionnel peut préserver son anonymat. Dans ce cas, il peut décider de ne communiquer que son pseudonyme ainsi que le nom, la dénomination ou la raison sociale et l'adresse de son hébergeur, sous réserve toutefois d'avoir communiqué à ce dernier certains éléments d'identification personnelle (LCEN article 6-III-2). A cet égard, la loi insiste sur la soumission de l'hébergeur au secret professionnel à moins que l'autorité judiciaire n'en requière autrement³¹⁶.

En mars 2005, entre 8 et 10 millions de blogs étaient recensés. Entre 35 000 et 40 000 nouveaux blogs seraient créés chaque jour dans le monde³¹⁷.

1-b. Les communications publiques du mineur.

Il va de soi que les communications privées (reconnues comme telles) du mineur doivent bénéficier du secret des correspondances privées. Mais le mineur ne circonscrit pas son expression à des espaces privés dans le cyberspace ; il est également amené à s'exprimer dans des espaces publics. Dans l'hypothèse de la manifestation de la libre expression du mineur dans des espaces publics, quel régime juridique doit régir sa liberté d'expression ?

targuent d'une plus grande indépendance d'esprit » ; A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.65

³¹⁵ <http://www.internenettes.fr/savoir/weblogs.html>

³¹⁶ Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, Dalloz 2006, p.580.

³¹⁷ Conférence de la famille 2005, « Protection de l'enfant et usages d'Internet », Rapport remis à Philippe Douste-Blazy par le Président du groupe de travail Joël Thoraval et le Rapporteur Olivier Péreldi, p. 35.

Les forums de discussion³¹⁸ et les chats. Un forum de discussion peut être défini comme étant un « un lieu public virtuel »³¹⁹. Les forums de discussion, lorsqu'ils ont le caractère de communications publiques, peuvent prendre la forme de véritables tribunes pour les mineurs. Il s'agit souvent d'espaces qui leurs sont propres et qui respectent certains codes (code de langage notamment). Toute personne ignorante ou faisant fi des codes en vigueur dans de tels espaces sera très vite démasquée et indexée. Ces forums peuvent être très spécialisés et ne porter que sur un ou des sujets bien définis, ou alors un espace fourre-tout d'expression. Un parallèle a été établi entre les forums de discussion et les émissions sur les radios libres destinées aux adolescents. Le maître mot semble être la liberté totale d'expression. En réalité, il existe toujours un modérateur qui reste discret mais n'hésite pas à intervenir dès lors que des abus, des débordements, sont constatés. Une nuance doit toutefois être observée, l'animateur de l'émission radiophonique joue le rôle de modérateur, tandis que sur le Web, tous les forums ne sont pas nécessairement dotés d'un modérateur³²⁰ ; cela devient cependant la norme dans un nombre croissant de cas.

Le recours à des modérateurs³²¹ permet d'empêcher les dérives, de repérer des intrusions nocives et malveillantes (prédateurs, discours racistes, négationnistes, etc.)³²². Par ailleurs, et à la différence de la radio, le Web a une dimension planétaire et intemporelle qui nécessite une veille constante.

Les pseudonymes jouent un rôle prépondérant dans la liberté d'expression des mineurs sur le Web. Abrisés derrière leur(s) identité(s) virtuelle(s), ils libèrent leur expression. Ils osent s'exprimer sur tous les sujets, d'une manière désinhibée qu'ils ne se permettraient pas dans leur identité réelle par opposition à leur identité virtuelle. Tout semble permis, c'est leur alter ego qui s'exprime sur des sujets autrement tabous. Certains auteurs rebondissant sur cette question ont pensé remettre en question les droits de la personnalité dont la liberté d'expression fait partie dans le cyberspace³²³. Cette position s'appuyait sur le fait que,

³¹⁸ Les forums de discussion furent créés en 1979 par deux étudiants en mal de communication, E. Wery, Sexe en ligne : aspects juridiques et protection des mineurs, Droit des technologies, Edition Larcier 2004, p.19.

³¹⁹ B. Ader, La loi de 1881 à l'épreuve d'Internet, Légipresse n°142, juin 1997. II., p.65.

³²⁰ Le site Kazibao, qui est un forum destiné aux adolescents est doté d'un animateur. Il s'agit d'une psychologue pour enfants et adolescents en la personne d'Annette Dumesnil.

³²¹ Ce sont des personnes chargées de surveiller la bonne moralité des messages circulant sur un chat ou forum.

³²² Internet et la liberté d'expression : www.cyberworkers.com/ledroit.fr/index_int_et_laliberte.shtml

³²³ UNESCO, Les droits de l'homme dans le cyberspace, Collection Droit du cyberspace, Mark Turnet (avocat associé au cabinet Herbert Smith – Londres), Economica 2005, p.32.

Internet permettant d'adopter plusieurs identités, ces personnes virtuelles et donc factices ne pouvaient bénéficier du droit des personnes à la liberté d'expression.

Tout n'est pour autant pas permis dans un forum de discussion. Pour ce faire il existe un triple dispositif qui vient en amont de la responsabilisation des auteurs de contenus préjudiciables sur Internet. Tout forum de discussion doit en principe afficher une charte de participation³²⁴, disposé d'un modérateur, et ses organisateurs doivent gérer les litiges³²⁵ préalablement à toute intervention judiciaire.

Les forums de discussion ou les chats sont de véritables tribunes dédiées à la liberté d'expression. Des communautés durables ou éphémères s'y créent autour de thèmes, centres d'intérêt aussi divers les uns que les autres. Les conversations et les relations qui en résultent peuvent être durables et se poursuivre hors du forum voire même de la Toile. Les liens noués dans ces espaces, peuvent ne durer que le temps de la discussion et s'éteindre au moment de la déconnexion du newsgroup.

Les conversations y sont de natures diverses. Elles ont vocation à être publiques et générales. Mais il peut arriver que des internautes ressentent le besoin de s'isoler dans un aparté. Les chat-room ou salons de discussion permettent « de discuter à plusieurs sur une page centrale et de tenir exclusivement ou simultanément des conversations privées avec d'autres interlocuteurs dans des chambres individualisées »³²⁶.

Dans ces forums de discussion, dès lors qu'est instaurée une limitation d'accès à des personnes présentant une même qualité, travaillant dans le même endroit ou s'agissant des mineurs appartenant au même établissement ou plus généralement présentant un critère distinctif et sélectif, on sort de la nature publique du forum de discussion pour pénétrer dans une sphère privée.

³²⁴ Selon une charte standard, le sujet du forum doit être respecté, précisé les aspects techniques d'accès et de participation au forum, les règles de bonne conduite à respecter, la détermination du type de modération *a priori* ou *a posteriori* et les responsabilités encourues par les auteurs, voire Le forum des droits sur Internet, Rapport d'activité 2003, La Documentation Française, 2004, p.243.

³²⁵ Le forum des droits sur Internet, Rapport d'activité 2003, La documentation française 2004, p.243.

³²⁶ B. Ader, La loi de 1881 à l'épreuve d'Internet, art. préc.

Tout ce qu'un mineur peut écrire dans un chat ou dans un forum de discussion n'est visible par d'autres que lorsqu'il est dans un espace public ou si dans le cadre d'un aparté il a invité d'autres personnes à le rejoindre lui et son interlocuteur principal. *A contrario*, dans les apartés « personne n'écoute ni ne filtre »³²⁷ selon le principe qui régit les échanges privés.

2. La liberté d'expression du mineur dans un espace privé.

La liberté d'expression du mineur dans un espace privé est caractérisée en majorité par de la correspondance privée. La nuance se trouve dans les différentes formes et natures de cette correspondance.

2-a. La correspondance électronique du mineur.

La correspondance électronique du mineur se décline sous plusieurs formes. Au fil du temps, elle s'enrichit de nouvelles applications que les jeunes internautes savent mettre à profit. A ce jour il existe deux modes principaux de correspondance électronique :

- le courrier électronique sous sa forme classique et qui s'apparente au courrier papier, la différence résidant dans la matérialité du courrier et dans son acheminement par les réseaux en lieu et place de moyens de transport classiques.
- il existe un autre type de correspondance électronique très prisée par les jeunes internautes du fait de son caractère instantané, et de la possibilité de communiquer simultanément avec plusieurs interlocuteurs : la messagerie instantanée. Ce mode de communication se rapproche des possibilités de communication en conférence que permet le téléphone. La différence est que l'une est uniquement orale, tandis que l'autre peut être écrite et orale.

2.a'. Le courrier électronique.

La liberté d'expression trouve à s'appliquer là où l'internaute mineur fait œuvre créatrice et donne son opinion. Le courrier électronique du fait qu'il est reconnu comme correspondance privée bénéficie des mêmes protections que la correspondance privée. Il en résulte que la liberté d'expression véhiculée dans un courrier électronique échappe en principe à tout contrôle, sauf dispositions légales précisément déterminées par la loi. Il s'agit notamment d'interceptions de correspondances légalement et légitimement ordonnées. En application de

³²⁷Droit du net Rubrique Junior : http://www.droitdunet.fr/par_profils/profil.phtml?it=3&type=profil_junior

ces dispositions le principe est simple : il est interdit d'intercepter les correspondances sauf à justifier d'un risque à l'ordre public³²⁸.

Le secret des correspondances est protégé, tant contre les ingérences de l'État que contre les atteintes issues de particulier (ce droit s'applique de la même façon aux communications téléphoniques et aux autres modes de transmission de données, du moment qu'il y a télécommunication). La loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication protège les libertés individuelles en garantissant le secret des correspondances. Seulement deux types d'interception sont légalement possibles: les "interceptions judiciaires" (autorisées par un juge lorsque l'infraction encourue est punie d'une peine d'au moins deux ans de prison) et les "interceptions administratives" (autorisées par une commission administrative pour les questions relevant de la sécurité de l'État)³²⁹.

Les correspondances émises par la voie des télécommunications sont protégées par la loi du 10 juillet 1991. Avant cette date, ce sont les dispositions relatives à la vie privée (notamment l'article 9 du Code Civil) qui fondaient le régime de protection. Aujourd'hui le code Pénal prévoit dans son article 226-15 des sanctions aux atteintes portées au secret des correspondances. Dans son alinéa 2 il se prononce explicitement sur la protection des télécommunications en disposant que : « *Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

2.a". Les messageries instantanées.

La messagerie instantanée dont il est question ici est d'une nature différente à celle des chats ou des forums de discussion. Si dans leur forme ces systèmes semblent similaires, la distinction est à faire au niveau de la sélection des interlocuteurs. Les messageries instantanées se situent dans le prolongement de la messagerie électronique personnelle³³⁰.

³²⁸ Ceci concerne donc sur un réseau scolaire par exemple tous les mails qui circulent sur le réseau de l'école. Le fait de prévoir de telles surveillances dans le règlement intérieur de l'école ne change rien au problème, la seule possibilité serait la divulgation par la personne de son courrier, mais ceci ne peut pas lui être imposé. Tiré du site Clic-Droit.com, site d'actualité et de service dédié au droit de la régulation d'Internet et des nouvelles technologies. Dossier du 30 mars 2004, L'interception des données sur le réseau d'une école.

http://www.clic-droit.com/web/editorial/dossier.php?dossier_id=38

³²⁹ Ibid.

³³⁰ MSN Messenger, Yahoo Messenger,... quasiment tous les fournisseurs d'accès ont désormais cette fonctionnalité qui contribue à créer des petites communautés.

C'est un élément à part entière de la correspondance privée électronique. La correspondance électronique privée et la messagerie électronique sont susceptibles d'avoir la même matière : le carnet d'adresse. Il n'est pas possible de communiquer avec des interlocuteurs autres que ceux prédéterminés dans une liste tirée du carnet d'adresse.

La messagerie instantanée est possible entre deux ou plusieurs personnes par le biais d'une conférence sur le modèle des téléconférences. Ce n'est pas une messagerie totalement spontanée. Le mineur internaute doit inviter un interlocuteur dont il a l'adresse à s'ajouter à sa liste de contacts. Il est nécessaire que cet interlocuteur accepte l'invitation. A partir de là, pour pouvoir communiquer en mode instantané, il faut que les deux interlocuteurs soient connectés au même moment ; dès lors ils peuvent donner libre cours à leur expression.

La liste de contacts est constituée la plupart du temps par des adresses qui figurent déjà dans le carnet d'adresse de la boîte email. Au départ, les listings des messageries instantanées (Messenger) étaient limités dans la mesure où il n'était possible d'échanger qu'avec des personnes ayant le même hébergeur pour leur adresse de messagerie. Pour contourner cette difficulté et éviter tout sectarisme, les mineurs étaient souvent détenteurs de multiples adresses Internet afin de pouvoir communiquer avec des interlocuteurs dépendants de divers hébergeurs. La technologie du Net étant en constante évolution, il est désormais possible de communiquer dans le cadre de messageries instantanées avec tous les interlocuteurs de son carnet d'adresse indépendamment de l'hébergement de sa messagerie électronique. En pratique, cela ne change pas les comportements des jeunes internautes qui continuent à compartimenter leurs interlocuteurs selon leur hébergeur, l'enjeu réside surtout dans les fonctionnalités dont il est possible de faire usage entre des interlocuteurs du même hébergeur³³¹.

Les messageries instantanées étant un prolongement de la correspondance privée, elles peuvent y être assimilées et bénéficier de la même protection. De ce fait, le mineur n'a pas *a priori* à répondre des propos qu'il y tient et qui sont donc couverts par le secret des correspondances sauf nécessité du respect de l'ordre public ce qui suppose une décision légale motivée.

³³¹ Emoticônes, échanges de fichiers photos et autres, utilisation de périphériques tels la Webcam, microphone, etc.

2-b. La communication privée du mineur.

La communication privée du mineur suppose qu'il s'adresse de manière délibérée à une personne déterminée dans le cadre d'une communication non publique. Il ne peut être question de communication privée si quiconque avait la latitude d'interférer sans qu'il n'ait été sollicité par les instigateurs de la communication initiale. Une telle communication peut se faire par le biais de la téléphonie sur Internet ou par la visioconférence possible grâce une webcam.

2.b'. La téléphonie via Internet.

Après un développement fulgurant de l'utilisation d'Internet dans ses applications principales que sont la recherche d'informations sur le Web et le courrier électronique (electronic mail ou plus simplement e-mail), la possibilité est apparue depuis quelques années de faire passer la voix sur le réseau, débouchant ainsi sur la perspective d'un véritable service de téléphonie sur Internet³³².

Internet est un média dont les applications ne cessent de se perfectionner. Il est possible d'avoir des communications vocales via Internet partout dans le monde. Cela nécessite une connexion Internet, mais aussi un minimum de matériel pour permettre la communication tel un microphone. Dès lors la communication est possible de PC à PC.

La téléphonie Internet est un procédé qui permet de substituer la téléphonie conventionnelle par l'utilisation d'un ordinateur et d'Internet. L'ordinateur multimédia remplace le téléphone et Internet est le lien entre les usagers³³³.

Il existe de nouveaux logiciels qui permettent les communications de PC à téléphones³³⁴. Les mineurs (on le dira jamais assez) sont parmi les plus grands utilisateurs d'Internet. Ils sont aussi souvent les premiers à découvrir les nouvelles fonctionnalités du cyberspace. La

³³² Rapport de Jean-Claude Merlin, Avril 1999, *La Téléphonie sur Internet*, Rapport présenté par Jean-Claude Merlin, Ingénieur Général, Rapporteur, avec la collaboration de Pierre Fritz, Ingénieur Christian Malet, Inspecteur général ministère de l'Economie et des Finances et de l'industrie, SEI, Conseil Général des technologies de l'Information (CGTI)

³³³ Site de Richard Vaillancourt, Université de Laval, Service de l'informatique et des télécommunications (SIT), Expérimentation et veille technologique, Téléphonie, vidéophonie et multimédia sur Internet.
<http://www.sit.ulaval.ca/pp/rva/presteleconf/>

³³⁴ Logiciels Skype, Skype est un logiciel gratuit, Skype est un logiciel de téléphonie vocale sur Internet, qui permet de téléphoner de pc vers pc, et de pc vers les téléphones dans le monde entier. MSN et Yahoo Messenger proposent également ce service.

téléphonie par le biais d'Internet représente cet avantage de ne pas générer de surcoût, l'acquittement de l'abonnement pour une connexion Internet suffit. En contre partie il est possible de téléphoner sans crainte de surcoût ; qu'il s'agisse ou non d'un appel longue distance tous les appels se valent. Les communications sur Internet ont l'avantage de réunir l'écrit, le son et l'image qui peuvent coexister simultanément.

2.b". La Webcam.

Au-delà de son rôle de diffuseur d'images, la Webcam est d'abord un moyen de communication électronique qui allie le son et l'image et peut parfois être complété par l'écrit. La Webcam est souvent un matériel de support des autres modes de communication sur le Web. Il a autant sa place dans un espace public³³⁵ ou plutôt dans un contexte public³³⁶ que dans un espace privé. Dans l'hypothèse où la diffusion est destinée à un nombre de personnes déterminées et dans le contexte d'une communication privée, son statut s'aligne sur celui des communications privées.

On a pu voir dans les exposés précédents l'importance croissante que la Webcam prenait dans les relations familiales, notamment entre les enfants et leur parent absent suite à une séparation. Au-delà du contact écrit ou oral, la Webcam contribue à pallier le manque de contacts physiques entre les familles séparées. C'est une alternative, notamment pour les enfants qui ne savent pas encore écrire, et cela permet un contact visuel et oral en simultané³³⁷. Plusieurs droits individuels de l'enfant se trouvent ainsi concernés : son droit à une correspondance privée (on est dans l'hypothèse d'une communication électronique privée filmée) ; son droit à la liberté d'expression, son droit de rester en contact avec son parent absent, etc.

La liberté d'expression du mineur ne peut pas être absolue ; c'est le cas même aux Etats-Unis où le premier amendement de la constitution semble pourtant lui consacrer ce caractère absolu. Des limites sont nécessaires à un minimum d'ordre social sinon ce serait l'anarchie,

³³⁵ Sur le site Doctissimo, dans le forum de discussion, une mère est intervenue pour parler du fait que sa fille de 16 ans s'était déshabillée devant sa Webcam dans un forum de discussion.

<http://forum.doctissimo.fr/psychologie/parents/fille-deshabillee-devant-webcam-sujet-148270-2.htm>

³³⁶ Le mineur peut ajouter son image aux « posts » qu'il fait dans les forums et autres systèmes de communications collectifs. Par ailleurs avec le phénomène des individus qui mettent leur vie privée en ligne on est également dans un contexte public : la vie privée est rendue publique.

³³⁷ Libération, 13-14 janvier 2001, Quand la Toile rapièce les liens familiaux, article préc.

une véritable cacophonie bafouant d'autres droits et libertés individuels. Aux limites de droit commun, il faut rajouter des limites inhérentes au statut particulier du mineur et de l'outil qu'est Internet.

B. Les limites à la liberté d'expression des mineurs.

Contrairement à ce qui a parfois été soutenu ou espéré, l'exercice de la liberté d'expression ne se conçoit pas sans limites sur Internet. La liberté d'expression exercée par un mineur peut au même titre que celle des internautes en général, donner lieu le cas échéant à la mise en cause de sa responsabilité³³⁸.

Une position classique s'inspirant du Premier amendement de la Constitution américaine affirme que la liberté d'expression se régule dans le débat et ne devrait donc pas souffrir d'interventionnisme notamment étatique. Pour d'autres, l'absence de régulation et de réglementation pourrait être source d'atteintes irréparables aux libertés de tous. Le caractère absolu de la liberté d'expression doit se trouver confronté à des limites induites par la nature même des sociétés démocratiques qui se sont bâties sur le respect des libertés d'autrui : c'est la position européenne et française en particulier³³⁹.

1. L'autorégulation de la liberté d'expression sur Internet par le mineur.

L'image ou la parole du mineur ne peut être diffusée sans l'autorisation préalable du ou des titulaires de l'autorité parentale conformément à l'article 99 du code civil et aux règles qui régissent l'autorité parentale. Le seul consentement du mineur capable de discernement demeure insuffisant³⁴⁰. En pratique le respect de ces conditions pour l'exercice de la liberté d'expression du mineur n'est pas facile à mettre en œuvre eu égard à l'instantanéité des relations ayant cours sur Internet ; les contenus d'Internet étant très volatiles, transfrontaliers, intemporels.

³³⁸ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.57.

³³⁹ Isabelle Falque-Pierrotin ; La liberté d'expression dans la société de l'information.

<http://www.foruminternet.org/telechargement/forum/disc-unesco20021115.html>

³⁴⁰ Mise en œuvre de la Convention internationale des droits de l'enfant en France et action du gouvernement en faveur de la situation des dans le monde. IV Libertés et droits civils.

<http://www.social.gouv.fr/hm/actu/convention/4c.htm>

Dès sa création, autant les créateurs que les utilisateurs de la Toile ont misé sur l'autorégulation de la liberté d'expression. L'idée était d'éviter une intrusion réglementaire qui aurait été assimilée à de la censure³⁴¹. Malgré l'évolution de la réglementation sur le cyberspace, la crainte de la censure ressurgit dès lors qu'il est question de réglementation dans et sur le cyberspace. Les anciens comme les nouveaux usagers du cyberspace continuent de rêver à un espace totalement libre ne souffrant aucune limite si ce n'est une régulation « dans le débat »³⁴². Cette position n'est pas uniquement attribuable à la conception américaine. Les pères fondateurs d'Internet avaient un penchant avoué pour cette position. Les internautes sont historiquement hostiles à la censure sous toutes ses formes de la liberté d'expression sur Internet. La seule limitation qu'ils entendent tolérer est celle qui vient de la « communauté des internautes » et qui est définie par eux. Ils entendent « *séparer le bon grain de l'ivraie* » par l'éthique dont tout internaute devrait faire preuve dans le cyberspace.

S'agissant du statut particulier du mineur, aucun texte mis à part la Convention internationale de droits de l'enfant de 1993 en son article 13, ne consacre expressément la liberté d'expression du mineur. On a déduit la liberté d'expression du mineur de la liberté d'expression de l'individu en droit commun. Des aménagements restent nécessaires quant à l'exercice de la liberté d'expression du mineur dans le cyberspace. La liberté d'expression du mineur dans le cyberspace bien que réelle, souffre de limites issues du droit commun et du droit spécifique régissant le statut des mineurs. Par exemple, même au nom de sa liberté d'expression le mineur n'est pas autorisé à consulter des sites notoirement pornographiques, ou ayant un contenu réservé aux adultes. Il n'a pas non plus le droit de faire usage de sa liberté d'expression pour nuire à autrui.

Cette autorégulation ou plutôt autocensure du mineur suppose qu'il maîtrise d'une part les règles de bonne conduite posées par la "Netiquette", mais aussi et surtout qu'il soit un internaute « citoyen », qu'il se dispense de propos licencieux, injurieux, diffamatoires. Comment attendre une telle maîtrise de soi des mineurs là où même les adultes dans leur majorité ne présentent pas cette qualité de probité. Cela suppose un internaute mineur mais

³⁴¹ « Beaucoup d'internautes affirment un attachement très fort à la liberté d'expression érigées en principe fondateur. Internet est vécu comme un espace de liberté d'expression et d'échange où toute velléité d'intervention des Etats est à regarder avec méfiance » ; Christian Paul, Rapport au Premier ministre, Du droit et des libertés sur Internet, Collection des rapports officiels, La documentation française 2001, p.33.

³⁴² Isabelle Falque-Pierrotin, La liberté d'expression dans la société de l'information, préc.

conscient de ses droits et devoirs envers autrui de même que de ses responsabilités. Dans la « vie réelle » nul ne prétend laisser une autonomie au mineur telle qu'il puisse s'autocensurer et prendre la pleine mesure de ses actes et des conséquences qui en découlent, c'est pour cette raison qu'il existe des règles pour protéger les mineurs d'autrui et d'eux-mêmes. « La vie virtuelle » ne saurait être soumise à des règles différentes, ce d'autant plus que les risques bien que différents sont aussi grands et lourds de conséquences. Même si « nul n'est sensé ignoré la loi », les mineurs du fait de leur vulnérabilité intrinsèque ne peuvent être tenus aux mêmes devoirs qu'un adulte ; en outre les mineurs n'ont pas la même maturité même à âge égal.

Il y a des internautes très jeunes³⁴³ qui ne disposent pas encore d'une capacité propre à leur conférer un bon discernement dans la « vie réelle » et *a fortiori* sur le Web. Toutefois la capacité de discernement ne fait pas tout, certains mineurs en disposent mais n'en demeurent pas moins vulnérables sur la Toile. Ils ne maîtrisent pas tous les arcanes des droits et devoirs qui doivent s'appliquer à eux sur la Toile. Dans un monde virtuel où ils sont confrontés à des internautes de toutes natures, les mineurs ne sont pas toujours bien armés devant la perversité de certains de leurs interlocuteurs.

Il serait possible d'envisager un autre mode d'autocensure : la modération mutuelle dans les forums et autres chats. Dans cette hypothèse, l'autonomisation de la responsabilité est encore trop grande pour le mineur, qui n'en mesure pas forcément tous les enjeux. Il est indispensable que le mineur soit accompagné, ou du moins assisté dans sa liberté d'expression par un adulte.

1.a. La Netiquette.

La Netiquette est un des outils phares de l'autorégulation. Elle n'a aucune force juridique mais plutôt une valeur morale. La netiquette a été initiée par la branche universitaire des fondateurs d'Internet « à l'âge d'or d'Internet » quand n'était encore concerné qu'un nombre limité de personnes³⁴⁴. La netiquette a été pensée comme une sorte de code de bienséance³⁴⁵. Les services de discussion par forum sont principalement visés par ce type d'autorégulation

³⁴³ On estime qu'un mineur se met à surfer sur la Toile vers six ans.

³⁴⁴ Estelle de Marco, Le droit pénal applicable sur Internet, DEA Informatique et Droit sous la direction du Professeur Michel Vivant, Université de Montpellier 1 : www.juriscom.net/uni/mem/06/crim01.htm

³⁴⁵ M.C. Marrie, Internet, la loi et l'éthique, MédiasPouvoirs, n°4, 1998, p.153.

ou d'autocensure. La netiquette se présente sous la forme de dix commandements très larges, dont le contenu a une forte connotation morale et, ne fait pas l'objet en l'état actuel du droit de sanctions juridiques. Elle peut néanmoins acquérir une valeur juridique lorsqu'elle est intégrée dans des contrats, comme faisant partie des obligations entre les cocontractants³⁴⁶.

La valeur morale de la netiquette se dilue au fil des années, de l'évolution d'Internet et de la croissance exponentielle du nombre d'internautes. Il est plus facile de fixer des règles communes dans un groupe restreint partageant de surcroît une communauté d'intérêt, que d'uniformiser des règles de bienséance à des catégories disparates d'internautes. Il faudrait que tous les internautes comprennent et reconnaissent comme leurs les règles préconisées par la netiquette.

A ce stade, intervient une difficulté supplémentaire liée à la situation juridique du mineur. Le mineur est une personne vulnérable, bien qu'il faille admettre qu'il maîtrise souvent mieux que les adultes l'outil informatique et Internet en particulier. Sa connaissance de cet outil couvre indifféremment l'aspect technique du fonctionnement du matériel informatique et la maîtrise des technologies que suppose l'utilisation du Web. Le mineur comme toute personne censée connaître la loi doit savoir ce qui est prohibé. En l'espèce il devrait connaître quelles sont les limites de sa propre liberté d'expression dans le cyberspace. La liberté d'expression du mineur s'exerce selon des schémas différents dans le cyberspace. Elle peut s'exprimer dans un cadre unilatéral ou bilatéral. Dans un cadre unilatéral, le mineur diffuse son expression (quel qu'en soit la forme : écrite, orale, etc.) vers autrui. Il n'attend pas *a priori* de réponse. Par contre dans le cadre d'une expression bilatérale, l'interactivité avec autrui est au centre de sa libre expression. Il s'exprime par rapport à un autre internaute. Il devrait donc savoir maîtriser sa liberté d'expression et savoir canaliser ou limiter celle des autres. On entre là dans une dimension juridique et relationnelle que tous les mineurs ne maîtrisent vraisemblablement pas. Il faudrait que le mineur connaisse et comprenne toutes les implications juridiques de la liberté d'expression dans le cyberspace. Par ailleurs même les internautes libertaires ont dû admettre que le cyberspace ne devait pas être un espace de non droit, et que la seule autorégulation ne pouvait venir à bout de la cybercriminalité découlant de la liberté d'expression.

³⁴⁶ Estelle de Marco, Le droit pénal applicable sur Internet, préc., p.130.

Lorsque le mineur se sent dépassé par le mode ou le contenu de l'expression de son interlocuteur, il lui reste la possibilité d'en référer à un adulte, un intermédiaire du cyberspace ou à une autorité légale compétente.

1.b. La dénonciation ou notification de contenus illicites.

Lorsqu'au cours de sa navigation un internaute mineur est confronté à des propos inconvenants ou à des contenus illicites³⁴⁷, il a la possibilité de dénoncer le site ou la page Web incriminée. La forme du contenu n'est pas précisée ; on peut en déduire que le contenu peut être visuel, sonore ou écrit.

Le principe de la dénonciation des contenus est bien admis en Europe. Il existe un accord en la matière en Belgique depuis 1999³⁴⁸. En France c'est la loi 2004-575 du 21 juin 2004 qui régleme cette question. En pratique ce procédé existait préalablement à cette loi. Il avait été mis en place à l'initiative de l'Association des fournisseurs d'accès (AFA)³⁴⁹.

En plus du dispositif de dénonciation mis en place en 1998 par l'Association des Fournisseurs d'Accès, le gouvernement français a prévu par un décret 2000-405 du 15 mai 2000, et un arrêté du 8 novembre 2001, de permettre aux internautes majeurs ou mineurs accédant à des contenus illicites, de les signaler directement auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Dans le site prévu à cet effet³⁵⁰, il est proposé un imprimé de signalement de sites ou autres services en ligne (email, newsgroup, chat) ayant permis la diffusion d'images de mineur à caractère pornographique ou de messages favorisant la corruption des mineurs. Il faut fournir le

³⁴⁷ La loi 2004-575 du 21 juin 2004 préconise la dénonciation en cas d'apologie de crimes contre l'humanité, d'incitation à la haine raciale et de pornographie infantine.

³⁴⁸ Internet Service Provider Association (ISPA) a signé en Belgique un accord de collaboration avec les ministres de la justice et des télécommunications le 25 mai 1999 ; Voir sur le site Droit et Nouvelles technologies, Etienne Wery ; Contenus illicites : la Belgique sur la voie de l'auto réglementation, 31 mai 1999. http://www.droit-technologie.org/1_2.asp?actu_id=179

³⁴⁹ En novembre 1998 l'Association des Fournisseurs d'Accès (AFA) a créé un premier point de contact en France ; il en existait déjà d'autres en Europe. Les points de contact doivent permettre une information sur les textes pénaux applicables à la cybercriminalité, notamment s'agissant de pédophilie et d'incitation à la haine raciale. Ils permettent d'identifier les sites illicites, l'interlocuteur à même de recevoir la réclamation et l'autorité devant laquelle on peut porter plainte. Ils permettent enfin de transmettre les réclamations auprès d'un fournisseur d'accès, du service membre d'un réseau ou à un autre point de contact membre du réseau Internet INHOPE (association de fournisseur de lignes d'assistance sur Internet), vu dans le site Le Forum des droits sur Internet-Fiches pratiques, Assurer la protection de l'enfant sur Internet, 05 septembre 2001.

³⁵⁰ <http://www.internet.mineurs.gouv.fr>

maximum d'information dans le formulaire de dénonciation : adresse Internet de la page Web concernée (forum de discussion, chat, courriel, nature du contenu inconvenant constaté, etc.).

Selon l'accord signé en Belgique, toute personne peut dénoncer à son fournisseur d'accès (ISP : Internet Service Provider), ou directement au point de contact, un contenu qu'il estime illicite. Lorsque la dénonciation est faite au fournisseur d'accès, il doit la transmettre au point de contact. Ce dernier est alors chargé de faire un tri avant de transmettre les contenus illégaux au parquet, parallèlement il doit signaler au dénonciateur et au fournisseur d'accès l'existence du contenu illicite. Les fournisseurs d'accès doivent prendre les mesures nécessaires pour faire cesser cette illicéité. Sont exclus de cet accord les communications privées via Internet, les courriers électroniques, les chats privés et les sites à accès limité.

La loi de 2004 fait peser une obligation sur les fournisseurs d'accès et d'hébergement : celle de mettre en place un dispositif permettant à toute personne de signaler un contenu illicite.

Il y a trois étapes dans la notification :

- l'envoi d'une lettre recommandée avec accusé de réception à l'éditeur du contenu illicite ou une justification de ce que l'auteur ou l'éditeur n'a pas pu être contacté,
- l'impression du formulaire de contenu illicite,
- l'envoi de la correspondance faite à l'éditeur et/ou le justificatif de non distribution plus le formulaire dûment rempli.

Une pratique se généralise auprès des fournisseurs d'accès, créateurs de sites et de pages Web : ces derniers prévoient désormais de manière quasi automatique la possibilité de dénoncer un contenu illicite qui aurait été répertorié dans leurs pages. Dans les chats et les forums, les mineurs peuvent notifier en temps réels les propos ou messages inconvenants aux modérateurs ou aux animateurs³⁵¹.

³⁵¹ Pour pallier les dénonciations arbitraires et calomnieuses, il était nécessaire que le législateur pose des gardes fous. Toute fausse dénonciation est sanctionnée aux articles 226-10 et 226-11 du code pénal.

2. L'intervention des intermédiaires dans la liberté d'expression.

Peu de mineurs sont à même de s'autocensurer ; il revient à leurs parents ou tuteurs légaux, et aux intermédiaires de s'assurer que la liberté d'expression du mineur n'est pas pervertie dans son exercice. Les intermédiaires qui sont confrontés aux manifestations publiques de la liberté d'expression des mineurs dans le cyberspace sont : l'organisateur, le médiateur des forums et chats.

Il existe un type de filtre parental dont les paramètres de sécurité sont modulables, l'objectif est conformément à des critères prédéfinis d'empêcher le mineur d'accéder à certains contenus, de communiquer certaines informations au cours de sa navigation. Ce système trouve à s'appliquer dans les sites et pages personnels, dans les forums de discussion et les chats, et lors de toute recherche par mots clés du mineur sur le Web.

S'agissant des intermédiaires, tous ne peuvent avoir la même promptitude, ni les mêmes capacités de contrôle de la liberté d'expression des mineurs sur Internet. Etant donné que nous allons analyser la responsabilité des intermédiaires dans les développements prochains, nous allons ici ne nous intéresser qu'aux organisateurs de forums de discussions dédiés aux mineurs. Ils sont ceux qui sont confrontés le plus directement à la liberté d'expression des mineurs.

Dans les forums de discussion, il existe trois catégories d'acteurs : les fournisseurs de solution, les organisateurs proprement dit (le commanditaire, le modérateur et le ou les animateurs), et enfin les utilisateurs (les lecteurs et les contributeurs)³⁵². Pour limiter ou tout du moins encadrer la liberté d'expression des mineurs dans les forums il y a trois axes.

³⁵² Le forum des droits sur Internet, Rapport d'activité 2003, Quelle responsabilité pour les organisateurs de forums de discussion sur le Web ?, La documentation française 2004, p.235-236.-. Le fournisseur de solution de forum de discussion est l'hébergeur, le commanditaire est l'opérateur. Un modérateur (ou une modératrice) est un internaute dont le rôle est d'animer et de modérer un forum, en effaçant les messages d'insulte, à caractère raciste, hors sujet, bref tous les messages n'ayant pas leur place dans un forum de discussion sur le web., les animateurs font la même chose que le modérateur mais on les retrouve plus souvent dans les chats, le lecteur contrairement au contributeur ne participe pas aux débats. <http://fr.wikipedia.org/wiki/Animateur>

2.a. La charte de participation.

Elle suppose une éthique de conduite à laquelle il faut se conformer sous peine d'exclusion. En règle générale et préalablement à l'accès à un forum de discussion ou un chat, il faut adhérer à une charte de participation. Il s'agit en quelque sorte d'un mode d'emploi qui prescrit et proscriit certains comportements en ligne. La charte indique que le sujet de discussion doit être respecté, précise les règles de bonne conduite à respecter. Les chartes se réfèrent souvent à la Netiquette sans plus de précision³⁵³. L'adhésion permet à l'internaute de s'enregistrer avec son identité ou son adresse Internet, il s'attribue alors une identité (un pseudonyme) et un mot de passe qu'il utilisera dans les forums ou les chats. Son enregistrement sous son identité réelle ou son adresse email est nécessaire pour pouvoir engager sa responsabilité sur des propos litigieux qu'il pourrait tenir. Le fournisseur de solution et les organisateurs doivent posséder des informations pouvant permettre l'engagement de sa responsabilité. La charte doit donc clairement énoncer aux internautes qu'ils engagent leur responsabilité pour leurs propos et leurs agissements en ligne. La charte doit enfin préciser quel type de modération est pratiqué dans le forum ou le chat.

2.b. La modération.

C'est la méthode de régulation de la liberté d'expression ; dans les forums elle incombe au modérateur, et dans les chats elle revient à un ou plusieurs animateurs. Elle consiste en la modification voire à la suppression de tout ou partie du message ne respectant pas les règles posées par la charte³⁵⁴. Il existe deux types de modération *a priori* et *a posteriori*.

2.b'. La modération a priori.

Il s'agit de l'intervention préalable à la parution du message. Cela entraîne un délai entre le moment où le mineur poste son message et le moment où ce dernier est accessible au public. C'est une activité lourde qui nécessite plusieurs modérateurs et modifie la charge de la

³⁵³ Un auteur Michel Elie a fait remarquer la difficulté que posait cette référence évasive à la Netiquette. Les organisateurs des forums partent du postulat qu'elle est connue de tous, ce qui est loin d'être le cas notamment pour les mineurs. Par ailleurs, on ne sait plus précisément à quoi la Netiquette fait référence ce, d'autant plus qu'une multitude de textes sont définis sous cette dénomination, des règles parfois différentes et plus ou moins adapté au public auquel on s'adresse. Il faudrait donc déterminer un texte de référence unique largement enseigné et diffusé et auquel les différentes chartes puissent se référer par le biais d'un lien explicite ; Le Forum des droits sur Internet, Rapport d'activité 2003, La documentation française 2004, p.243.-. Quelle responsabilité pour les organisateurs de forums de discussion sur le Web ?, Recommandation du 8 juillet 2003

³⁵⁴ Le Forum des droits d'Internet, préc. p.244; il s'agit au premier rang, du non respect du sujet de la discussion, le respect de certaines civilités et même des règles de droit.

responsabilité des contenus qui passe de l'auteur au modérateur et au commanditaire³⁵⁵. La liberté d'expression est livrée à l'arbitraire du modérateur sur qui aucun contrôle n'est exercé afin de vérifier une éventuelle violation du droit du mineur à sa libre expression. Ce type de modération est plus aisément réalisable dans les forums de discussion que dans les chats ou la messagerie est par définition instantanée.

2.b". La modération a posteriori.

Dans cette hypothèse, le modérateur ou l'animateur peut intervenir spontanément pour retirer un contenu préjudiciable. Il peut intervenir à la demande d'un utilisateur. La modération peut être systématique par un contrôle régulier de tous les contenus mis en ligne, ou ponctuelle c'est-à-dire sur demande. Le risque est de laisser passer des messages préjudiciables aux échanges.

Dans les deux cas les organisateurs doivent faire une gestion précontentieuse des litiges.

2.c. La gestion des litiges par les organisateurs.

Cette gestion relève pour l'essentiel du travail de modération étudié supra. Modification, suppression des contenus, avertissement puis exclusion de l'internaute fautif, et en dernier recours fourniture aux autorités judiciaires des données permettant d'identifier et d'incriminer le contrevenant.

Comme on a déjà pu le noter, peu de domaines font l'objet d'un traitement uniforme dans le Cyberespace et la liberté d'expression ne fait pas exception à la règle. L'étendue de la liberté d'expression en général et du mineur en particulier est tributaire des courants politiques et culturels des pays dans lesquels elle s'exerce. Traditionnellement, on présente les deux positions contradictoires que sont les positions européenne et américaine comme représentatives des deux courants principaux dans le monde. Ce serait compter sans les myriades de courants pas toujours très visibles qui émaillent le cyberespace. Il faudrait rajouter un courant absolutiste : il regroupe pêle-mêle les pays totalitaires, les régimes dictatoriaux où la liberté d'expression et les droits individuels en particulier ne sont pas encouragés à s'épanouir, ou un Internet peu encouragé est placé sous "très haute

³⁵⁵ Dossier du forum des droits d'Internet du 18 juillet 2002, Les responsabilités liées à l'activité des forums de discussion ; Légipresse n°194 septembre 2002.IV.75, Foruminternet.org
<http://www.foruminternet.org/publications/lire.phtml?id=358>

surveillance³⁵⁶. Ces pays n'ont pas pour autant une manière uniforme de traiter la liberté d'expression, leur point commun réside dans la similitude de leur organisation politique.

La liberté d'expression connaît également une limitation logistique. Certains pays, notamment ceux dit en voie de développement, du fait de leurs insuffisances logistiques, ne peuvent fournir d'accès qu'à un nombre très limité de leur population. Les connexions à domicile sont très restreintes pour des raisons tant techniques qu'économiques. L'accès des mineurs et par conséquent l'exercice de leur liberté d'expression sur la Toile s'en trouve réduite à une portion congrue. Reste le mode de connexion le plus répandu dans ces pays : les connexions dans les cybercafés qui par des considérations économiques excluent une majorité de mineurs de son système.

La liberté d'expression du mineur suppose qu'il soit auteur de contenus sur Internet. Le droit d'auteur est un droit fondamental de la personne, qui est souvent remis en question sur la Toile.

§ 2. La liberté créatrice du mineur : le droit d'auteur du mineur dans le cyberspace.

Conformément au code de propriété intellectuelle, le droit d'auteur est un droit « *conféré à l'auteur d'une œuvre littéraire et artistique de nature pécuniaire et morale* »³⁵⁷. Le mineur au même titre que tous, peut revendiquer ce droit et les protections qui en découlent. Il va de soi que la diffusion de son œuvre doit être soumise à son autorisation, et/ou à celle de ses parents ou tuteurs légaux.

³⁵⁶ On peut citer la Chine

³⁵⁷ Art. L.111-1 et s., L.121-1 et s. Définition donnée par le Dictionnaire du vocabulaire juridique ; sous la direction de Rémy Cabrillac, Jurisclasseur, Objectif Droit, Litec 2003.- Le droit d'auteur fait partie du patrimoine de celui-ci. Juridiquement, il forme une catégorie autonome de droits patrimoniaux, car il n'est ni un droit réel, ni un droit de créance. L'auteur, titulaire de droits patrimoniaux et d'un droit moral, ne les exerce pas contre un débiteur, ni sur une chose corporelle, c'est-à-dire matérielle, mais sur un objet incorporel (immatériel) ; par exemple, une œuvre de l'esprit. fr.wikipedia.org/wiki/Droit_d'auteur

Le droit d'auteur consiste en la protection patrimoniale et morale gratuite des œuvres de l'esprit. www.cnrs.fr/SDV/Dept/glossaireindus.html

Ensemble de tous les droits patrimoniaux et moraux que détient le premier titulaire du droit d'auteur sur le texte. www.aqad.qc.ca/lexique.asp

Droit exclusif d'exploitation. Le titulaire du droit d'auteur est la seule partie autorisée à copier l'œuvre visée ou à permettre à une autre partie de le faire. Ce droit comprend généralement le droit exclusif de publier une œuvre, de la produire, de la reproduire et de l'exécuter en public. www.geoconnexions.org/ICDG.cfm/fuseaction/policySupporting.seeFile/id/95/gcs.cfm

L'apparition du droit d'auteur fait suite avec un certain décalage à la création de l'imprimerie. Sa mise en place concernera dans un premier temps les œuvres littéraires car, c'était là que la reproduction et la contrefaçon étaient possibles. Des privilèges furent accordés aux libraires imprimeurs dans le but de les protéger de la concurrence d'autres professionnels plutôt que de récompenser leur travail de création³⁵⁸. Sous sa forme moderne, la protection des œuvres de l'esprit naît avec la législation révolutionnaire qui régira le système jusqu'à la loi de 1957³⁵⁹.

L'expression droit d'auteur sera utilisée pour la première fois en 1838 par A.C. Renourard, à l'occasion de la publication d'un traité sur le sujet³⁶⁰. Dans les pays anglo-saxons plutôt que l'expression "*author rights*" traduction littérale de droit d'auteur, on utilise l'expression *copyright*. Pour qu'une œuvre soit protégée, il suffit qu'elle soit originale dans sa forme d'expression ; il n'est pas nécessaire qu'elle soit nouvelle (le brevet se charge de protéger les premiers inventeurs). Le droit d'auteur protège l'expression des idées et non les idées elles mêmes³⁶¹.

La propriété intellectuelle a fait l'objet d'un Code en France en 1992 : on a collationné tous les textes existants en les ordonnant en chapitres pour former le Code de la Propriété Intellectuelle. Ce code comprend deux parties : la Propriété Littéraire et Artistique d'une part et la Propriété Industrielle d'autre part. Il est applicable aux actes effectués sur le réseau Internet. Il en résulte que nul n'a le droit de diffuser sur le réseau un document protégé par le droit d'auteur sans l'autorisation préalable de l'auteur, et dans certaines hypothèses de l'éditeur. Nul n'a le droit de modifier un document, de retoucher une photographie, de la reproduire ensuite.

Les droits d'auteur doivent être étudiés à plusieurs niveaux. Cette étude suppose que l'on apporte une réponse à un certain nombre de questions se posant lors de l'exercice des droits d'auteurs dans le cyberspace :

- qui en est titulaire et selon quels critères ?
- quel type d'œuvre peut bénéficier de sa protection sur Internet ?

³⁵⁸ Joëlle Farchy, Internet et le droit d'auteur. La culture Napster ; CNRS Communication 2003, p.24.

³⁵⁹ L'assemblée constituante consacre le « droit de représentation » par les décrets-lois des 13 et 19 janvier 1791 relatifs aux spectacles. Les décrets des 19 et 24 juillet 1793 instituent les « droits exclusifs de reproduction » relatifs aux « droits de la propriété des auteurs d'écrits en tout genre, des compositeurs de musique, des peintres et des dessinateurs ». L'expression droit d'auteur n'apparaît encore nulle part ; Joëlle Farchy, Internet et le droit d'auteur, préc., p.24.

³⁶⁰ Ibid.

³⁶¹ Ibid., p.28.

- dans le fond quelle est la valeur intrinsèque de la liberté d'expression du mineur ?
- de quels types de protection ses œuvres diffusées dans le cyberspace peuvent bénéficier ?

A. Les droits d'auteur du mineur dans la forme.

La question que l'on peut se poser au sujet des droits d'auteur du mineur est la suivante : doit-on se référer au droit commun régissant le droit d'auteur ou faut-il envisager un traitement spécifique qui prendrait en compte les spécificités respectives des statuts juridiques du mineur et d'Internet ?

1. Les titulaires des droits d'auteur.

Selon la définition consacrée, le droit d'auteur est un droit « *conféré à l'auteur d'une œuvre littéraire et artistique de nature pécuniaire et morale* ». Nulle précision n'est faite quant à la catégorie d'individu pouvant prétendre à la qualité d'auteur. Aucune catégorie d'individu n'en est pour autant exclue ; on en conclut logiquement que le mineur comme tous, est fondé à recevoir la qualité d'auteur avec les droits qui en découlent dès lors qu'il réunit les conditions requises.

La loi de 1957 régissant le droit d'auteur sera complétée par celle du 3 juillet 1985. Cette dernière loi va créer les droits voisins du droit d'auteur. Ces droits voisins différencient les auteurs des titulaires des droits d'auteurs. Dès lors, les titulaires de ces nouveaux droits peuvent être des intermédiaires d'Internet comme l'énonce la loi de 1985.

1-a. L'auteur.

L'auteur est la « *personne sous le nom de laquelle une œuvre est divulguée* » conformément à l'article L.113-1 du CPI³⁶² ; c'est le créateur de l'œuvre, celui dont la personnalité s'exprime dans l'œuvre.

On pourrait en déduire que l'auteur ne peut être qu'une personne physique et, qu'en revanche, une personne morale (société, association, administration...) ne peut prétendre à cette qualité, tout au moins à titre initial (sauf œuvre de collaboration).

³⁶² Dictionnaire de vocabulaire juridique, sous la direction de Rémy Cabrillac, préc.

Une œuvre de collaboration sous certaines conditions³⁶³ voit reconnaître aux collaborateurs de l'œuvre la qualité de coauteurs. S'agissant de l'œuvre composite³⁶⁴ l'article L.113-2 du CPI reconnaît comme auteur celui qui l'a réalisée, et lui en attribue la propriété. Vient ensuite l'œuvre collective³⁶⁵ régie par l'article L.113-2 alinéa 3 ; elle n'appartient qu'à celui qui dirige l'équipe chargée de la réaliser. Les membres de l'équipe ne disposent pas de la qualité d'auteur³⁶⁶. L'œuvre collective a ceci de particulier, qu'elle laisse la possibilité d'attribuer la qualité d'auteur à une personne morale.

L'auteur est également entendu comme le titulaire de droits patrimoniaux et du droit moral sur une œuvre de l'esprit, un objet incorporel qui n'est pas une chose corporelle³⁶⁷ (c'est-à-dire matérielle). Il n'exerce pas ses droits contre un débiteur. Quand il s'agit d'un droit intellectuel qui porte sur une création de l'esprit, il est attaché à la personne de son auteur. Le droit d'auteur donne à son titulaire un droit exclusif d'exploitation sur son œuvre³⁶⁸.

Comment insérer une définition d'auteur qui s'adapte au statut particulier du mineur ? Le mineur bien qu'il dispose de droits inhérents à sa personne a besoin pour exercer ses droits d'auteur de la caution de ses parents ou tuteurs légaux.

Comment identifier l'auteur ? C'est l'une des principales difficultés que l'on rencontre lorsque l'on veut exploiter une œuvre en l'intégrant sur un site Web. En principe l'auteur, personne physique est le seul titulaire des droits d'auteur au terme de l'article L.111-1 du code de propriété intellectuelle. En matière d'œuvres collectives, la propriété de l'œuvre appartient à la personne physique ou morale sous le nom de laquelle elle a été divulguée - art. L. 113-5 du CPI³⁶⁹.

³⁶³ L'œuvre de collaboration est faite par deux ou plusieurs personnes physiques. Il faut que chaque collaborateur ait procédé à une réalisation de forme à l'occasion d'une réalisation commune et concertée.

³⁶⁴ L'œuvre composite est celle qui est faite en incluant une œuvre préexistante mais sans collaboration de l'auteur de l'œuvre initiale.

³⁶⁵ L'œuvre collective suppose quatre conditions : 1) elle doit être réalisée à l'initiative ou sous la direction d'un entrepreneur (personne physique ou morale), 2) celui-ci doit l'édition, le diffuser ou le publier sous son nom, 3) l'œuvre doit résulter de la fusion des diverses contributions, 4) il doit être impossible d'identifier l'apport individuel de chaque contributeur.

³⁶⁶ Le Chêne et le Gland, Site de Sébastien Canevet (Maître de Conférence en droit privé) et consacré au droit d'Internet, jurisprudence, doctrine, actualité législative ; Qui est l'auteur d'une œuvre ?, 18 janvier 2005, Sébastien Canevet : www.canevet.org/article.php3?id_article=24

³⁶⁷ Ecrits, musique, photographie, ...

³⁶⁸ http://fr.wikipedia.org/wiki/Droit_d%27auteur

³⁶⁹ Droit d'auteur et Multimédia, Le droit d'auteur, dossier réalisé par Pierre Perez pour le site Educnet. <http://www.educnet.education.fr/juri/auteur1.htm>

Les caractéristiques énoncées dans le présent paragraphe correspondent plutôt aux œuvres littéraires.

Le cyberspace a ceci de particulier que, grâce au développement des sites et autres pages personnels ; quiconque peut devenir créateur de contenus en ligne. Les webzines, les blogs sont des supports qui favorisent l'apparition d'auteurs directement sur le Web. C'est ainsi que fleurissent des journalistes, écrivains, poètes, paroliers, musiciens, photographes et tout type d'auteurs³⁷⁰ que l'ont englobent sous l'appellation générique d'auteurs mais qui n'en sont pas tous au sens puriste du terme mais, plutôt des créateurs quoiqu'ils bénéficient des mêmes droits.

1-b. Les créateurs.

« *L'auteur, c'est le créateur de l'œuvre* »³⁷¹.

La loi de 1985, en créant les droits voisins du droit d'auteur, a étendu la catégorie des auteurs et y a inclus les créateurs. Ils bénéficient des mêmes droits que les auteurs. Les droits connexes³⁷² se distinguent du droit d'auteur en ce qu'ils appartiennent à des titulaires considérés comme des intermédiaires dans la production, l'enregistrement ou la diffusion des œuvres. Le lien avec le droit d'auteur existe du fait que les trois catégories de titulaires de droits connexes fonctionnent comme des auxiliaires dans le processus de création intellectuelle en prêtant leur assistance aux auteurs des œuvres pour la communication de celles-ci au public³⁷³.

L'expression « droit d'auteur » est aujourd'hui ambiguë, dans la mesure où ce droit ne se confond plus exclusivement avec le droit des auteurs. Il s'agit du droit des créateurs. Il faut entendre par créateurs, les écrivains, traducteurs, journalistes, pigistes, auteurs dramatiques, scénaristes et dialoguistes (radio-tv-ciné), réalisateurs paroliers, compositeurs, artistes plasticiens, etc.³⁷⁴

³⁷⁰ Joëlle Farchy, Internet et le droit d'auteur. La culture Napster, CNRS communications, CNRS éditions 2003, p.116-117.

³⁷¹ Sébastien Canevet, Qui est l'auteur d'une œuvre ?, article préc.

³⁷² Ils appartiennent aux artistes interprètes, aux producteurs de phonogramme, aux organismes de radiodiffusion en rapport avec leurs interprétations ou exécutions, leur phonogramme et leurs émissions de radiodiffusion.

<http://www.wipo.int/copyright>

³⁷³ <http://www.wipo.int/copyright>

³⁷⁴ Joëlle Farchy, Internet et le droit d'auteur, préc., p.30.

La diversité de la création et des modes de création a permis de réaliser que l'utilisation du terme d'auteur pouvait se révéler assez restrictive.

2. Les objets du droit d'auteur.

L'avènement et l'évolution des technologies numériques ont généré des contenus si diversifiés que très tôt, s'est posée la question de la protection juridique qu'il convenait de leur affecter. La numérisation d'œuvres matérielles (textes, musique, photographie, etc.) est une des grandes caractéristiques introduite par les nouvelles technologies. Il s'agit d'œuvres matérielles bénéficiant d'une protection du droit d'auteur conformément au droit commun. Ces œuvres nées dans le "monde réel", connaissent avec la technologie numérique une deuxième vie dans le "monde virtuel" grâce aux perspectives de diffusion que leur confère la numérisation. Ces nouvelles technologies ont consacré un nouveau type d'œuvre propre au cyberspace qui pour autant reste réglementé par le droit d'auteur : les œuvres numériques ou multimédia.

2-a. Les supports numérisés.

Il y a encore quelques années, la numérisation n'était à la portée que d'un nombre limité de personnes. La sélection se faisait sur deux critères :

- le critère économique car le coût des appareils de numérisation était prohibitif pour la majorité ;
- le critère technique car la maîtrise de la technologie de ces appareils de numérisation n'était pas accessible à tous.

L'accessibilité aux technologies de numérisation s'est considérablement simplifiée au fil des années. Tout le monde peut devenir éditeur et diffuseur de contenus informationnels et culturels par le biais de la numérisation. La copie est aisée, rapide, de bonne qualité et sa diffusion bénéficie d'une couverture planétaire et d'une audience illimitée³⁷⁵ grâce à Internet. Grâce à la numérisation et à une connexion Internet, il est possible de diffuser ses photographies, vidéo dans le cyberspace.

³⁷⁵ Séverine Dusollier (chercheur au CRID) du 7 mai 2001, Internet et droit d'auteur.
<http://www.droit-technologie.org>

Les mineurs, comme souvent en matière de maîtrise de nouvelles technologies ont été parmi les premiers à assimiler et à utiliser ces nouvelles techniques de numérisation. Ils ont très vite saisi le potentiel d'enrichissement de leur navigation dont lesdites techniques de numérisation étaient porteuses. La numérisation d'œuvres (les leurs ou celles d'autrui) leur est devenue banale, dans leurs activités habituelles dans le cyberspace. Ces œuvres (photographies, textes, musiques³⁷⁶, etc.) qu'ils numérisent, servent pour la plupart à alimenter leurs pages et sites personnels ; elles sont également transformées en fichiers qu'ils s'échangent par courriers électroniques et messagerie instantanée ou qu'ils partagent par le biais de bases de données fonctionnant sur le mode Peer to Peer³⁷⁷. Le droit d'auteur des mineurs en la matière ne présente pas de spécificités telles, qu'il soit nécessaire de mettre en œuvre une protection particulière de ce dernier.

Les œuvres et prestations circulant dans le cyberspace le sont le plus souvent sous forme digitale ou numérique. Ces œuvres de nature audiovisuelle, musicale, écrite, ne sont plus uniquement sous la forme analogique. Cette confusion des supports est une mutation importante de la société de l'information et est susceptible de bouleverser la matière du droit d'auteur et des droits voisins qui raisonnent en général selon une typologie précise des œuvres³⁷⁸. Le Conseil d'Etat a entériné l'application du droit d'auteur aux œuvres en lignes. Il a considéré qu'il n'était pas « *nécessaire de créer un droit spécifique de transmission numérique, de distribution numérique ou de mise à disposition du public sur le réseau, comme cela paraît envisagé dans certains pays comme les Etats-Unis ou le Japon* »³⁷⁹.

Pour pouvoir intégrer dans un site Web des œuvres numérisées, quelle qu'en soit la nature (photographie, tableau, poème, texte, chanson, etc.), il est nécessaire qu'elles aient été

³⁷⁶ La musique est numérisée sous la forme de MP3 qui est un format de compression numérique qui permet que les musiques circulent sur le Web avec la facilité d'un texte, Séverine Dusollier, préc.

³⁷⁷ Le terme poste-à-poste est la traduction (initialement adoptée au Canada) de l'anglais peer-to-peer, laquelle est souvent abrégée P2P. On peut aussi traduire par « pair à pair » ou « égal à égal ». fr.wikipedia.org/wiki/Peer_to_peer.

Il s'agit d'une forme particulière de réseau dans laquelle n'y a pas de serveur mais un ensemble de machines connectées entre-elles par des câbles dans un même lieu. La gestion de ce réseau est assurée par des pilotes et utilitaires qui sont ajoutés au système d'exploitation. Chaque ordinateur agit en tant que client et serveur et chaque utilisateur décide des ressources qu'ils partagent sur sa machine assistance.ascomedia.com/index/IPR_0-17_RC_17_AC_73.html

Ou P2P. Cette technologie permet d'échanger des fichiers de client à client sans autre intermédiaire. Ainsi, deux internautes peuvent troquer des données sans passer par un serveur central. www.visionduweb.com/lesplus/lexique/p.php4

³⁷⁸ Le site Droit & Nouvelles Technologies présente S. Dusollier, Internet et le droit d'auteur, in Actualités du droit des technologies de l'information et de la communication, Formation Permanente CUP, février 2001 - Vol. 45, p. 161-220 : http://www.droit-technologie.org/2_1.asp?dossier_id=56

³⁷⁹ Rapport du Conseil d'Etat, Internet et les réseaux numériques, La Documentation Française, p.135.

reproduites légalement en vue d'un usage public. Pour pouvoir les exploiter et les diffuser, il est impératif d'obtenir une autorisation écrite des titulaires des droits d'auteur sur cette œuvre. Cette autorisation doit expressément mentionner les utilisations admises : elle doit préciser leur étendue, leur destination, leur localisation et enfin leur durée³⁸⁰.

Comme pour toutes les infractions préexistantes au cyberspace, Internet a joué un rôle amplificateur des atteintes faites aux droits d'auteurs. Ces atteintes prennent une autre ampleur sur Internet :

- d'une part à cause de son universalité tous les contenus peuvent être consultés, diffusés ou téléchargés sur la Toile grâce aux différents moteurs de recherche, même lorsque aucune autorisation ne permet une telle utilisation,
- d'autre part la gratuité semblant être la règle dans la majorité des cas dans le cyberspace accélère les phénomènes de téléchargements attentatoires au droit d'auteur.

Les techniques utilisées sur Internet fragilisent les règles classiques du droit d'auteur. Il s'est très vite révélé nécessaire de préciser la frontière entre les prérogatives relevant du monopole exclusif de l'auteur, et les exceptions légales que certains internautes tentent d'invoquer pour justifier l'exploitation libre et sans autorisation des œuvres protégées³⁸¹. Malgré ces spécificités, Internet n'est pas une zone de non droit pour ce qui est du droit d'auteur.

Un tribunal belge statuant sur une affaire de droit d'auteur dans le cyberspace, s'est prononcé sur le fait que la numérisation devait être considérée comme une reproduction³⁸² au sens du droit de reproduction. Cette jurisprudence pionnière a été suivie dans d'autres pays européens qui, d'une seule voix ont affirmé que le droit de reproduction couvrait bien les actes de numérisation et de stockage sur la mémoire d'un ordinateur³⁸³.

Le droit d'auteur n'est en aucune façon limité par la nature du support de diffusion. Les créations numériques présentes sur le réseau seront soumises comme n'importe quelle autre

³⁸⁰ Article L.131-3 CPI.- Pierre Perez, Le droit d'auteur : <http://www.educnet.education.fr/jur/auteur1.htm>

³⁸¹ Christiane Féral-Shuhl, Cyberdroit : le droit à l'épreuve d'Internet, 2^e édition Dalloz-Dunod 2000, p.7.

³⁸² Tribunal de 1^{ere} instance Bruxelles 16 octobre 1996, RIDA avril 1997, n°172, p.238 ; Bruxelles 28 octobre 1997 RIDA juillet 1998, n°177, p.204.

³⁸³ TGI Paris (référé) 14 août 1996, RIDA janvier 1997, n°171, p.361 ; TGI Paris 5 mai 1997, JCP 1997.II.22906 ; TI Strasbourg 3 février 1998, RIDA avril 1998, n°176, p.410 ; TI Paris 14 avril 1999, Gaz. Pal. 23-24 juillet 1999, p.38.

œuvre au droit d'auteur, qu'elles soient proposées à titre gratuit ou non³⁸⁴. En vertu de la théorie de " *l'unité de l'art* ", le droit d'auteur protège toutes les œuvres, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination (L112-1 CPI). La numérisation des œuvres présentes sur Internet n'a aucune incidence sur leur protection ce, d'autant plus que la numérisation est reconnue comme étant une reproduction par la déclaration jointe à l'article 1-4 du traité de l'Organisation Mondiale de la Propriété Intellectuelle. Peuvent être protégées aussi bien des œuvres d'art traditionnelles que des créations plus utilitaires comme des logiciels (L112-2 13° CPI) et les bases de données³⁸⁵.

Une œuvre numérisée peut tout à fait être signée. Les techniques de cryptage et de codification permettent d'associer à chaque document une sorte de fiche d'identité précisant son origine, son auteur, l'heure et le lieu de sa copie³⁸⁶. On admet que suite à une modification l'on puisse au titre des droits voisins, être titulaire de droits sur une œuvre à laquelle on aura en quelque sorte donnée une nouvelle naissance. La condition étant l'originalité de l'œuvre.

2-b. Les supports numériques

Le Conseil d'Etat a entériné l'application du droit d'auteur aux œuvres on-line. Il a par la même occasion, considéré qu'il n'était pas nécessaire « *de créer un droit spécifique de transmission numérique, de distribution numérique ou de mise à disposition du public comme cela paraît envisagé dans certains pays comme les Etats-Unis ou le Japon* »³⁸⁷. On a pu penser que les formes de créations numériques fragilisaient les règles classiques du droit d'auteur en rendant obligatoire la délimitation entre les prérogatives relevant du monopole exclusif de l'auteur et les exceptions légales permettant une exploitation sans autorisation d'œuvres protégées³⁸⁸.

³⁸⁴ Site Internet de veille juridique : Educnet ; Pierre Perez, Grégoire Jocquel, Jean-françois Gilot, Philippe Amblard, Guide pratique du droit d'auteur sur Internet, mars 2005

<http://www.educnet.education.fr/juri/droitauteur/>

³⁸⁵ Ibid.

³⁸⁶ Gabriel de Broglie, Le droit d'auteur et Internet, Rapport du groupe de travail de l'Académie des sciences morales et politiques, Cahier des sciences morales et politiques, PUF 2001, p.31.

³⁸⁷ Rapport du Conseil d'Etat, « Internet et les réseaux numériques », La Documentation Française, p.135.

³⁸⁸ Christiane Féral-Shuhl, Cyberdroit : le droit à l'épreuve d'Internet, préc., p.7.

Sur Internet, la création est souvent le fait d'un investisseur et l'œuvre le produit des efforts conjugués d'un grand nombre d'intervenants (graphiste, programmeurs, scénariste, etc.). L'enjeu repose sur à la titularité des droits d'auteur³⁸⁹.

L'œuvre multimédia³⁹⁰ est l'œuvre numérique³⁹¹ par essence. Elle peut être définie comme « toute œuvre de création incorporant sur un même support un ou plusieurs éléments suivants : texte, son, images fixes, images animées, programmes informatiques dont la structure et l'accès sont régis par un logiciel permettant l'interactivité »³⁹². Un Décret du 31 décembre 1993 relatif au dépôt légal définit en son article 3 l'œuvre multimédia comme : « tout document qui, soit regroupe deux ou plusieurs supports mentionnés dans la loi de du 20 juin 1992³⁹³ ; soit associe sur un même support deux ou plusieurs documents soumis à l'obligation de dépôt ». Il s'agit d'une création intellectuelle susceptible d'être reproduite sur un support matériel. L'œuvre doit être originale c'est-à-dire que, au sens du droit civil elle doit être imprégnée de la personnalité de son auteur³⁹⁴ ; ce qui devrait suffire à lui conférer un caractère original.

Les Cd-rom, les jeux vidéo, les weblogs, les pages personnelles sont des œuvres numériques, des œuvres multimédias. Il se pose la question du régime juridique dont ces œuvres dépendent. Relèvent-elles du droit commun ? Doivent-elles faire l'objet d'un régime dérogatoire ? Sont-elles régies par les dispositions spéciales du droit d'auteur conformément aux conditions posées à l'article L112-2 du code de propriété intellectuelle³⁹⁵?

³⁸⁹ Ibid., p.8.

³⁹⁰ Le mot multimédia est entré dans notre vocabulaire en 1980 comme un adjectif qualifiant un objet décliné sur différents supports. Une œuvre multimédia concerne plusieurs médias, elle peut être diffusée par plusieurs médias. Un arrêté ministériel de l'Industrie, des Postes et Télécommunications et du Commerce extérieur du 2 mars 1994 relative à la technologie des télécommunications propose comme définition du multimédia « ce qui associe plusieurs modes de représentation des informations, tels que textes, sons et images », Delphine Valleteau de Moulliac, Copyright et droit d'auteur - Définition de l'œuvre multimédia, 28 août 2004. <http://www.avocats-publishing.com/Qualifier-1-oeuvremultimedia-I-A>

³⁹¹ Le terme multimédia ne s'entend plus comme une multiplicité de supports mais plutôt comme une multiplicité de contenus rendus possibles grâce à la numérisation des informations. Ce terme est désormais utilisé dans le langage courant comme un nom commun synonyme de numérique, Delphine Valleteau de Moulliac, préc.

³⁹² Livre Blanc du groupe de travail audiovisuel et multimédia de 1994, voire page 7.

³⁹³ Les supports pouvant constituer une œuvre multimédia sont des documents imprimés, des graphismes et photographies, des progiciels, des bases de données et systèmes experts, des phonogrammes, des vidéogrammes autres que ceux fixés sur un support photochimique, voire le site Droit de l'Informatique du Multimédia et des réseaux, Droitweb.com. <http://www.droitweb.com/dw2/articles.jsp?pArticleID=4&pSectionID=7>

³⁹⁴ Delphine Valleteau de Moulliac, Copyright et droit d'auteur - Définition de l'œuvre multimédia, op.cit. <http://www.avocats-publishing.com/Qualifier-1-oeuvremultimedia-I-A>

³⁹⁵ Ibid.

La seule condition nécessaire pour que soit mis en œuvre une protection inhérente au droit d'auteur est l'existence d'une forme originale, même éphémère de l'œuvre. Le support de l'œuvre est indifférent. Il peut être matériel ou non, palpable ou seulement visible. La notion d'œuvre est au sens de la propriété intellectuelle, indépendante de la qualité, de la nature ou même de la matérialité du support. Dès lors, la dématérialisation (par la numérisation notamment) des œuvres ne saurait avoir pour effet de les faire échapper à la législation réglementant la propriété intellectuelle³⁹⁶.

Une nécessaire formalisation implique que l'œuvre soit perceptible par les sens (ce qui exclut les simples idées); cependant son mode d'extériorisation est indifférent (écrit, oral, analogique, numérique...). L'originalité tient à une notion-cadre laissée à l'appréciation du juge. Il devra au cas par cas rechercher la marge de liberté laissée à l'auteur dans la composition de son œuvre. Ne serait pas considérée comme originale une œuvre dont la forme est entièrement dictée par une application industrielle.

Traditionnellement définie comme “*l’empreinte de la personnalité de l’auteur*“, cette notion d'originalité s'est révélée inadaptée aux créations plus utilitaires que sont les logiciels et les bases de données. Pour ce type de création, elle est désormais appréhendée comme un “*apport intellectuel propre à son auteur*“³⁹⁷.

B. La matière des droits d’auteur du mineur dans le cyberspace.

Les droits d’auteur constituent l’élément essentiel de la propriété littéraire et artistique. Ils sont tout à fait distincts du droit de propriété, puisque ce ne sont pas des droits réels (c'est-à-dire portant sur des choses, *res* en latin). L'usage du terme propriété intellectuelle est né d'une traduction approximative de l'anglais « *property* » signifiant « bien » et non « propriété ». De l’avis d’Edmond Picard, il conviendrait mieux d'utiliser le terme droit intellectuel qui serait plus adéquat d’un point de vue juridique³⁹⁸.

Un écrivain a des droits sur ses œuvres littéraires, ce qui implique un monopole d'exploitation de ses œuvres lui permettant de négocier la publication de l'œuvre par un éditeur, moyennant rémunération (droits d'auteur). Cette exploitation de son œuvre est un droit patrimonial car il

³⁹⁶ Gabriel de Broglie, Le droit d’auteur et Internet, préc.,p.28.

³⁹⁷ Ibid. Cf note 305 educnet.

³⁹⁸ http://fr.wikipedia.org/wiki/Droit_d%27auteur

en tire un profit pécuniaire. L'auteur a également un droit moral sur son œuvre. Ce droit est extrapatrimonial et rangé dans la catégorie des droits de la personnalité. Ce droit moral permet à l'auteur de faire respecter son œuvre, par exemple d'en faire interdire la contrefaçon³⁹⁹.

1. La nature juridique des droits d'auteur du mineur.

Le droit d'auteur est un droit incorporel qui prend naissance dans la création de l'intelligence. Le code de procédure pénale qui régit la matière, présente le droit d'auteur comme un ensemble d'œuvres de l'esprit. Ses droits découlent automatiquement de l'acte de création et ne sont pas subordonnés à des modalités de dépôt ; la seule condition est l'originalité de l'œuvre. Il n'existe pas une catégorie de droit d'auteur propre au mineur. Il s'agit simplement d'opérer des aménagements au regard du statut juridique spécifique du mineur.

Le droit d'auteur d'un mineur sur ses créations lui est propre. Lui et ses parents doivent selon les circonstances donner leur accord pour une publication sur Internet. Lors de sa diffusion l'œuvre du mineur doit comporter une mention quant à son droit d'auteur⁴⁰⁰. Le droit d'auteur est de nature patrimoniale et extrapatrimoniale. L'élément patrimonial est caractérisé par le droit que l'auteur a de tirer un avantage pécuniaire de l'œuvre ou de son exploitation commerciale. L'élément extrapatrimonial ou droit moral quant à lui consiste au droit au respect du nom, de l'intégrité de l'œuvre et de la qualité de l'auteur⁴⁰¹.

1-a. Les droits d'auteur, droits de la personnalité : l'aspect moral.

Le droit d'auteur est un droit moral perpétuel, inaliénable et incessible : il s'agit du droit au nom (droit à la signature de l'œuvre), du droit de divulgation (seul l'auteur peut décider de porter son œuvre à la connaissance du public) et du droit au respect de l'œuvre, à son intégrité⁴⁰².

³⁹⁹ http://fr.wikipedia.org/wiki/Droit_d%27auteur

⁴⁰⁰ Nancy E. Willard, *Supporting the Safe and Responsible Use of Internet by Students - A Children'Internet Protection Act Planning Guide*, Center for Advanced Technology in Oregon, 2001, pp. 152,156 et 164. Publié sur un site canadien Droit sur internet: Guide des droits sur Internet; Consignes relatives au droit d'auteur concernant le contenu publié pour l'usager mineur.

http://www.droit sur internet.ca/pratique_5_39.html

⁴⁰¹ Voir le site Internet de l'Association pour la gestion de la sécurité sociale des auteurs (AGESSA.)

<http://www.agemssa.org/activiteEtService/auteur/auteur.htm>

⁴⁰² Ce message a été diffusé sur la liste "edufraçais@univ-rennes1.fr" le 25 janvier 1996 par Christophe GUY, Attaché Linguistique de l'Ambassade de France au Canada, d'après les informations du Service juridique du CNRS : <http://clicnet.swarthmore.edu/CNRS.droits.html>

1.a'. Le droit au nom et à la paternité.

Une œuvre numérisée comporte, au même titre que d'autres œuvres, une signature. Cela est rendu possible par les techniques de cryptage et de codification qui lui confèrent une fiche d'identité avec un historique⁴⁰³. Il n'existe donc aucun obstacle technique à ce qu'un mineur puisse signer son œuvre numérique ou multimédia. C'est la première étape pour la reconnaissance de son droit d'auteur dans le cyberspace.

1.a''. Le droit de divulgation

Il s'agit du pouvoir discrétionnaire qui permet à l'auteur de décider le moment et le mode de communication de son œuvre au public. Il est admis en principe que le droit de divulgation se renouvelle avec chaque procédé. Dès lors, l'auteur peut en faire usage à chaque utilisation d'une nouvelle technique à laquelle il n'avait pas encore donné son consentement pour la diffusion de son œuvre⁴⁰⁴. La numérisation limite considérablement l'effectivité de ce droit, il n'en demeure pas moins que l'auteur peut user de son droit d'opposition et au besoin engager des poursuites à l'encontre du contrevenant⁴⁰⁵. Le mineur en tant qu'auteur doit pouvoir donner son consentement pour la divulgation de son œuvre, même si ce consentement doit être renforcé par celui de ses parents ou tuteurs légaux.

1.a'''. Le droit au respect de l'œuvre.

Ce droit est énoncé par le premier alinéa de l'article L.121-1 du CPI. Il permet à l'auteur de s'opposer à ce qu'il soit porté atteinte à l'intégrité de son œuvre, soit par une modification, soit par une utilisation qui en trahirait l'idée⁴⁰⁶.

1.a'''. Le droit de retrait ou de repentir

Il s'agit de la possibilité qu'a l'auteur de faire cesser la diffusion ou l'exploitation de son œuvre. Ce droit est d'une certaine manière assimilé à une coquille vide par le procédé de numérisation et la diffusion sur le Web de l'œuvre. La facilité de reproduction, la fluidité de la communication et la densité des connexions rendent quasiment irréversible la divulgation d'une œuvre dans la sphère publique qu'est le réseau. L'auteur qui souhaite user de son droit

⁴⁰³ Ibid., p.31

⁴⁰⁴ Gabriel de Broglie, Le droit d'auteur et Internet, Rapport du groupe de travail de l'Académie des sciences morales et politiques, Cahier des sciences morales et politiques, PUF 2001, p.30.

⁴⁰⁵ Ibid.

⁴⁰⁶ Ibid., p.31.

de retrait se retrouvera vraisemblablement dans l'impossibilité matérielle de le faire appliquer⁴⁰⁷.

1-b. L'aspect patrimonial du droit d'auteur

Le droit d'auteur a une dimension patrimoniale impliquant qu'aucune reproduction, aucune représentation de l'œuvre ne puisse être faite sans l'accord préalable de l'auteur ou de ses ayants droit ; l'auteur a en outre droit à une rémunération proportionnelle aux recettes tirées de l'exploitation de son œuvre⁴⁰⁸. L'auteur est libre de diffuser ses propres œuvres⁴⁰⁹ sur Internet, sous réserve de ne pas avoir accordé au préalable une exclusivité de diffusion à un tiers, éditeur ou distributeur. L'auteur devient ainsi lui-même éditeur ou producteur en même temps qu'auteur bien que désintéressé⁴¹⁰. C'est ce cas de figure qui se retrouve dans les sites personnels, les blogs, que les mineurs créent en ligne. Ils mettent en ligne leurs créations, à la disposition de tous et à titre gracieux. Il peut s'agir de photographie, de musique, d'articles, de graphisme ou plus globalement d'œuvres littéraires, artistiques. Cette mise à disposition gracieuse ne dissout pas pour autant leur droit d'auteur et encore moins le caractère patrimonial de ce droit par rapport à autrui.

1.b'. Le droit de suite

Le droit de suite désigne le droit, pour l'auteur d'une œuvre d'art originale, à percevoir un pourcentage sur le prix obtenu pour toute revente de cette œuvre effectuée par les professionnels du marché de l'art (maisons de vente aux enchères, galeries ou tout autre marchand d'art)⁴¹¹. L'auteur qui cède une de ses œuvres graphiques ou plastiques peut

⁴⁰⁷ Gabriel de Broglie, Le droit d'auteur et Internet, préc., p.31.

⁴⁰⁸ Liste "edufançais@univ-rennes1.fr" 25 janvier 1996, Christophe GUY, op.cit. <http://clinet.swarthmore.edu/CNRS.droits.html>

⁴⁰⁹ Le mineur se sert de ses pages personnelles (B I ro) III C d Ñ a Ñ : C C ó C y C L à, journal intime en ligne, sites personnels pour diffuser des textes, des images, de la musique et tout autre type d'œuvre dont il est l'auteur. Le cyberspace a le rôle d'un outil de promotion. Il ne s'agit pas que d'un outil de communication, visant la diffusion et l'échange d'œuvres avec autrui.

⁴¹⁰ Article de Christophe Guy, op.cit..

⁴¹¹ Directive 2001/84/CE du Parlement européen et du Conseil, du 27 septembre 2001, relative au droit de suite au profit de l'auteur d'une œuvre d'art originale.

continuer à tirer un profit de la revente ultérieure de son œuvre. L'article L 122-8 du code de la propriété intellectuelle met en place à son profit un droit inaliénable de participer au produit de toute revente à partir du moment où elle s'effectue aux enchères publiques ou par l'intermédiaire d'un commerçant. La revente par un particulier à un autre particulier en dehors d'enchères publiques ne bénéficie donc pas de ce droit de suite⁴¹².

La durée de protection correspond à celle prévue par la directive 93/98/CEE relative à la durée de protection du droit d'auteur et de certains droits voisins, à savoir 70 ans à partir de la mort de l'auteur. Ce droit existe en France depuis 1920.

1.b''. Le droit de reproduction

Le droit de reproduction consiste en la fixation matérielle de l'œuvre, par tout procédé, qui permette de la communiquer au public de manière indirecte. Les modes de reproduction peuvent être très variés : l'imprimerie, la photocopie, la photographie, le dessin, la numérisation, etc. (l'article L122-3 CPI en dresse une liste non exhaustive). Il y a reproduction chaque fois qu'il y a changement de support de l'œuvre. L'autorisation de l'auteur est requise pour chacun des procédés envisagés dès lors que le droit de reproduction n'est pas destiné à un usage privé. Il existe, sous réserve que soient clairement indiqués le nom de l'auteur et la source, des exceptions à l'obligation de demander l'autorisation de l'auteur (article L 122-5 CPI) :

- les analyses et courtes citations : la citation doit être justifiée, courte (l'emprunt ne doit pas reprendre l'essentiel de l'œuvre), et ne doit pas porter atteinte au droit moral de l'auteur cité ;
- les revues de presse : « la diffusion, même intégrale, par la voie de la presse ou de la télédiffusion, à titre d'information d'actualité, des discours destinés au public prononcés dans les assemblées politiques, administratives, judiciaires ou académiques, ainsi que dans les réunions publiques d'ordre politique et les cérémonies officielles »;
- la parodie, le pastiche et la caricature⁴¹³.

⁴¹² Les chroniques juridiques (Juritel – Droit d'Internet, informations légales, Benoît Mahot, Le droit de suite des auteurs, http://www.juritel.com/Liste_des_chroniques-104.html

⁴¹³ Le site du CNRS, Direction des affaires juridiques, Propriété intellectuelle - Droit d'auteur <http://www.sg.cnrs.fr/daj/propriete/droits/droits3.htm>

La numérisation est également reconnue comme une reproduction par la déclaration jointe à l'article 1.4 du traité de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI)⁴¹⁴.

1.b'''. Le droit de représentation.

Il « *consiste dans la communication de l'œuvre au public par un procédé quelconque et notamment :*

- *Par récitation publique, exécution lyrique, représentation dramatique, présentation publique, projection publique et transmission dans un lieu public de l'œuvre télédiffusée ;*
- *Par télédiffusion. La télédiffusion s'entend de la diffusion par tout procédé de télécommunication de sons, d'images, de documents, de données et de messages de toute nature. Est assimilée à une représentation l'émission d'une œuvre vers un satellite » (art. L 122-2 du CPI).*

Ces trois aspects patrimoniaux du droit d'auteur correspondent à des catégories spécifiées d'œuvres protégées par le droit d'auteur. De prime abord il semble difficile de trouver une adéquation avec les droits d'auteurs tels qu'ils peuvent être mis en œuvre sur Internet ; mais ce serait ignorer la dimension universaliste de la Toile et la prépondérance du commerce électronique dans l'évolution sans cesse croissant d'Internet.

En vertu de la loi sur la propriété intellectuelle, diffuser les œuvres de tiers constitue un acte d'exploitation qui n'est possible qu'avec l'autorisation de l'auteur même mineur. Une diffusion sans autorisation de l'auteur empêche, ce dernier de vivre de son travail et méconnaît les investissements des éditeurs et / ou des producteurs. Lors de la diffusion d'une de ses œuvres, sans autorisation préalable de sa part, l'auteur est susceptible de demander des dommages et intérêts au titre du préjudice moral et patrimonial subi.

Si l'on considère dans un premier temps le droit de suite qui concerne la vente d'objet d'art ; il est notoire que les ventes aux enchères sur la Toile connaissent un développement croissant. On peut subdiviser ces ventes aux enchères en deux catégories : les ventes aux enchères

⁴¹⁴ Gabriel de Broglie, le droit d'auteur et Internet, préc., p.32.

spécifiques au cyberspace⁴¹⁵, et les ventes prenant naissance dans le “monde réel“ et qui sont relayées sur Internet par un procédé de visioconférence par exemple.

2. La mise en œuvre des droits d’auteur du mineur.

Le mineur dispose d’une personnalité juridique, il est titulaire de droits et d’obligations. Il est légitime à exercer ses droits d’auteur dans le cyberspace. Ses droits nécessitent une protection légale. Dans certaines circonstances cependant, cette protection ne sera pas absolue et fera l’objet d’aménagements.

2-a. Le principe de la protection des droits d’auteur du mineur.

La reconnaissance des droits d’auteur du mineur suppose un dispositif de protection de ceux-ci. Il peut être mis en œuvre une protection temporelle d’une part, ou une protection par le biais de la technologie.

2.a'. La protection temporelle.

La protection de l’élément moral du droit d’auteur est perpétuelle tandis que la protection des aspects patrimoniaux du droit d’auteur subsiste pendant soixante-dix ans à compter du 1^{er} janvier de l’année civile suivant :

- la mort de l’auteur (art. L.123-1 al. 2 CPI).
- la mort du dernier coauteur pour les œuvres de collaboration (L123-2 al. 1 CPI).
- le jour de leur publication pour les œuvres anonymes, pseudonymes et collectives.

Une œuvre entre dans le domaine public lorsque les droits patrimoniaux sont épuisés. C’est le cas, par exemple en droit européen, 70 ans après la mort de son auteur. Cette œuvre devient alors utilisable gratuitement, la seule contrainte étant liée aux droits extrapatrimoniaux. Il suffit de citer le titre et l’auteur de l’œuvre utilisée⁴¹⁶.

2.a". La protection technologique.

⁴¹⁵ EBay est à ce propos un des sites de références des enchères en ligne.

⁴¹⁶ http://fr.wikipedia.org/wiki/Droit_d%27auteur

Elle consiste en la protection des œuvres par des dispositifs technologiques. Cela peut se traduire par l'impossibilité de copier l'œuvre, par un système de contrôle d'accès, de certification ou un marquage des œuvres. Il faut entendre par dispositifs techniques, toute technologie, dispositif ou composant qui est destiné à empêcher ou à limiter les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin, par le moyen d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'objet protégé ou d'un mécanisme de contrôle de copie (voir pour la définition complète l'article 6-3 de la Directive 2001/29/CE du 22 mai 2001). Ces procédés sont initiés par les titulaires des droits d'auteur et des droits voisins afin de protéger leurs œuvres et enregistrements contre des utilisations non autorisées. Ils sont aujourd'hui largement répandus, particulièrement dans l'environnement numérique. L'article 6 de la directive du 22 mai 2001 sur le droit d'auteur dans la société de l'information⁴¹⁷ prévoit que la protection par des mesures techniques concerne tous les actes non autorisés par le titulaire des droits et/ou son représentant légal.

Il existe deux niveaux de protection : la protection technique et la protection juridique des mesures techniques. La protection par la technique du droit d'auteur a fait surgir un effet pervers : les systèmes techniques sont susceptibles de restreindre l'accès à des œuvres qui ne seraient pas protégées par le droit d'auteur. Ils peuvent empêcher des usages même autorisés. En théorie, l'utilisateur devrait contourner la mesure technique pour réaliser des actes autorisés et ce faisant, commettre un acte illicite⁴¹⁸. Même si l'utilisateur contourne la barrière technique pour effectuer une utilisation de l'œuvre autorisée, il reste susceptible d'être poursuivi pour avoir neutralisé la mesure technique et tomber sous le coup des lois incriminant l'intrusion non autorisée⁴¹⁹. Cette protection technique des droits ne doit pas *in fine*, priver les utilisateurs des exceptions aux droits prévues par la loi. La Directive européenne du 22 mai 2001 s'est prononcée sur cette question en instaurant un impératif : la recherche de l'équilibre entre les droits et les exceptions

Les dispositifs techniques de protection sont divers :

⁴¹⁷ La Directive européenne du 22 mai 2001 (directive n° 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, JOCE L 167/10 du 22 juin 2001

⁴¹⁸ Valérie Sedallian, Internet et droit d'auteur, article présenté lors des rencontres de la manifestation « Autour du Libre 2002 » INT Evry 19.05.2002, paru sur le Site Internet juridique.

<http://www.internet-juridique.net/publications/droitcomm/libreetcontenu2002.html>

⁴¹⁹ Ibid.

- Le cryptage (ou technique de chiffrement⁴²⁰) est un des procédés de la protection technologique du droit d'auteur. Le contenu est enveloppé dans un système de cryptage et associé à une application logicielle nécessaire à son utilisation⁴²¹.
- La technique de marquage fonctionne selon une logique de traçabilité ou d'empreinte (watermaking). Elle consiste à marquer une œuvre ou une prestation de telle manière que toute modification puisse être décelée⁴²².

La protection technique bien que légitime risque de créer un déséquilibre au profit des titulaires de droit en augmentant le contrôle de l'industrie du contenu sur l'usage des contenus sur le réseau⁴²³.

2-b. Les exceptions du droit d'auteur.

L'article L.121-1 du CPI dispose que « *l'auteur jouit du droit au respect (...) de son œuvre* ». Cette prérogative lui permet de s'opposer à toute utilisation indue, toute modification portant atteinte à l'intégrité de l'œuvre, ainsi qu'à toute utilisation portant atteinte à l'esprit de son œuvre. Il existe une possibilité de faire exception à cette règle : l'hypothèse où l'auteur a choisi de placer son œuvre sous le régime du contenu libre⁴²⁴, entendant ainsi renoncer à son droit à l'intégrité de son œuvre. La notion de contenu libre est apparue à la suite de celle de logiciel libre et en constitue une extension.

Des débats sont encore en cours pour définir les droits minimaux qui devraient être associés à une production intellectuelle pour que ce contenu puisse être considéré comme libre.

⁴²⁰ Gabriel de Broglie, Le droit d'auteur et Internet, Rapport du groupe de travail de l'Académie des sciences morales et politiques, Cahier des sciences morales et politiques, PUF 2001, p.24.

⁴²¹ Par exemple, une image peut être visionnée, une musique écoutée mais pas enregistrée sur le disque dur sauf possession d'une clé ou d'une application spécifique dont les droits d'utilisation doivent être acquis, Joëlle Farchy, CNRS Communication, Internet et le droit d'auteur. La culture Napster, CNRS Editions 2003, p 150-151.

⁴²² Joëlle Farchy, op.cit., p.150-151.

⁴²³ Valérie Sédallian, Internet et droit d'auteur, op.cit.

⁴²⁴ Un contenu libre désigne tout contenu de création intellectuelle ou artistique proposé à la libre diffusion et redistribution. Ces contenus peuvent être des documents, des images, des textes, de la musique, des logiciels, etc. ; dont les auteurs ont choisi de définir les conditions d'utilisation de façon plus souple que celles définies par défaut dans la législation par le droit d'auteur. La notion de contenu libre ne concerne donc pas la liberté d'expression mais la libre diffusion. Les droits donnés par les auteurs sont alors définis dans une licence dite 'libre' associée au document. Ces libertés peuvent concerner la consultation (recopie, réutilisation, modification...) des contenus et peuvent être associées à des obligations (citer l'auteur original, obligation de maintenir la licence originale...) et des restrictions (pas d'usage commercial, interdiction de certains médias ...). Il existe différentes licences, qui proposent éventuellement différentes options permettant aux auteurs de choisir le type d'utilisation de leur travail qu'ils souhaitent ou non autoriser (rendre libre).

http://fr.wikipedia.org/wiki/Contenu_libre

- Le droit de redistribution est unanimement considéré comme indissociable de la notion de "contenu libre".
- Le droit de modification est considéré par certains comme une option pour certains types de contenus, artistiques ou scientifiques notamment. D'autres, plus proches de la logique originale des logiciels libres, considèrent qu'aucun contenu ne peut être défini comme libre si l'utilisateur n'a pas le droit de le modifier.
- Le droit d'utilisation commerciale est aussi considéré comme évident par les uns, alors que d'autres souhaitent pouvoir le restreindre ou l'interdire, réservant les libertés à l'utilisateur final de l'œuvre.

Ces différences apparaissent à la lecture des différentes licences, ou parfois des différentes options de ces licences se revendiquant comme libres ; certaines sont contestées dans cette revendication de liberté⁴²⁵.

Une interrogation demeure quant à la légalité de cette renonciation, surtout s'agissant du mineur. L'article L.121.1 alinéa 2 du CPI prévoit que le droit de l'auteur concerné est « *perpétuel et inaliénable et imprescriptible* », ce faisant cet article introduit un élément impératif conférant au droit d'auteur un aspect d'ordre public. On en vient à parler d'un consentement de l'auteur à toute adaptation, transformation ou arrangement ultérieur plutôt qu'à une renonciation⁴²⁶.

On retiendra trois principales situations dans lesquelles il est possible de reproduire, de représenter des œuvres en l'absence d'autorisation de l'auteur, du titulaire des droits ou de ses représentants légaux : les exceptions pour copies techniques, les exceptions d'utilisation privée et les exceptions d'utilisation publique.

2.b'. Les exceptions pour copies techniques

⁴²⁵ http://fr.wikipedia.org/wiki/Contenu_libre

⁴²⁶ Article L.122-7 du CPI, Gratuité et nouvelles technologies, Communication du Colloque « La gratuité, une question de droit ? », 26 et 27 avril 2000 par le Centre d'étude et de recherche : Fondement du droit public (Université de Cergy Pontoise et Paris X Nanterre) publié par les éditions de L'Harmattan en 2003, Paru sur le site de Sébastien Canevet « Le Chêne et le Gland » en date du 16 janvier 2005.
http://www.canevet.org/article.php3?id_article=20#nh16

Les copies techniques consistent en des « *actes de reproduction provisoires [...] qui sont transitoires et accessoires et constituent une partie intégrante et essentielle d'un procédé technique, ayant pour unique finalité de permettre une transmission dans un réseau entre tiers..* »⁴²⁷. Cette exception a pour objectif de permettre aux opérateurs de télécommunications, de ne pas encourir le grief de contrefaçon pour la réalisation de copies d'œuvres protégées ne constituant en réalité que des étapes de leur transmission sur les réseaux informatiques, en particulier la réalisation de "cache"⁴²⁸.

2.b". Les exceptions d'utilisations privées⁴²⁹.

Lorsqu'une œuvre a été divulguée, l'auteur ne peut interdire les représentations privées et gratuites effectuées exclusivement dans un cercle familial : des copies, des reproductions strictement réservées à un usage privé du copiste. Les copies de sauvegarde d'un logiciel, ainsi que les copies ou les reproductions d'une base de données électroniques⁴³⁰. La condition indispensable à respecter est d'indiquer clairement le nom de l'auteur et la source de l'œuvre.

La copie doit être faite par le copiste pour son propre usage ; ne sont pas admises les copies de copie ou les copies pour autrui. Il est cependant possible de copier une œuvre que l'on ne possède pas, la loi ne précise pas que l'original doit avoir été acquis par le copiste. La loi ne précise pas non plus que l'accès doive avoir été licite, mais sous-entend que la copie obtenue illégalement (vol, téléchargement en violation des droits d'auteur) serait un recel de contrefaçon⁴³¹.

La présentation sur un site Internet privé d'œuvres sans l'autorisation des titulaires des droits, ne peut être considérée comme entrant dans le champ de l'exception de copie privée, dès lors que des tiers connectés peuvent visiter les pages privées et prendre copie des œuvres⁴³².

⁴²⁷ Article 5 de la Proposition de directive sur « l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, Légipresse, n°178-janvier/février 2001, Chroniques et opinions, p.4.

⁴²⁸ Ce sont des copies intermédiaires des données transmises dont le seul but est d'améliorer l'accès par les internautes à des informations, accessibles par ailleurs sur le réseau – Stéphanie Berghe et Laurent Cohen-Tanugi : Droit d'auteur et copyright face aux technologies numériques : comparaisons transatlantiques, Chroniques et opinions, p.4.

⁴²⁹ Article L.122-5 du CPI.

⁴³⁰ Dans les conditions prévues au II de l'article L.122-6-1 du Code de propriété intellectuelle.

⁴³¹ Les exceptions au droit d'auteur. Site Wikipédia.

http://www.wikipedia.org/wiki/Droit_dauteur#les_exceptions_au_droit_d.27auteur

⁴³² TGI Paris 14 août 1996, Société Ed. Pouchenel, Brel et autres contre Ecole centrale de Paris et autres ; Société Art Music France, Warner Chappel France et autres contre Ecole nationale supérieure des télécoms et autres, Gabriel de Broglie, Le droit d'auteur et Internet, préc., p.34.

2.b'''. Les exceptions d'utilisations publiques

Certaines utilisations publiques d'œuvres restent possibles sous réserve que soient indiqués clairement le nom de l'auteur et la source.

- Les analyses et courtes citations justifiées par le caractère critique, polémique et pédagogique, scientifique ou d'information de l'œuvre à laquelle elles ont incorporées.
- Les revues de presses.
- La diffusion même intégrale par presse ou télédiffusion à titre d'information d'actualité, des discours destinés au public dans les assemblées politiques, administratives, judiciaires ou académiques, ainsi que des réunions publiques d'ordre politique et les cérémonies officielles.
- Les reproductions intégrales ou partielles d'œuvres d'art graphique ou plastique destinées à figurer dans le catalogue d'une vente judiciaire effectuée en France pour les exemplaires mis à disposition publique avant la vente avec but descriptif.
- La parodie, le pastiche, caricature, etc.⁴³³

Il y a également les œuvres qui sont tombées dans le domaine public c'est-à-dire celles dont les droits patrimoniaux sont expirés. Sont également concernées par cette exception, les œuvres qui par nature ne bénéficient pas de la protection du droit d'auteur : les textes de loi, les décisions de justice, etc.

Au même titre que les violations des droits du mineur génèrent l'engagement de la responsabilité de ceux qui en sont les auteurs, il peut voir sa propre responsabilité engagée lorsqu'il ne respecte pas ses obligations et ce faisant viole les droits d'autrui.

⁴³³ Ibid.

Titre 2. LA SANCTION JURIDIQUE DES DROITS ET OBLIGATIONS DU MINEUR DANS LE CYBERESPACE.

Le mineur est une personne physique qui doit se soumettre aux règles juridiques en vigueur dans le pays où il réside. Sa personnalité juridique, et les droits et obligations qui en découlent ne peuvent en aucun cas être mis en cause. En réalité, ce n'est pas l'effcience de ces droits et obligations qui posent problème ; la difficulté (si on peut la définir comme telle) réside dans l'étendue de ses droits et obligations.

Il est établi que le mineur est un internaute qui interagit dans le cyberespace au même titre que tous les internautes. Simplement, les conséquences juridiques de ses actes (voulus ou subis) ne relèvent pas toujours du droit commun eu égard à la double spécificité juridique du mineur et du cyberespace.

Le véritable enjeu n'est donc pas de savoir si mais plutôt comment doivent être juridiquement sanctionnés les droits et obligations du mineur dans le cyberespace. Pour ce faire, il faudra établir la capacité juridique du mineur à agir dans le cyberespace et analyser la sanction qu'il convient de porter aux manquements des mineurs aux droits d'autrui.

Chapitre 1. LA CAPACITÉ JURIDIQUE DU MINEUR DANS LE CYBERESPACE.

En principe, toute personne jouit de la capacité juridique ; ainsi chacun peut accomplir seul tout acte juridique sans avoir besoin ni de l'assistance d'une autre personne, ni d'une autorisation. La capacité est la règle, l'incapacité l'exception⁴³⁴. Le législateur a prévu une catégorie de personnes dites "incapables". Il s'agit de personnes qui ne pourront accomplir certains actes que si elles sont représentées ou assistées par une autre personne (un tuteur par exemple), ou si elles obtiennent une autorisation. La minorité fait partie de l'un des critères de l'incapacité juridique.

L'incapacité du mineur est une incapacité d'exercice qui se traduit par une diminution de son pouvoir d'agir. Cette incapacité est naturelle chez un jeune enfant (moins de 7 ans) mais artificielle chez le grand adolescent proche de la majorité (entre 16 et 18 ans)⁴³⁵. Cette incapacité vise à protéger le mineur contre lui-même et contre les tiers qui pourraient abuser de son inexpérience ou de ses passions. Elle est présentée comme une incapacité de protection⁴³⁶. Dans la réalité l'incapacité du mineur ne peut être absolue. Il est admis que le mineur encadré par ses parents puisse poser certains actes juridiques susceptibles d'avoir une portée juridique plus ou moins limitée.

Le mineur est un acteur à part entière dans le cyberespace. Il est amené dans le cadre de conventions conclues (de manières tacite ou explicite avec autrui) à s'engager, à remplir des obligations ou à engager sa responsabilité juridique. La règle s'applique pour toutes les conventions que le mineur serait amené à conclure y compris dans le cyberespace. L'article 1108 du code civil définit les éléments indispensables à la validité d'un contrat comme étant : le consentement, la capacité des cocontractants, la cause et l'objet. Le contrat électronique ne déroge pas à ces conditions de validité.

⁴³⁴ Capacité et incapacité. <http://www.notanamur.be/articles/CAPACITE.html>

⁴³⁵ Jean Carbonnier, Droit civil Tome 2, La famille, l'enfant, le couple, préc., p. 130.

⁴³⁶ Jean Carbonnier, Droit civil Tome 2, op.cit, p. 130.

Le commerce électronique constitue une des principales activités pratiquées sur la Toile ; il est souvent identifié à Internet⁴³⁷. Le commerce électronique est essentiellement fondé sur le passage de contrats⁴³⁸. On lui doit plus qu'au reste, le développement exponentiel du cyberspace. Il génère en principe l'essentiel des contrats qui sont conclus entre les cybernautes.

Toute personne souhaitant commercer ou entendant proposer des biens et/ou des services sur le réseau est tenue de respecter certaines règles propres ou non au cyberspace ; le mineur ne fait pas exception à cette condition pour les contrats électroniques qu'il est susceptible de conclure sur le Web.

§ 1. Le contrat électronique conclu par un mineur.

Conformément à l'article 1123 du code civil, « *Toute personne peut contracter, si elle n'en est pas déclarée incapable par la loi* ». Selon l'article 1124 du même code, « *Sont incapables de contracter, dans la mesure définie par la loi : les mineurs non émancipés ; les majeurs protégés au sens de l'article 488 du présent code* »⁴³⁹.

Le commerce électronique est pour beaucoup dans l'essor d'Internet. Internet est devenu l'une des plus grandes vitrines commerciales offrant une visibilité mondiale, qui n'est limitée par aucune contrainte temporelle. Selon la définition posée par la Loi pour la Confiance dans l'Économie Numérique, « *le commerce électronique est l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services* ». Le commerce électronique est essentiellement fondé sur le passage de contrats⁴⁴⁰.

⁴³⁷ Eric. A. Caprioli, Règlement des litiges internationaux et droit applicable dans le commerce électronique, Jurisclasseur Litec 2002, p. 1.

⁴³⁸ Xavier Linant de Bellefonds, Le droit du commerce électronique, Que-sais-je ?, PUF 2005, p.36.

⁴³⁹ Loi n° 68-5 du 3 janvier 1968 Journal Officiel du 4 janvier 1968 en vigueur le 4 juillet 1968.

⁴⁴⁰ Xavier Linant de Bellefonds, Le droit du commerce électronique, op.cit.

Un contrat est une convention par laquelle une ou plusieurs personnes s'obligent, envers une ou plusieurs autres, à donner, à faire ou ne pas faire quelque chose⁴⁴¹. Un contrat électronique quant à lui est un contrat qui prend naissance dans le cyberspace, même si ses effets s'appliquent en dehors de ce dernier. Dans leur majorité, les contrats électroniques sont conclus dans le domaine du commerce électronique et concernent la vente et l'achat.

Le seul fait de conclure par voie électronique des contrats pose la question du moment de la formation des contrats par ce vecteur nouveau. L'étude des contrats électroniques conclus par les mineurs implique deux types de contrats : ceux conclus entre professionnels et non professionnels et ceux conclus entre non professionnels.

L'Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique, plutôt que de modifier une série de textes insère dans le Code civil des dispositions générales. Pour une part, les règles relatives au contrat électronique procèdent à l'adaptation de règles existantes, pour une autre part, elles le soumettent à un régime spécifique⁴⁴².

Les contrats électroniques entrent dans la catégorie juridique soit des ventes par démarchage, soit des ventes à distance. Lorsque le consommateur a reçu une offre commerciale directement sur sa messagerie, sans aucune demande de sa part, l'achat qui en découlerait relève du démarchage⁴⁴³. Si au contraire l'internaute s'est connecté de son propre chef, il y aura éventuellement vente à distance⁴⁴⁴. Dans ces deux hypothèses, et dans la majorité des contrats électroniques, les deux parties ne sont pas en présence l'une de l'autre au moment de la conclusion du contrat. Rentrent également dans la catégorie des contrats électroniques, ceux qui se concluent par voie électronique alors même que les parties sont ensemble⁴⁴⁵ ; l'hypothèse est rare mais peut se présenter.

Tous les auteurs s'accordent sur les risques accrus que comporte la conclusion d'un contrat électronique. Ces risques sont entre autres liés au fait qu'il est plus difficile de mémoriser les énonciations relatives à la formation du contrat électronique. Cette difficulté tient à la

⁴⁴¹ Sous la direction de Rémy Cabrillac, Dictionnaire du vocabulaire juridique, Jurisclasseur ;- Code civil article 1101.

⁴⁴² Le nouveau régime des contrats électroniques, article publié le 19 septembre 2005 par Pierre Matringe sur les sites DROIT – NTIC voir : <http://www.droit-ntic.com/news/afficher.php?id=320>

⁴⁴³ L. Bochuberg, Internet et commerce électronique.

⁴⁴⁴ Philippe Le Tourneau, Contrats informatiques et électroniques, Dalloz 3^e édition, p. 291.

⁴⁴⁵ A. Raynouard, Le contrat électronique, p. 15-17.

présentation de ces contrats. L'internaute doit faire défiler l'information sur son écran lors de sa lecture. Dès lors les erreurs de compréhensions sont plus fréquentes. Il n'en demeure pas moins que ce contrat doit respecter les règles de droit commun des contrats tels qu'énoncés à l'article 1108⁴⁴⁶ du code civil, règles qui trouvent leur pendant dans plusieurs législations étrangères⁴⁴⁷.

A. La validité des contrats électroniques conclus par le mineur.

La question de la validité des contrats électroniques est inhérente à l'omniprésence des mineurs dans le cyberspace. Du fait de l'usage qu'ils font d'Internet, se pose la question des incapacités pouvant affecter la validité d'un contrat électronique qu'ils auraient conclu dans le cyberspace.

1. La capacité juridique du mineur

Les contrats électroniques, bien qu'ils ne soient pas conclus *intuitus personae* doivent prendre en considération la personnalité juridique des cocontractants. Cet aspect révèle toute son importance lorsqu'un incapable tel que le mineur est partie au contrat. Il faut noter que tous les mineurs ne se valent pas ; la minorité est découpée en groupes où l'on reconnaît au mineur un discernement plus ou moins important. La capacité ou plutôt l'incapacité juridique du mineur pourrait être indexée à ce découpage.

Au quotidien, tout individu est amené à contracter sans en avoir conscience pour les actes courants de la vie ; ainsi le moindre achat (pains, confiseries, cigarettes...) suppose la conclusion tacite d'un contrat d'achat et de vente, bien qu'aucun document ne soit signé. Si l'on appliquait strictement le code civil, aucun mineur ne serait en mesure de s'acheter un encas, un café, du pain, sans être accompagné d'une personne majeure à même de valider son

⁴⁴⁶ Pour qu'un contrat soit valablement conclu :

- il faut que les parties en cause soient en mesure de contracter, c'est-à-dire qu'une incapacité à contracter ne vienne pas bloquer le processus ;
- il faut que l'objet du contrat soit parfaitement licite et porte sur des choses qui soient dans le commerce ;
- le consentement des parties doit être exprimé sans être infecté d'un vice tel que l'erreur, le dol ou la violence.

⁴⁴⁷ Philippe Le Tourneau, Contrats informatiques et électroniques, op.cit. p. 276.

consentement⁴⁴⁸. La capacité juridique du mineur à contracter est tolérée dans des actes de la vie courante dans la “vie réelle“. Est-ce également le cas dans le monde virtuel ?

L'internaute cocontractant doit avoir la capacité juridique. La difficulté à laquelle on est confronté lors de la conclusion de contrat sur Internet est la suivante : la capacité à déterminer la qualité de mineur, majeur ou majeur incapable⁴⁴⁹ de son cocontractant. La question de l'identification en ligne des mineurs, est un élément crucial dans l'analyse des contrats électroniques qu'il est susceptible de conclure dans le cyberspace. Une évolution de la technologie dans le sens d'une identification “sûre“ de son interlocuteur en tant que mineur par exemple supposerait que le cocontractant révèle des aspects contrôlables de sa personnalité⁴⁵⁰. Une telle possibilité repose sur la collecte des données personnelles et de l'usage qui en est fait.

La considération de la capacité juridique est importante, étant donné que le réseau est couramment utilisé par des mineurs, très au fait des procédures permettant d'avoir accès à tout site y compris ceux qui leur sont interdits du fait de leur âge, et de passer des contrats alors qu'ils ne devraient pas pouvoir le faire⁴⁵¹. En principe le droit français dispose de nombreux outils propres à rassurer les parents quant à la possibilité qu'ont leurs enfants mineurs de conclure des contrats à leur insu. Le droit français pose le postulat selon lequel l'incapacité juridique des mineurs les empêcherait de contracter⁴⁵². Toutefois, depuis quelques années, la jurisprudence a traduit les évolutions sociales ; appliquant les articles 389-3 et 450 du code civil qui autorisent le mineur à accomplir seul les actes admis par la loi ou l'usage, les juges ont admis la validité d'un certain nombre d'actes qualifiés d'« actes de la vie courante ».

Le mineur ne possède pas une pleine capacité contractante : sa capacité contractante est restreinte. Pour déterminer si un mineur dispose de cette capacité contractante restreinte, deux éléments doivent être pris en compte : son âge et sa capacité de discernement. En effet, un mineur de moins de 14 ans a une meilleure capacité de discernement qu'un enfant âgé de

⁴⁴⁸ Le Droit de l'Achat en ligne, Un mineur peut valablement contracter, même lors d'un achat en ligne, Fabrice Wang, 30 novembre 2004, http://www.droitail.net/article.php3?id_article=18

⁴⁴⁹ Travaux de l'association Henri Capitant, Le contrat électronique ; Arnaud Raynouard, La formation du contrat électronique, Journées nationales Tome V – Toulouse 2000, Edition Panthéon Assas, LGDJ, p.16. – Céline Halpern, Droit et Internet, Editions de Vecchi, p.28.

⁴⁵⁰ Céline Halpern, Droit et Internet, op.cit., p.28.

⁴⁵¹ Ibid.

⁴⁵² Article 1124 du code civil : « *Sont incapables de contracter, dans la mesure définie par la loi :*

Les mineurs non émancipés ;

Les majeurs protégés au sens de l'article 488 du présent code ».

7 ans. Dans de nombreux pays, les enfants de moins de 7 ans ne disposent d'ailleurs d'aucune capacité contractante. Des nuances existent entre les pays de l'Union européenne. La notion de capacité contractante restreinte existe dans la plupart des pays. Elle permet aux mineurs de conclure uniquement des contrats qui sont à leur avantage ou des contrats portant sur une somme d'argent limitée⁴⁵³. Dans la plupart des pays, les parents doivent toujours entériner un contrat conclu par leur enfant mineur sous peine de nullité dudit contrat.

Pour reconnaître aux mineurs le droit de contracter pour des actes de la vie courante, trois conditions doivent être réunies : l'acte doit être autorisé par l'usage, avoir une faible valeur pécuniaire et être couramment effectué par un mineur agissant seul. L'appréciation au cas par cas reste néanmoins très subjective. Cette appréciation est particulièrement difficile dans le cyberspace qui est un média relativement nouveau et en constante mutation. Quels sont les actes conclus par le mineur sur Internet pouvant satisfaire à ces critères ? Selon quels critères pourra-t-on classer des actes comme appartenant à la vie courante ou comme étant d'usage dans le cyberspace.

Dans leur majorité, les contrats électroniques conclus dans le cyberspace sont des contrats de vente. Selon les critères posés par le droit commun des contrats (article 1108 du code civil), pour qu'un acte conclu par un mineur sur Internet soit valable, il ne faut pas que son objet soit illicite, onéreux et il doit constituer une transaction courante pour un mineur. S'agissant de licéité de l'objet il ne se pose pas de difficulté majeure. S'agissant par contre de l'appréciation de la faible valeur pécuniaire quel est le seuil qui permet de déterminer qu'un bien est ou non peu coûteux ? Cela n'est mentionné nulle part, on peut donc supposer que cette appréciation est laissée à qui aura à connaître de la validité du contrat conclu par un mineur. L'acte doit être couramment effectué par un mineur agissant seul, qui est juge de cette appréciation et selon quels critères ?

⁴⁵³ Récemment, les Centres Européens des Consommateurs ont reçu de nombreuses plaintes à l'encontre de la société Iglusoft Mediem GmbH (www.eusms.com) qui offre sur son site 99 sms gratuits. Il s'agissait en réalité d'un abonnement dont les frais d'installation s'élevaient à environ 100€. Cet abonnement « offrait » 99 sms, les sms suivants étant payants. De nombreux mineurs ont inscrit leurs coordonnées sur le site et ont par conséquent conclu un contrat sans s'en rendre compte. Outre le fait qu'il s'agit d'une publicité trompeuse, la validité d'un tel contrat peut être contestée étant donné que les mineurs ne disposent en principe pas de la capacité contractante. Dans le cas présent, la validité de ce type de contrats peut être mise en cause dans la mesure où il s'agit d'un contrat continu, conclu pour une durée indéterminée et qui représente un risque financier pour le mineur. Voir le site European Consumer Centre Belgium : http://www.eccbelgium.be/FR/infocenter/news_detail.asp?h=10&nID=304

Tous les pays connaissent l'incapacité de contracter dérivant de la minorité du mineur, mais ils ne fixent pas l'âge de celle-ci de manière uniforme non plus que la sanction qui l'assortit⁴⁵⁴.

Quels rôles doivent jouer les parents ou tuteurs légaux dans la conclusion de contrats électroniques par les mineurs ? Pour qu'un contrat conclu par un mineur soit valide, il est nécessaire en principe qu'il soit contresigné par le parent ou tuteur légal du mineur. Dans le "monde réel", la matérialité de cette contre signature est aisément vérifiable ce qui n'est pas le cas dans le cyberspace. La meilleure solution est l'utilisation de la signature électronique sécurisée pour s'assurer de l'identité et de la capacité juridique de son cocontractant.

La signature électronique est régie par la loi du 13 mars 2000⁴⁵⁵. Cette loi a reconnu à la signature électronique la même valeur qu'à la traditionnelle signature manuelle. Cette loi est une transposition de la directive européenne 1999/93/CE de décembre 1999⁴⁵⁶, elle a donné lieu à des adaptations dans le code civil : l'article 1316-4 du code civil relatif à la signature électronique⁴⁵⁷. Un décret 2001-272 du 30 mars 2001⁴⁵⁸ indique la procédure à suivre et le dispositif pour créer et vérifier une signature électronique⁴⁵⁹.

Le décret 2001-272 du 30 mars 2001, donne la définition d'une signature électronique sécurisée⁴⁶⁰ ; il énonce les dispositifs sécurisés de sa création, les dispositifs de vérification. En son chapitre III le décret 2001-272, régit la matière des certificats électroniques qui doivent être délivrés par des prestataires de service et de certification électronique.

⁴⁵⁴ Xavier Linant de Bellefonds, Le droit du commerce électronique, Que-sais-je ? PUF 2005, p. 37.

⁴⁵⁵ Loi n° 2000-230 du 13 mars 2000 : http://www.legifrance.gouv.fr/html/frame_jo.html

⁴⁵⁶ Directive 1999/93/CE <http://www.marianne-village.fr/reglement/SMW00363.htm>

⁴⁵⁷ Article inséré par Loi n° 2000-230 du 13 mars 2000 art. 4 Journal Officiel du 14 mars 2000. « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat ».

⁴⁵⁸ Décret n° 2001-272 du 31 mars 2001 : http://www.legifrance.gouv.fr/citoyen/jorf_no.ow?numjo=JUS

⁴⁵⁹ Magali Jakusic, Historique de la loi sur la signature. <http://www.securite.teamlog.com/publication/3/4/53/index.html>

⁴⁶⁰ Pour être comme une signature électronique sécurisée, la signature doit être propre au signataire, être créée par des moyens que le signataire peut garder sous contrôle exclusif, garantir avec l'acte auquel elle s'attache un lien que toute modification ultérieure de l'acte soit détectable. Il faut entendre par signataire toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de la signature électronique.

Ces deux dispositifs (la signature électronique sécurisée et le certificat électronique) ont pour double objectif de garantir l'identité de l'internaute d'une part et d'autre part l'authenticité et la validité des actes qu'il réalise dans le cyberspace. Cela permettrait de résoudre la question de l'identification des mineurs et les problèmes découlant de leur incapacité à conclure des actes juridiques dans le cyberspace.

Il existe deux types d'incapacité : une incapacité d'exercice et une incapacité de jouissance⁴⁶¹. Bien que le mineur puisse réunir les deux incapacités, nous n'allons retenir que l'incapacité d'exercice. Elle suppose que l'intéressé n'est pas privé du droit de contracter, mais qu'il ne peut lui-même exercer ce droit : il doit être assisté par un tiers ou représenté. Les contrats ainsi conclus sont parfaitement valables et produisent leurs effets dans le patrimoine de l'incapable (en l'occurrence le mineur) comme si il les avait conclus lui-même : c'est donc lui qui deviendra créancier ou débiteur des obligations contractuelles⁴⁶².

La jurisprudence a atténué le principe légal selon lequel un mineur ne peut pas valablement conclure un contrat. La cour de cassation avait rejeté le motif de minorité que le contractant mineur avait opposé, pour se soustraire à sa responsabilité dans le cadre d'un contrat qu'il avait lui-même conclu⁴⁶³. Comme le droit commun s'applique au cyberspace, on peut en conclure que le mineur peut valablement contracter en ligne quoique dans certaines limites.

2. La sanction de l'incapacité juridique du mineur.

Le mineur en dessous d'un certain âge serait soumis à une incapacité générale. Dans cette phase le mineur ne pourrait s'obliger à aucun contrat. Un tel contrat serait nul de nullité absolue. Une interrogation demeure quant à la détermination de l'âge de référence pour mettre en œuvre cette incapacité absolue. L'âge de 13 ans retenu par l'ordonnance du 2 février 1945 alinéa 2 comme minimum en dessous duquel il ne peut y avoir de responsabilité pénale, serait trop élevé pour le droit civil et le droit commun des contrats⁴⁶⁴. A l'inverse, l'âge de 7 ans

⁴⁶¹ Une incapacité de jouissance est une interdiction de conclure un contrat en particulier, l'intéressé ne peut exercer son droit par autrui, il est purement et simplement privé de ce droit, cf. Hubert Bitan dans Contrats électroniques, Litec, Editions du Juris-Classeur.

⁴⁶² Hubert Bitan, Contrats informatiques, op.cit, p. 43.

⁴⁶³ Cass. Civ. 1^{ère}, 4 novembre 1970, JCP 1971 II 16631. Les faits : un mineur souscrit un contrat de location d'un véhicule de tourisme. A la suite d'un accident de la circulation, le véhicule est endommagé. La société de location lui demande de payer les réparations vu que le jeune homme n'avait souscrit qu'une assurance au tiers. Ce dernier refuse au motif que le contrat de location n'était pas valablement formé compte tenu de sa minorité ; par conséquent il ne devait pas assurer les réparations du véhicule endommagé. Solution : la Haute juridiction rejette le motif minorité.

⁴⁶⁴ Jean Carbone, Droit civil Tome 2, op.cit., p. 132

visé trop bas. Il faut s'en remettre alors au cas par cas, prendre en considération tous les éléments et les circonstances particulières comme dans le cas de contrats électroniques.

La doctrine a considéré quelquefois que l'acte accompli par un enfant privé de discernement en raison de son âge devait être nul de nullité absolue pour absence de consentement⁴⁶⁵. Seulement la nullité d'un acte pour incapacité visait à protéger le contractant dont la volonté n'avait pas été libre. Un mineur qui a conclu un contrat ne l'a pas nécessairement fait sous la contrainte ou par manque de discernement ou en étant victime d'un dol. Comment appliquer au contrat conclu une nullité absolue sans autre considération ? Intervient alors une idée de nullité relative pouvant être invoquée par l'auteur de l'acte ou par son représentant, administrateur légal ou tuteur.

Le contrat électronique ne peut en principe pas prospérer si l'incapacité d'un des cocontractants est connue des deux parties. Le vendeur qui prend connaissance de l'incapacité est en droit de récupérer le produit vendu en restituant le prix⁴⁶⁶ perçu. La nullité des actes juridiques accomplis par un mineur est une mesure de protection nécessaire ; cette nullité reste encourue en cas de fausse déclaration de majorité⁴⁶⁷, les intérêts de l'incapable sont supérieurs à ceux du tiers⁴⁶⁸.

Les actes accomplis par le mineur ne sont pas nuls sans distinction, la nullité peut être subordonnée à une lésion⁴⁶⁹, c'est-à-dire que l'acte a été conclu sous des conditions anormales laissant penser que l'on a profité de l'inexpérience du cocontractant, ou qu'il est inutile ou disproportionné aux moyens du mineur⁴⁷⁰ (article 1305 et suivant et du code civil)⁴⁷¹.

Le fait qu'un mineur ait indiqué son âge lors d'une commande ne suffit pas à annihiler la possibilité d'annuler le contrat pour incapacité. Qu'en est-il lorsque le fournisseur a négligé

⁴⁶⁵ Christian Larroumet, *Droit civil. Les obligations. Les contrats*, Tome 3, Economica 3^e Edition 2003, p. 289. – Le mineur est de plein droit incapable, sans qu'il y ait lieu de provoquer une intervention judiciaire à cette fin, art. 488 du code civil.

⁴⁶⁶ Xavier Linant de Bellefonds, *préc.*, p. 38.

⁴⁶⁷ Art. 1307 du code civil.

⁴⁶⁸ Florence Laroche Gisserot, *Les droits de l'enfant*, 2^e Edition Dalloz, *Connaissances du droit*, p. 42.- Cour de cassation, chambre criminel, 30 mars 1999, *Dalloz*. 1999, IR 130 ; un mineur avait usurpé une fausse identité.

⁴⁶⁹ Christian Larroumet, *op.cit.*

⁴⁷⁰ Florence Laroche Gisserot, *Les droits de l'enfant*, *op.cit.*

⁴⁷¹ Article 1305 issu de la Loi n° 64-1230 du 14 décembre 1964 *Journal Officiel* du 15 décembre 1964 en vigueur le 15 juin 1964 ; « La simple lésion donne lieu à la rescision en faveur du mineur non émancipé, contre toutes sortes de conventions ».

de vérifier une mention relative à l'âge destinée à établir l'incapacité de son client⁴⁷². Cependant l'absence de mentions relatives à l'âge conduisant à l'impossibilité pour le vendeur de vérifier la capacité de son client aboutit à l'application de la théorie de l'apparence : l'obligation d'honorer le montant de la transaction retombe sur les parents du mineur. Par ce biais on entend indirectement contraindre les parents des mineurs à limiter l'activité de ces derniers sur Internet par le biais de logiciels restreignant l'accès aux sites marchands⁴⁷³ ou du moins à prendre leurs responsabilités par rapport aux actes posés par leurs enfants mineurs dans le cyberspace.

En tout état de cause, les parents ne peuvent être tenus responsables des obligations nées de contrats passés par leur enfant mineur, que ce soit ou non dans le cadre des actes de la vie courante. Dès lors, le cocontractant d'un mineur doit vérifier, avant de s'engager, la capacité juridique de la personne qu'il a en face de lui. Est-ce à dire que tous les risques pèsent sur le cocontractant du mineur qui n'a pas recherché ou qui n'a pas su ou pu déterminer la minorité et donc l'incapacité juridique à contracter de ce dernier? Le parent ou tuteur légal est responsable des dommages que le mineur a infligés à autrui conformément à l'article 1183 du code civil. Peut-on assimiler le fait que le cocontractant du mineur n'ait pas été en mesure de déterminer sa minorité comme un fait dommageable ? Assurément pas. La minorité d'un cocontractant ne génère pas nécessairement la nullité du contrat. La nullité pour erreur sur la personne ne peut être invoquée que pour les contrats conclus *intuitus personae*.

En définitive, force est de constater qu'aucun texte n'a expressément réglé la question de la capacité ou plutôt de l'incapacité contractante du mineur en ligne. Ce contrat est nul selon le droit commun ce qui représente un risque considérable pour les entreprises dépendantes du commerce électronique⁴⁷⁴. Dans la pratique (en cela Internet s'aligne sur le droit commun), on admet que le mineur puisse conclure des contrats en ligne mais avec le concours et l'autorisation des parents (même si ce n'est pas souvent le cas notamment pour des transactions d'un faible montant). Dès lors que l'on admet que le mineur peut conclure des contrats électroniques, se pose la question de leurs conditions de validité comme pour tout autre contrat.

⁴⁷² Florence Laroche Gisserot, Les droits de l'enfant, op.cit.

⁴⁷³ Ibid.

⁴⁷⁴ Philippe Le Tourneau, Contrats informatiques et électroniques, Dalloz 3^e édition, p.294.

B. La validité intrinsèque du contrat électronique.

Le contrat qu'il soit électronique ou non obéit aux normes posées par l'article 1108 du code civil : le consentement, la capacité des cocontractants, la cause et l'objet du contrat⁴⁷⁵.

L'objet du contrat. Pour être valide, un contrat doit avoir un objet déterminé, licite et qui est dans le commerce. L'extranéité d'Internet pose encore quelques problèmes ; la licéité d'un objet varie selon les législations nationales. Certains objets font cependant l'objet d'une condamnation générale, à l'instar des stupéfiants.

La cause du contrat. Elle doit être existante et licite. A la différence de l'objet illicite, la cause illicite procède du caractère illicite de la motivation du débiteur de l'obligation.

1. Le consentement du mineur dans un contrat électronique

Le consentement résulte de la rencontre de volontés allant dans le même sens. Dans le cas d'Internet, ces volontés successives sont enfermées dans des messages. La question est de savoir sous quelles formes et à quel moment le contrat se forme⁴⁷⁶. A quel moment peut-on considérer que le consentement du mineur est manifeste. Dans le cas du contrat électronique, la formation du contrat est dématérialisée, elle s'opère par un ou des gestes électroniques. Pour autant le consentement reste de même nature que celui qui est donné sur un support papier ou verbalement. La formation du contrat si elle peut-être quasiment instantanée, implique en réalité une série d'opérations électroniques caractérisant la réalité du consentement⁴⁷⁷.

La LCEN en son article 19 et le code civil en son article 1369-2, posent des exigences juridiques à la validité du contrat. D'aucuns considéreront qu'un message d'acceptation d'un client suivant un message d'offre d'un fournisseur établit théoriquement la formation du contrat⁴⁷⁸. L'internaute manifeste son intention de contracter en adressant sa commande au vendeur par voie numérique. Ce dernier doit en accuser réception, notamment par e-mail, dans les meilleurs délais. Grâce à cette formalité, l'internaute a la certitude que son intention

⁴⁷⁵ Céline Halpern, op.cit, p.27-28.

⁴⁷⁶ Travaux de l'association Henri Capitant, Le contrat électronique, Journées nationales Tome V Toulouse 2000, Editions Panthéon Assas, LGDJ, p. 15.

⁴⁷⁷ Philippe Le Tourneau, Contrats informatiques et électroniques, op.cit, p.293.

⁴⁷⁸ Xavier Linant de Bellefonds, Le droit du commerce électronique, op.cit, p. 38-39.

de contracter a bien été prise en compte. Le cocontractant (souvent le vendeur) lui adresse ensuite sur un support durable, un récapitulatif confirmant les caractéristiques de l'objet du contrat, son prix, ainsi que les informations relatives au service après-vente et aux garanties commerciales⁴⁷⁹. Ce récapitulatif mentionne également le délai de rétractation de sept jours et permet à l'internaute de vérifier les clauses du contrat avant de donner son accord définitif. Il lui restera alors à réitérer matériellement son consentement par le procédé du double clic⁴⁸⁰. S'agissant de la matérialisation du consentement du mineur et sachant qu'il ne peut en principe conclure de contrat sans le consentement de ses parents, lequel des consentements (le sien ou celui du parent ou tuteur légal) conclura effectivement le contrat du mineur ? Le double-clic final synonyme de conclusion du contrat électronique conclu par le mineur revient-il à ce dernier ou au parent ou tuteur légal ?

Le code civil retient que le consentement n'est pas valable s'il a été donné par erreur, extorqué par violence ou surpris par dol⁴⁸¹. Un contrat qui aurait été conclu dans ces conditions s'expose à l'annulation. Il s'agit là de critères de consentement général. Il n'est pas fait de mention spécifique au mineur.

2. L'effectivité de la formation du contrat électronique conclu par un mineur : le double clic

La loi n°2000 -230 du 13 mars 2000 a donné à l'écrit sur support électronique la même valeur probatoire que l'écrit sur support papier (écrit *ad probationem*)⁴⁸². La question ne se pose plus de la validité contractuelle des écrits sur support électronique. Ceci étant, l'écrit sur support électronique doit remplir deux conditions conformément à l'article 1316-1 du code civil :

- « *que puisse être dûment identifiée la personne dont il émane* »
- « *qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

A ce stade l'écrit sur un support électronique peut être constitutif de la preuve d'un contrat électronique. La loi sur la confiance dans l'économie numérique du 21 juin 2004 a consacré quant à elle le principe de la preuve de l'écrit *ad validitatem*.

⁴⁷⁹ La revue d'information juridique pour les particuliers, IntérêtsPrivés.com, Conclure un contrat électronique. <http://interetsprives.grouperf.com/article/0626/ms/intprim0626intcon01.html>

⁴⁸⁰ Il a cliqué une première fois pour passer commande, et clique une deuxième fois pour valider cette commande.

⁴⁸¹ Article 1109 du code civil.

⁴⁸² L. n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature, JO 14 mars p.3968.

La détermination du moment de la formation du contrat est liée à des questions purement techniques. La détermination du moment de formation du contrat revêt une grande importance pour les deux parties. « *Si un incident devait se produire dans la communication, il est nécessaire de décider dans quelle mesure le contrat est déjà formé, nonobstant le défaut de réception du message d'acceptation* »⁴⁸³. La théorie de l'émission préserve les droits de l'acceptant ; il lui sera inopposable, la rétractation opérée par le pollicitant pendant l'incident technique ou la caducité de l'offre. Cette théorie facilite « la preuve de la formation du contrat et des conditions auxquelles il a été conclu », l'acceptant détenant dans sa messagerie, son ordinateur, la matérialité de l'émission du message d'acceptation et l'étendue de son contenu⁴⁸⁴. Ainsi, ce dernier n'est pas à la merci de l'arbitraire de son partenaire. Les auteurs de la directive n° 2000/31/CE du 8 juin 2000 ont opté pour ce mécanisme.

Le clic fait partie de la terminologie informatique. C'est l'acte qui consiste par une pression sur la souris à sélectionner un élément sur son écran. Le double-clic qui consiste en une double pression sur la souris permet de fixer le moment de la conclusion d'un accord sur Internet.

2.a. La vérification de la commande.

La directive prévoit que le contrat est conclu lorsque le destinataire de l'offre a émis son acceptation, ce après avoir eu la possibilité de vérifier le détail de sa commande et son prix total, ainsi que d'en corriger les éventuelles erreurs afin de confirmer celle-ci pour exprimer son acceptation⁴⁸⁵. Pour ce faire, le cybermarchand doit fournir au consommateur les moyens techniques lui permettant de vérifier sa commande, notamment le détail et le prix⁴⁸⁶ de l'objet du contrat. Cette mesure est d'ordre public sauf entre des professionnels qui peuvent y déroger⁴⁸⁷. Le procédé du « double clic » reçoit ainsi sa consécration légale.

⁴⁸³ L. Grynbaum, Contrats entre absents : les charmes évanescents de la théorie de l'émission de l'acceptation, Dalloz 2003, chronique, p. 1707.

⁴⁸⁴ L. Grynbaum, préc.

⁴⁸⁵ Directive du 8 juin 2000, art. 11 point 2, article 1369-5 al. 1 nouveau inséré par ordonnance du 16 juin 2005, - code civil art. 1369-2 al.1^{er} ancien issu de la loi pour la confiance dans l'économie numérique art. 14.

⁴⁸⁶ Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, op.cit, p.201.

⁴⁸⁷ Code civil art 1369-3 al. 2.

2.b. La confirmation de la commande.

La théorie de l'émission en sort enrichie : l'acceptation ne produit d'effet que si elle est vérifiée et confirmée⁴⁸⁸. La loi prévoit que le destinataire de l'offre doit confirmer sa commande pour exprimer son acceptation⁴⁸⁹. On peut supposer que, dans le cas du mineur c'est à ce moment que le parent ou tuteur légal doit intervenir pour confirmer les velléités contractuelles du mineur en y apportant sa caution, ce faisant il valide le contrat conclu par le mineur.

2.c. L'accusé de réception.

Il est précisé que le prestataire est tenu d'accuser réception de la commande sans délai injustifié et par voie électronique⁴⁹⁰. Cet accusé de réception n'a pour l'heure qu' « un rôle purement technique, dépourvu de toute valeur contractuelle »⁴⁹¹. Il s'agit simplement d'une étape technique qui n'est aucunement liée au lien contractuel résultant de l'acceptation par le client de l'offre du cybermarchand. Il permet uniquement (pour l'heure en tout cas) d'avoir confirmation que la commande a bien été prise en compte par le cybermarchand⁴⁹².

La commande, la confirmation de l'acceptation de l'offre et l'avis de réception sont considérés comme reçus, lorsque les parties auxquelles ils ont été adressés peuvent y avoir accès.

Dans certaines hypothèses juridiquement encadrées, le mineur peut conclure des contrats électroniques. Il est titulaire de droits et d'obligations découlant de cette faculté. Comme toute personne juridique, les droits dont il dispose ont pour corollaire une responsabilité envers autrui dans le cyberespace.

⁴⁸⁸ Philippe Le Tourneau, Contrats informatiques et électroniques, préc., p. 293. - Xavier Linant de Bellefonds, Le droit du commerce électronique, op.cit, p. 41.

⁴⁸⁹ Code civil article 1369-5 al. 2 nouveau, inséré par l'ordonnance du 16 juin 2005 – code civil article 1369-2 al.2 issu de la LCEN du 21 juin 2004.

⁴⁹⁰ Directive 8 juin 2000, art.11 point 1 1^{er} tiret.

⁴⁹¹ Avis n° 608, présenté par Mme Michèle Tabarot, député, au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n°528) pour la confiance dans l'économie numérique, 11 février 2003, p.61. www.assemblee-nationale.fr

⁴⁹² Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, Dalloz 2006, p.201.

3. La sanction des contrats électroniques illégalement conclus par un mineur.

La sanction d'un contrat électronique illégalement conclu par un mineur est l'annulation⁴⁹³. L'incapacité juridique du mineur n'est pas seule prise en compte pour aboutir à cette sanction suprême. En droit commun, les articles 1305 et 1311 du code civil statuent sur la sanction de l'incapacité juridique du mineur. En deux hypothèses, la loi se réfère implicitement aux pouvoirs du tuteur.

- Le mineur agissant seul a fait un acte qu'un tuteur n'aurait pu faire valablement qu'avec l'autorisation du conseil de famille (article 457). C'est le type d'acte le plus grave, pour lesquels la sanction serait la nullité relative si le tuteur avait opéré seul (article 1311). Le juge doit prononcer la nullité sans apprécier si l'opération était bonne ou mauvaise.
- Le mineur agissant seul a fait un acte que le tuteur aurait pu faire sans formalité, sans le minimum de formalités, c'est-à-dire sans l'autorisation du conseil de famille. L'acte ainsi accompli n'est pas nécessairement nul. On recherche si le mineur a subi une lésion.

Le mineur est amené à logiquement engagé sa responsabilité du fait de ses activités contractuelles dans le cyberspace. Cette responsabilité découle automatiquement du préjudice dont autrui peut être la victime, que l'action du mineur ait été volontairement ou non préjudiciable. Le fait qu'il exerce ses droits et libertés fondamentaux ne le dispense pas d'engager sa responsabilité en cas de préjudice.

§2. Les responsabilités du mineur découlant de l'exercice de ses droits et libertés fondamentaux dans le Cyberespace.

⁴⁹³ L'arrêt de principe en matière de nullité de droit, date du 25 mars 1861 et précise que si le mineur fait seul un acte de disposition, l'acte est nul en la forme, d'une nullité relative, sans qu'il y ait à apprécier si l'opération était bonne ou mauvaise ; Cass. Civ., 25 mai 1861.

Le mineur comme toute personne physique dotée de droits et de devoirs se voit opposer le respect du droit. Il ne peut en principe pas y déroger ; notamment selon le principe qui veut qu'en droit français « nul n'est censé ignorer la loi ». Le cyberspace n'est pas une zone de non droit contrairement à ce que certains libertaires du Net ont cru pouvoir proclamer⁴⁹⁴, encore moins un espace qui n'obéit qu'à des règles qui lui sont spécifiques. La question n'est pas de savoir si le droit s'applique à Internet mais plutôt quel droit s'y applique. Pour cela il faut tenir compte de nombreux critères : la spécificité de la matière en cause par rapport au droit commun, la localisation géographique, la nature de la personnalité juridique de l'internaute concerné, etc.

Tout ce qui est illégal en droit commun l'est également dans le cyberspace. Dans la plupart des cas, une infraction ou un délit qui prend naissance dans le cyberspace (le monde virtuel) se prolonge dans le monde réel ; ou alors une infraction ou un délit qui a pris naissance dans le monde réel peut se prolonger ou se trouver aggravé par l'utilisation d'Internet.

La personnalité juridique du mineur a été conçue pour l'essentiel sur le postulat de sa vulnérabilité. Le mineur n'en est pas pour autant exonéré de toute responsabilité dans le cyberspace. Il est un acteur à part entière du cyberspace, sa liberté d'agir doit s'accompagner de l'engagement de sa responsabilité.

A. La responsabilité pénale du mineur dans le cyberspace.

L'âge de la majorité pénale est l'âge à partir duquel un délinquant relève du droit pénal commun ; il est fixé à dix-huit ans dans presque tous les pays européens⁴⁹⁵. En revanche l'âge de la responsabilité pénale c'est l'âge à partir duquel les mineurs sont considérés comme suffisamment âgés pour pouvoir commettre une infraction et pour être soumis à un droit pénal qui leur est spécifique. Cet âge varie beaucoup selon les pays européens⁴⁹⁶. Il peut arriver que ces deux âges coïncident. L'âge pris en compte pour la responsabilité pénale du mineur est

⁴⁹⁴ De l'avis de A. Lepage, « Certains zéloteurs d'un Internet affranchi des contraintes du monde "réel" auraient vu bon d'un bon œil que le droit se tint à l'écart du réseau [...] Internet n'est sûrement pas une zone de non droit, pour autant il n'est pas nécessairement une zone de droit spécifique », voire « Libertés et droits fondamentaux à l'épreuve d'Internet », op.cit, p.3

⁴⁹⁵ C'est le cas en Allemagne, en Angleterre et Pays de Galles, en Belgique, en France, en Italie, aux Pays-Bas et en Suisse. En Espagne il est de seize ans ; mais un projet de loi visant à le porter à dix-huit est en examen. Au Portugal, le code pénal n'est pas applicable aux jeunes de seize à vingt-et-un ans.

⁴⁹⁶ Bienvenu au Sénat, « *La responsabilité pénale des mineurs* », http://www.senat.fr/lc/lc52_mono.html

celui qu'il avait à la date de commission de l'infraction et non celui qu'il a au moment de son arrestation.

Il existe deux écoles s'agissant de la responsabilité pénale du mineur.

- La première école, celle de l'irresponsabilité absolue regroupe l'Angleterre, le Pays de Galles, l'Espagne, les Pays-Bas, le Portugal et la Suisse. Elle prône le fait que, le mineur qui n'a pas atteint l'âge de la responsabilité pénale ne peut en aucun cas être considéré comme pénalement responsable⁴⁹⁷.
- La deuxième école, celle de l'irresponsabilité pénale relative regroupe, la France, l'Allemagne, la Belgique et l'Italie. Dans ces pays, le mineur qui n'a pas atteint l'âge de la majorité pénale est présumé irresponsable. Cependant, à partir d'un âge inférieur à celui de la majorité pénale, sa responsabilité pénale peut être mise en jeu si certaines circonstances sont réunies⁴⁹⁸.

1. Le droit commun de la responsabilité pénale du mineur.

La responsabilité pénale de droit commun du mineur a pour l'essentiel été établie par l'ordonnance n° 45-174 du 2 février 1945 relative à l'enfance délinquante. Cette ordonnance pose les critères de la responsabilité : l'âge de la responsabilité pénale du mineur, les mesures et les peines qui lui sont applicables.

1-a. L'âge de la responsabilité pénale.

L'article 122-8 du code pénal pose le principe de l'irresponsabilité pénale absolue du mineur de moins de treize ans. Les mineurs « délinquants » de moins de treize ans ne peuvent faire l'objet que de « mesures de protection, d'assistance, de surveillance et d'éducation ». A

⁴⁹⁷ Bienvenu au Sénat, « *La responsabilité pénale des mineurs* », http://www.senat.fr/lc/lc52_mono.html. Dans ces cinq pays, l'âge de la responsabilité varie entre sept et seize ans : il est de sept ans en Suisse, dix ans en Angleterre et au Pays de Galles, douze ans aux Pays-Bas, seize ans en Espagne et au Portugal.

⁴⁹⁸ L'âge de l'irresponsabilité pénale relative varie : il est de treize ans en France, de quatorze ans en Allemagne et en Italie et de seize ans en Belgique. Les circonstances qui permettent de déroger à la présomption d'irresponsabilité des mineurs varient également. L'Allemagne et l'Italie retiennent un critère d'ordre essentiellement moral : la première évoque la maturité et le discernement du jeune délinquant, et la seconde sa « capacité de vouloir et de comprendre ». La Belgique et la France insistent sur l'adéquation des mesures que peuvent prendre les tribunaux spécialisés. Bienvenu au Sénat, « *La responsabilité pénale des mineurs* », op.cit. http://www.senat.fr/lc/lc52_mono.html

contrario, le mineur de plus de treize ans peut parfaitement voir sa responsabilité pénale engagée⁴⁹⁹.

1-b. Les mesures applicables aux mineurs.

Les mesures ou sanctions qui peuvent être prises à l'encontre du mineur sont de différentes natures :

1.b'. Les mesures éducatives.

Le juge pour enfants peut imposer plusieurs mesures à l'encontre du mineur conformément à l'article 8 de l'ordonnance de 1945 relative à l'enfance délinquante :

- Une dispense de peine ; ce dans la mesure où le dommage causé a été réparé et que le trouble résultant de l'infraction a cessé.
- L'admonestation
- La remise aux parents, au tuteur, à la personne qui a la garde de l'enfant ou à une personne digne de confiance
- La mise sous protection judiciaire pour une durée n'excédant pas cinq ans.
- Le placement dans une institution ou un établissement public ou privé, d'éducation ou de formation professionnelle, dans un établissement médical ou médico-pédagogique, dans un internat approprié ou, pour les mineurs de moins de treize ans, la remise au service de l'assistance de l'enfance.
- La liberté surveillée jusqu'à un âge qui ne peut excéder la majorité.

1.b''. Les mesures de médiation – réparation.

Le mineur doit alors participer à la réparation du dommage qu'il a causé en effectuant une activité d'aide ou de réparation au profit de la victime ou dans l'intérêt de la collectivité. Cette mesure ne peut être ordonnée qu'avec l'accord de la victime, et peut être accompagnée d'excuses adressées à cette dernière. De surcroît, il peut être prononcé pour les mineurs entre seize et dix-huit ans une obligation d'effectuer des travaux d'intérêt général « *présentant un caractère formateur ou de nature à favoriser l'insertion sociale* ».

⁴⁹⁹ L'article 2 de l'ordonnance de 1945 relative à l'enfance délinquante précise que le tribunal pour enfants et la cour d'assise des mineurs « pourront cependant, lorsque les circonstances et la personnalité du délinquant leur paraîtront l'exiger, prononcer à l'égard du mineur âgé de plus de treize ans une condamnation pénale ».

1.b'''. Les mesures d'enfermement.

La mesure ultime et la plus sévère qui puisse être prononcée à l'encontre d'un mineur de plus de treize ans est *la peine d'emprisonnement*. Cette peine ne peut pas être supérieure à la moitié de la peine encourue par un majeur pour la même infraction. Toutefois en cas d'extrême gravité, la peine infligée au mineur (entre treize et dix-huit ans) peut être la même que celle infligée à un majeur. Les mineurs effectuent leur peine dans des établissements spécialisés habilités à les recevoir, ou dans des quartiers séparés des maisons d'arrêt⁵⁰⁰.

2. Les hypothèses de responsabilité pénale du mineur dans le cyberspace.

Le mineur va engager sa responsabilité chaque fois qu'il commettra des actes délictueux dans le cyberspace. Sa responsabilité prend sa source dans le cyberspace et s'applique selon les règles du droit commun bien que l'on prenne en compte le caractère spécifique d'Internet. Il y a deux catégories d'infractions :

- Les actes délictueux communs qui ont été commis par le biais et/ou relayés par Internet. Ce qui peut s'avérer être un facteur aggravant.
- Les infractions qui sont spécifiques à Internet.

2-a. Les infractions communes commises via Internet ou aggravées par l'utilisation d'Internet.

La diffamation et l'injure sont des infractions sanctionnées dans la législation sur les infractions de presse. L'utilisation d'Internet a un caractère amplificateur de l'infraction du fait de la publicité et de la diffusion planétaire dont cet outil est porteur. Il était logique que la sanction de ces délits prenne en considération Internet comme un facteur aggravateur dont il doit être tenu compte lors du prononcé de la sanction de ces délits.

La sanction de l'utilisation d'Internet dans la commission des délits de négationnisme et d'incitation à la haine raciale obéit à la même logique. De manière générale, il faut noter que l'utilisation d'Internet est souvent retenue comme un caractère aggravant pour un délit qui préexistait au cyberspace.

⁵⁰⁰ La responsabilité pénale des mineurs, Le site du sénat. <http://www.senat.fr/lc/lc52/lc525.html>

Les pages personnelles et notamment les blogs sont un terrain propice aux infractions du type des atteintes à la vie privée et au droit à l'image. Dans la plupart des cas, il s'agit de la part des mineurs d'une infraction imputable à leur méconnaissance des règles juridiques applicables en la matière, sauf hypothèse où la nature de la photographie ou de l'information transmise par ce bien est manifestement infamante. Les blogs fourmillent de photographies de leurs auteurs, de leurs amis, familles, de personnes qui les accompagnent (connues d'eux ou non) sans que les éditeurs ne se soient préoccupés d'obtenir l'autorisation des personnes concernées. Ils partent du postulat que les personnes ne se sont pas dérobées à la caméra et parfois ont posées, que les photographies sont leur possession puisque faites par eux avec leur matériel. Ils s'estiment en droit de les publier librement dans leur blog, sans avoir conscience de contrevenir au droit à l'image d'autrui. Or, l'article 226-1 du code pénal incrimine le fait de fixer, d'enregistrer ou de transmettre sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. L'article 226-2 sanctionne de peines d'un an d'emprisonnement et 45 000 euros d'amende « le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1 ». Aucune disposition spécifique n'étant consacrée aux mineurs, on peut supposer qu'ils sont soumis aux mêmes règles sauf atténuation circonstanciée à leur âge. Ce n'est pas tant la fixation de l'image qui pose problème mais sa diffusion qui ce faisant, porte atteinte à l'intimité de la personne concernée. La cour d'appel de Paris, dans un arrêt du 22 mars 2005⁵⁰¹ a considéré que la personne qui diffuse sur un site Internet des photographies prises d'une autre personne dans son intimité, sans le consentement de cette personne, se rend coupable de l'infraction prévue par l'article 226-1 du code pénal.

2-b. Les infractions spécifiques à Internet.

Le mineur éditeur d'un blog peut être pénalement responsable conformément à l'article 122-8 du Code pénal. Cet article prévoit que, « les mineurs capables de discernement sont pénalement responsables des crimes, délits ou contraventions dont ils ont été reconnus coupables, dans des conditions fixées par une loi particulière qui détermine les mesures de protections, d'assistance, de surveillance et d'éducation dont ils peuvent faire l'objet ». Dans cette optique, cet article détermine également les sanctions éducatives qui peuvent être

⁵⁰¹ CA Paris, 11^e ch. A, 22 mars 2005, L. B.. c/ministère public et L. A..., Comm. com. électr. Novembre 2005, p.37.

prononcées à l'encontre des mineurs de dix à dix-huit ans, ainsi que les peines auxquelles peuvent être condamnés les mineurs de treize à dix-huit ans. Il est tenu compte de circonstances d'âge atténuant leur condamnation.

Le téléchargement illégal est né avec Internet. Les internautes qui le pratiquent vont chercher dans des fichiers mis en ligne des contenus qu'ils n'ont pas le droit de copier quel qu'en soit l'usage. Le téléchargement est possible grâce à la technique de la numérisation des contenus combinée à la technologie d'Internet. Les mineurs toujours au fait des nouveautés et possédant un portefeuille à capacité limitée, on fait du téléchargement un mode de consommation de la musique, du cinéma, des jeux vidéos et des logiciels. Ils téléchargent et échangent entre copains les dernières nouveautés, grâce à Internet.

La diffusion de virus suppose que l'auteur du virus infecte autant de systèmes et de matériels que possible. Internet est le moyen de diffusion le plus efficace et le plus rapide. On ne peut imaginer de grande incidence en termes de nuisance du virus sans le relais d'Internet. Dans la plupart des cas la messagerie électronique est le vecteur de prédilection de cette cybercriminalité. Du fait du grand volume des échanges faits par les mineurs ils véhiculent également par ce biais, volontairement ou non des virus.

Le piratage ; il faut entendre par là l'accession et le maintien frauduleux dans des systèmes de tiers afin de les altérer, de les piller, de les paralyser voire de les détruire. Il existe un véritable terrorisme propre à Internet. Des Pirates pour des raisons idéologiques, mercantiles ou par souci de l'exploit accompli, s'attaquent tous les jours à des systèmes protégés en cassant leurs codes de sécurité. Les pirates du Web ont comme dénominateurs communs : une très bonne connaissance des techniques de l'informatique, voire un réel talent novateur en matière de nouvelles technologies informatiques, le goût du défi, etc. Nulle mention n'est faite de la condition d'âge. C'est l'un des "cercles" où il est fait fi de l'âge du pirate, seule compte ses compétences. Il ne sera célébré, respecté que pour ses exploits accomplis.

Les infractions commises dans le cyberspace ou relayées par ce dernier engagent à chaque fois que cela est possible la responsabilité pénale du mineur et la sienne seule. Il arrive qu'il engage sa responsabilité alors même qu'il n'a commis aucune infraction : il engage alors sa responsabilité civile.

B. La responsabilité civile.

La responsabilité civile, c'est l'obligation pour une personne de réparer le préjudice qu'elle a causé à autrui par sa faute, par le fait ou la faute d'une autre personne ou par le fait d'un bien qu'elle a sous sa garde.

Longtemps ce fut un axiome que, l'enfant dépourvu de discernement était civilement irresponsable⁵⁰² ce, bien qu'il soit énoncé à l'article 1310 du code civil le principe de la capacité délictuelle du mineur sans distinction aucune entre les mineurs. Communément cependant, il convenait de ne pas l'appliquer à l'enfant trop jeune pour mesurer les conséquences de ses agissements. Il avait y avait un dommage matériellement causé, mais juridiquement aucune faute n'était retenu en l'absence d'une volonté raisonnable reconnaissable chez l'enfant. La jurisprudence viendra inverser cette tendance, la Cour de cassation par plusieurs arrêts rendus en 1984, a décidé que les juges du fond ne sont pas tenus de vérifier si le mineur dont la responsabilité est en question était capable de discerner les conséquences de son acte. Cela revient à admettre qu'une faute au sens des articles 1382 et 1383 du code civil peut être imputée au mineur⁵⁰³.

Le mineur peut voir sa responsabilité civile engagée à tout moment pour les dommages causés à autrui conformément à l'article 1382 du code civil. Il s'agit d'une responsabilité objective. Le mineur est civilement responsable des dommages qu'il cause quelle que soient son âge et sa capacité de discernement⁵⁰⁴. Le législateur n'a pas explicitement fixé l'âge de la responsabilité civile. Il revient au juge d'évaluer la capacité de l'enfant de discerner le bien du mal, capacité dont découlerait sa responsabilité civile. Dans sa majorité, la jurisprudence a

⁵⁰²Jean Carbonnier, Droit civil Tome 2, La famille, l'enfant, le couple, Thémis 2002, p.132

⁵⁰³ Si le mineur a subi le dommage, sa faute ou la faute de la victime, peut être invoquée à son encontre pour exclure ou diminuer son droit à réparation ; Si le mineur a causé le dommage, il peut être condamné personnellement à le réparer.

⁵⁰⁴ Cass. 9 mai 1984, 3 arrêts. La question de la responsabilité civile de l'enfant ainsi que celle de l'employeur sur son employé sont des questions très complexes qui ont été résolues par la Cour de cassation dans son arrêt Lemaire du 9 mai 1984. la Cour de cassation a reconnu la responsabilité civile du prévenu en affirmant que la cour d'appel, qui n'était pas tenue de vérifier si le mineur était capable de discerner les conséquences de son acte, a pu estimer sur le fondement de l'article 1382 du code civil que la victime avait concouru à la réalisation de son dommage. Cet arrêt est intéressant dans la mesure où il tranche la question de la responsabilité civile de l'enfant dans le sens où il la reconnaît dans une certaine mesure. Jurisclasseur Périodique 1984 N° 20255, note N. DEJEAN de LA BATIE. Dalloz 1984 N° 37 p. 525, conclusions Jean CABANNES, note F. CHABAS. Cahiers juridiques des assurances mutuelles agricoles, octobre 1984, P. 590, note Hubert GROUDEL. Répertoire du notariat Defrénois, 1984, p. 557, note Raymond LEGEAIS.

fixé l'âge de raison à sept ans. Pour un enfant jugé non doué de raison (*l'infans*), l'acte posé par ce dernier sera considéré comme un acte de force majeure. De ce fait toute demande d'indemnisation de la part de la victime contre l'enfant sera rejetée. Cependant, la preuve de l'état de raison de l'enfant n'est pas suffisante pour retenir sa responsabilité. Il doit être établi trois éléments essentiels de la responsabilité civile : la faute de l'enfant, le préjudice que la victime a subi et le lien de causalité entre la faute et le préjudice.

1. La responsabilité civile délictuelle ou quasi délictuelle du mineur dans le cyberspace.

Pour engager la responsabilité civile d'un mineur il faut au moins trois éléments selon l'article 1382 du code civil : le dommage, le fait générateur et le lien de causalité. La responsabilité civile du mineur sera rarement recherchée seule, car les mineurs sont dans leur majorité « insolvables »⁵⁰⁵.

Le dommage ou préjudice subi doit être certain, direct et déterminé pour pouvoir être réparable. Un préjudice déjà subi et qui peut être prouvé a un caractère certain. Cette certitude peut également s'étendre aux conséquences futures, dans la mesure où leur réalisation est inévitable. S'agissant du caractère direct, le dommage doit résulter directement du fait reproché au responsable.

Le fait générateur est le fait matériel qui est à l'origine de la responsabilité. Il peut être fondé sur la faute ou le risque. Le mineur peut commettre une faute envers autrui conformément à l'article 1382 du code civil. Il appartient à la victime de prouver la faute du mineur. La charge de la preuve reste inchangée dans le cyberspace avec la difficulté supplémentaire qui tient à la nature du cyberspace. La responsabilité du mineur peut également être fondée sur une absence de faute.

Le lien de causalité ; la responsabilité civile suppose un lien de cause à effet direct entre le fait dommageable et le préjudice. Le fait doit avoir provoqué le dommage. En cas de pluralité de causes, il ne peut être retenu que les causes principales. Par contre, en cas de pluralités d'auteurs, la victime peut en principe demander réparation à n'importe lequel des auteurs, leur responsabilité est solidairement engagée.

⁵⁰⁵ Code junior, Les droits et obligations des moins de dix-huit ans, Justice-Famille-Education-Société, Dalloz.

La force majeure, le fait d'un tiers ou la faute de la victime exonère totalement ou partiellement l'auteur du dommage de sa responsabilité.

Il existe trois types de responsabilités civiles : la responsabilité du fait personnel, la responsabilité du fait d'autrui (à l'instar de la responsabilité des parents du fait de leurs enfants mineurs) et la responsabilité du fait des choses qu'on a sous sa garde. Je retiendrais en l'espèce la responsabilité du fait personnel du mineur. Cette responsabilité pour faute (volontaire ou involontaire) comprend deux éléments :

- Un élément matériel qui est un agissement du mineur se traduisant par une action ou une abstention. Si c'est une action, elle peut également avoir des conséquences pénales (injures, diffamation, etc.). L'abstention se traduit généralement par une négligence.
- Un élément moral qui est caractérisé par une volonté libre et une conscience suffisante pour comprendre la faute : autrement dit la capacité de discernement.

2. La responsabilité civile contractuelle du mineur dans le cyberspace.

La responsabilité contractuelle du mineur est celle qui résulte de l'inexécution par ce dernier d'une obligation née d'un contrat. Pour que la responsabilité contractuelle d'une partie puisse être engagée, il faut la réunion de trois éléments : l'existence d'un *manquement* à une obligation ayant été à l'origine d'un *préjudice* subi par l'autre partie, ce qui suppose un *lien de causalité* entre le manquement et le dommage. C'est l'article 1146 du code civil qui régit la matière de la responsabilité contractuelle.

En pratique, il n'est pas toujours évident de déterminer si il s'agit d'une responsabilité contractuelle ou délictuelle. S'agissant de la responsabilité contractuelle, les parties ont en général prévu les conséquences de la responsabilité en fixant forfaitairement le montant des dommages-intérêts ; il s'agit de la clause pénale. En amont de l'engagement de la responsabilité contractuelle du mineur, cela suppose que l'on reconnaisse qu'il a pu valablement conclure un contrat électronique.

La responsabilité du fait personnel du mineur peut trouver à s'appliquer dans les contrats de vente que le mineur conclut en ligne. Il propose un objet à la vente, dans le cas où il ne

livrerait pas l'objet de la transaction selon les termes du contrat, son manquement peut conduire à l'engagement de sa responsabilité contractuelle.

En matière contractuelle, les causes d'exonération du débiteur de l'obligation dépendent de la nature de son obligation. S'il s'agit d'une obligation de moyen, le débiteur pourra s'exonérer totalement ou partiellement en prouvant son absence de faute, l'existence d'une cause étrangère, le fait d'un tiers ou de la victime. En revanche, s'il s'agit d'une obligation de résultat, le débiteur ne pourra en principe s'exonérer que par la preuve d'une cause étrangère. La preuve de son absence de faute est sans incidence sur l'engagement de sa responsabilité.

Il existe deux types de réparation :

- La **réparation en nature**. Toute forme de réparation autre que pécuniaire est considérée comme une réparation en nature. La pratique montre une réticence des juges à appliquer ce mode de réparation dans le domaine informatique et par extension aux contrats électroniques. Le principe est de l'exclure (article 1142 du code civil⁵⁰⁶). Rien n'interdit pour autant qu'une réparation en nature soit combinée avec une réparation pécuniaire.
- La **réparation par équivalent** (le plus souvent réparation pécuniaire). On retombe dans le cas de figure où les parents vont se trouver pécuniairement et civilement responsables des dommages causés par leur enfant mineur à autrui.

Au regard du principe de la liberté contractuelle, les parties contractantes peuvent décider de substituer aux règles légales, des règles conventionnelles qui auront vocation à s'appliquer en cas d'inexécution des obligations. Parmi ces clauses, il peut y avoir des clauses exonératoires et/ou des clauses limitatives de responsabilité ou des clauses pénales. Les clauses pénales permettent de fixer forfaitairement dès la conclusion du contrat le montant des dommages-intérêts dus en cas de retard ou d'inexécution. La clause pénale est régie par les articles 1152 et 1126 à 1233 du code civil. La clause pénale a des avantages certains en ce qu'elle élude les questions d'évaluation judiciaire des dommages-intérêts et prévient l'inexécution du contrat par la menace qu'elle représente. Elle présente toutefois des dangers en particulier lorsqu'elle est imposée par la partie la plus forte. C'est pour cette raison que le juge peut d'office

⁵⁰⁶ Il existe des exceptions à l'article 1142 suivant que l'exécution en nature est possible ou non. L'article 1443 autorise le créancier à demander la destruction aux frais du débiteur, de choses accomplies en violation du contrat. Selon l'article 1444, le créancier peut, en cas d'inexécution, faire lui-même exécuter les obligations du débiteur par un tiers et aux frais du débiteur défaillant.

l'aménager conformément à l'article 1152 al. 2⁵⁰⁷. Le véritable enjeu est de savoir si le contrat électronique conclu par le mineur est valable. Si tel est le cas le mineur sera-t-il considéré comme disposant de suffisamment de discernement pour en plus du contrat, établir des clauses contractuelles susceptibles de régir sa responsabilité contractuelle. La question se posera d'autant plus si le contrat est conclu avec un adulte qui savait contracter avec un mineur. Ne pourrait-on pas considérer systématiquement que cette règle a été imposée au mineur par une partie plus forte qui serait le cocontractant non mineur. On peut envisager comme en droit québécois que la capacité de discernement (du mineur en l'occurrence) soit une condition suspensive de la responsabilité contractuelle du cocontractant débiteur de l'obligation⁵⁰⁸.

La vulnérabilité du mineur reste l'élément central dans les actes qu'il peut poser dans le cyberspace. Cette vulnérabilité est également prise en compte dans les actes commis pour ou contre lui dans le cyberspace. Le mineur a certes des droits et obligations dans le cyberspace mais les tiers (adultes en général) en ont également à son égard.

⁵⁰⁷ Loi du 9 juillet 1975 « ...le juge peut, même d'office, modérer ou augmenter la peine qui avait été convenue, si elle est manifestement excessive ou dérisoire. Toute stipulation contraire sera réputée non-écrite », voir F. Chabas, La réforme de la clause pénale : D. 1976, chronique. P.229.

⁵⁰⁸ Jean-Louis Baudouin et Patrice Deslauriers, La responsabilité civile, 6^e édition, Editions Yvon Blais, 2003.

Chapitre 2. LA SANCTION DES MANQUEMENTS DU MINEUR AUX DROITS D'AUTRUI DANS LE CYBERESPACE.

Dès lors qu'un mineur est considéré comme un acteur à part entière du cyberespace, il y pose des actes qui sont porteurs de conséquences juridiques. On peut aisément considérer que la liberté d'expression est pour les internautes l'un des droits phares dans le cyberespace. Le mineur exerce sa liberté d'expression de diverses manières sur la Toile. Il dialogue avec autrui par le biais de courriers, messageries instantanées, etc. Il communique également unilatéralement grâce au statut d'éditeur qu'il endosse (plus ou moins inconsciemment) lorsqu'il diffuse des contenus dont-il est l'auteur ou qu'il relaie des contenus d'autrui. Au cours de ses activités d'éditeur, il engage sa responsabilité pour peu que ses activités aient été porteuses de préjudice pour autrui. Tout délit informatique dont-il serait l'auteur ou le co-auteur engage directement sa responsabilité.

§1. Les infractions liées au statut d'auteur ou d'éditeur de contenus du mineur.

Le cyberespace est dans une logique d'évolution continue. Ses fonctionnalités et les possibilités qu'il offre aux internautes sont dans une logique de perpétuelle innovation. La diffusion de contenus étant la raison d'être d'Internet, ce sont les modes de diffusion qui sont révolutionnés au gré des innovations technologiques. Dès sa banalisation Internet a offert, à ceux qui en maîtrisaient la technologie la possibilité de créer des sites et des pages personnelles. Le phénomène d'appropriation du cyberespace a connu avec les blogs⁵⁰⁹ une

⁵⁰⁹Aucune définition claire n'existe actuellement pour le terme blog. Le blog est plutôt défini par les fonctionnalités qu'il regroupe que par sa nature seule. Le blog peut être un journal intime anonyme ou non en ligne ; un site personnel pour parler de soi et présenter ses activités professionnelles ou personnelles ; un site d'une personne physique ou morale, civile ou politique ; il peut s'agir d'une vitrine pour un artiste soucieux de faire connaître ses œuvres, un album photo en ligne, etc.

véritable explosion. Le blog présente l'originalité par rapport aux pages ou sites personnels, de laisser une place importante à l'interactivité. Nul besoin d'être un informaticien chevronné, la diffusion est facilitée par l'emploi de logiciels spécialisés tel qu'un système de gestion de contenu. Ce dernier met en forme le texte et les illustrations sous la direction du blogueur. Il construit des archives automatiquement. Il offre des moyens de recherche au sein de l'ensemble des billets et gère enfin les commentaires des internautes lecteurs. Ces outils permettent ainsi à chacun de publier du contenu, sans que cela nécessite des connaissances techniques préalables relatives à la conception de sites Web. Cette facilité d'utilisation a contribué pour une grande part à l'explosion des blogs ces dernières années⁵¹⁰. Très vite a émergée la question de la nature juridique des blogs et de leur réglementation. Une réglementation spécifique était-elle nécessaire ou pouvait-on appliquer le droit commun et en l'occurrence la législation sur les infractions de presse. Plus concrètement, l'appropriation de cet outil par le mineur induit une interrogation sur le traitement qui devrait être fait des infractions commises par ce dernier dans son rôle d'éditeurs de contenus.

Conformément à la loi du 29 juillet 1881, est désigné comme auteur principal de l'infraction et donc passible de poursuites, le directeur de publication ou l'éditeur, l'auteur, à défaut de celui-ci, les imprimeurs ou subsidiairement encore, les vendeurs, distributeurs ou afficheurs⁵¹¹. Le mineur du fait des contenus qu'il diffuse sur Internet directement ou par une technique de relais peut engager sa responsabilité pénale et/ou civile. Le blogueur sera considéré au sens de la loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique⁵¹², comme un « éditeur d'un service de communication publique en ligne ». En tant que blogueur, il a une double responsabilité : vis-à-vis de la loi sur la presse du 29 juillet 1881 quant aux contenus dont-il est l'auteur sur son blog⁵¹³ et vis-à-vis des contenus d'autrui qu'il

Le concept *blog* est assez vague pour autoriser toutes ces utilisations. Le phénomène blog connaît un grand succès grâce à une grande facilité de diffusion, une grande liberté éditoriale et une grande capacité d'interaction avec les internautes. La majorité des blogs s'utilisent à des fins d'autoreprésentation, et la plupart se forment autour des affects et des idées propres à leur(s) auteur(s). C'est pour cette raison que la presse et l'opinion populaire sont parfois amenées à fustiger l'égoïsme des blogs. <http://fr.wikipedia.org/wiki/Blog>

⁵¹⁰ <http://fr.wikipedia.org/wiki/Blog>

⁵¹¹ Loi de 1881, art. 42.

⁵¹² LCEN article 6-III.

⁵¹³ Blandine Poidevin, Le cadre juridique de la responsabilité des blogs, 28 février 2006.

http://www.jurixpert.net/blogs/index.php?title=le_cadre_juridique_de_la_responsabilite_1&more=1&c=1&tb=1&pb=1

a relayé dans son blog et dans certaines hypothèses des commentaires délictueux faits par les intervenants sur son blog⁵¹⁴.

A. Les infractions de presse.

La liberté de la presse est étroitement liée à la liberté d'expression⁵¹⁵. Elle prend ses racines dans l'article 11 de la Déclaration des droits de l'homme selon lequel, « *la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ». Ce sont ces infractions qui se trouvent « définies et sanctionnées par la loi du 29 juillet 1881 »⁵¹⁶. Sont réprimés :

- les provocations aux crimes et délits (art. 23 à 25),
- les délits contre la chose publique, l'offense au Président de la République et la diffusion de fausses nouvelles (art. 26 et 27),
- les délits contre les personnes que sont les diffamations, les injures, les atteintes à la présomption d'innocence et les atteintes à la dignité des victimes d'infractions (art. 29 à 35 *quater*),
- les publications interdites auxquelles sont jointes les immunités de la défense (art. 38 et 39 *bis*).

Il n'y a pas de délit de presse sans publicité ; il s'agit d'une règle absolue. L'auteur d'une allégation susceptible de caractériser une infraction prévue par la loi de 1881 ne pourra être

⁵¹⁴ La loi du 29 juillet 1881 sur la communication audiovisuelle prévoit que : « *au cas où l'une des infractions prévues par la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public* ». On peut considérer que cette fixation préalable n'existe pas sur un blog où, de la même manière que sur un forum de discussion sans modérateur, les messages des participants sont immédiatement affichés sans contrôle préalable. Il revient au blogueur de rappeler de manière expresse à ses visiteurs les règles à respecter afin de s'exonérer de toute responsabilité en tant que directeur de la publication. La responsabilité du blogueur peut être écartée en tant que directeur de la publication mais sera recherchée si l'auteur n'est pas identifiable. Enfin il peut voir sa responsabilité pénale engagée en tant que complice sur le fondement de l'article L. 121-7 du Code pénal qui dispose qu'est complice « *la personne qui sciemment par aide ou assistance, en a facilité la préparation ou la consommation* ».

http://www.jurixexpert.net/blogs/htsrv/trackback.php?tb_id=239

⁵¹⁵ Sur les relations entre la liberté de la presse et la liberté d'expression voir Cass. Crim., 13 juin 1995 : Bull. crim. n°217 : « les dispositions de la loi du 29 juillet 1881, qui protègent et délimitent la liberté de la presse, ne concernent pas la liberté de pensée prévue par l'article 9 de ladite Convention, mais la liberté d'expression régie par son article 10 ».

⁵¹⁶ M. Véron, La responsabilité pénale du directeur de la publication. Infractions de presse et infractions par voie de presse : Droit pénal, février 1996, chronique. p. 1.

poursuivi que, si il a donné à son écrit une publicité qui seule aura pu la porter à la connaissance d'autrui⁵¹⁷. Internet est entièrement voué et tourné vers la publicité de ses contenus. La responsabilité en matière de délits de presse est régie par l'article 42 de la loi de 1881 qui édicte une hiérarchie : la responsabilité en « cascade »⁵¹⁸.

L'avènement des blogs est pour beaucoup dans l'accroissement des hypothèses d'engagement de la responsabilité d'éditeur des mineurs. L'internaute mal ou non informé endosse involontairement des responsabilités qui sont généralement celles de professionnels de l'information et de la communication. Pour autant, leur ignorance ne les décharge pas de leur responsabilité. Ils sont tenus de répondre des conséquences des contenus diffusés sur les personnes citées de celles en prenant connaissance⁵¹⁹.

Les infractions retenues pour cette étude seront : la diffamation, l'injure et la contestation des crimes contre l'humanité. Ce sont des délits récurrents s'agissant des infractions de presse sur Internet.

1. La diffamation, l'injure.

Il s'agit dans les deux cas de délit visant une personne physique ou morale dans sa réputation, son honneur, etc.

1-a. La diffamation.

Il s'agit d'un « délit ou une contravention consistant à alléguer ou imputer un fait portant atteinte à l'honneur ou à la considération d'une personne ou d'un corps »⁵²⁰.

La loi sur la confiance dans l'économie numérique du 21 juin 2004 a définitivement établi que, comme les publications dans la presse écrite et audiovisuelle, les publications sur

⁵¹⁷ Philippe Bilger, *Le droit de la presse, Que sais-je ?* PUF 2003, p. 22.

⁵¹⁸ Seront retenus comme auteurs principaux des infractions de presse, les directeurs de publication ou éditeurs ; à défaut les auteurs ; à défaut des auteurs les imprimeurs ; à défaut des imprimeurs les vendeurs, distributeurs et afficheurs. Longtemps applicable à la seule presse écrite, elle a été étendue à tout service de la communication audiovisuelle par la loi du 13 décembre 1985 qui impose l'existence d'un directeur de la publication et la responsabilité automatique de ce dernier sauf en cas de diffusion « en direct » ; Paris, 1^{ère} Ch., 6 octobre 1987, Polac c/ Romanet.

⁵¹⁹ Conférence de la famille 2005, « Protection de l'enfant et usages d'Internet », Rapport de propositions remis à Philippe Douste-Blazy, préc. p.36, *Légipresse* n°227.

⁵²⁰ Rémy Cabrillac, *Dictionnaire du vocabulaire juridique*, Jurisclasseur, Litec. – Loi du 29 juillet 1881, art. 29 et s.

Internet (et notamment les messages diffusés sur un forum de discussion à accès restreint ou non) sont soumises aux dispositions de la loi sur la presse du 29 juillet 1881⁵²¹. Cette loi condamne expressément et sévèrement, la diffamation et l'injure qu'elles soient publiques ou non. La diffamation publique peut être punie d'un an et de 45.000 euros d'amendes ; elle est réputée commise le jour où l'écrit est porté à la connaissance du public.

Les forums de discussion ne sont pas les seuls visés, les mineurs faisant un usage très varié des ressources du cyberspace. La liberté d'expression du mineur se manifeste aussi bien dans les sites personnels, les blogs, les webzines, etc. Tous ces supports sont susceptibles de favoriser ou du moins de faciliter des dérapages tels que la diffamation et/ou l'injure.

Ce sont en grande partie des affaires de diffamation qui ont alimentées le débat sur l'application de l'article 65 de la loi de 1881⁵²². La personne morale tout comme la personne physique peut être victime de diffamation⁵²³, il suffit que la victime soit identifiée ou identifiable.

La diffamation est juridiquement sanctionnée, quel qu'en soit l'auteur. Si la preuve de la diffamation est établie le mineur engage sa responsabilité pénale⁵²⁴ ; une action civile est également envisageable. Les parents ou tuteurs légaux peuvent voir leur responsabilité solidairement engagée.

L'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle prévoit la responsabilité pénale du directeur ou du codirecteur de publication « *comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au*

⁵²¹ Article de Muriel Cahen paru sur le site Avocat Online, Quelles démarches accomplir pour poursuivre l'auteur d'une injure ou d'une diffamation ? Le droit de la preuve en la matière. http://www.murielle-cahen.com/p_forum2.asp

⁵²² Article 65 modifié par la Loi n°93-2 du 4 janvier 1993 article 52 (JORF 5 janvier 1993).

« L'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescriront après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait.

Toutefois, avant l'engagement des poursuites, seules les réquisitions aux fins d'enquête seront interruptives de prescription. Ces réquisitions devront, à peine de nullité, articuler et qualifier les provocations, outrages, diffamations et injures à raison desquels l'enquête est ordonnée.

Les prescriptions commencées à l'époque de la publication de la présente loi, et pour lesquelles il faudrait encore, suivant les lois existantes, plus de trois mois à compter de la même époque, seront, par ce laps de trois mois, définitivement accomplies ».

⁵²³ Cass. 1^{re} civ., 5 juillet 2000 : Comm. com. électr., commentaire. n°21, obs. A. Lepage.

⁵²⁴ L'article 48-6 de la loi du 29 juillet 1881 précise que dans le cas de diffamation envers des particuliers et dans[...] le cas d'injure[...], la poursuite n'aura lieu que sur la plainte de la personne diffamée ou injuriée.

public». Cette notion implique une prise de connaissance par ce dernier du contenu avant diffusion dans le cyberspace.

Au cours du printemps 2005, plusieurs chefs d'établissement scolaires ont temporairement ou définitivement exclu des élèves, qui avaient mis en ligne des photos dérobées de leurs enseignants, assorties de propos moqueurs voire injurieux⁵²⁵.

Il existe cependant deux possibilités de s'exonérer de cette responsabilité :

- Par l'exception de vérité (*exceptio veritatis*). Sauf cas particulier, la personne incriminée peut rapporter la preuve de la véracité des faits qu'il a imputé à autrui. Il y a tout de même un encadrement strict à cette exception. En vertu de l'article 35 de la loi de 1881, il n'est pas possible d'invoquer et d'user de l'*exceptio veritatis* lorsque l'affirmation incriminée concerne la vie privée du plaignant ; lorsqu'elle se réfère à un fait remontant à plus de 10 ans, amnistié, prescrit ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision.
- Par la preuve de la bonne foi et de façon dérogatoire aux principes du droit pénal qui veulent qu'en matière de diffamation le prévenu soit présumé de mauvaise foi. Il s'agit d'une présomption simple, le prévenu a donc la possibilité de démontrer son innocence en prouvant sa bonne foi. La bonne foi suppose quatre critères : la modération, l'absence d'animosité personnelle, le but légitime et le respect du devoir d'enquête⁵²⁶.

La preuve de la vérité et/ou de la bonne foi détruit donc la diffamation. La loi de 1881 en son article 55 ne laisse que dix jours pour offrir cette preuve sous peine d'irrecevabilité. Ces règles datent d'une époque où la publication n'était l'affaire que de quelques uns : éditeurs, groupe de presse, monopole d'Etat sur la radio et la télévision. Aujourd'hui des millions de personnes publient chaque jour sur Internet d'où le problème de l'adéquation de ces réglementations à Internet. Aucun internaute (non professionnel de la presse) ne pré constitue d'une part les preuves de la véracité des contenus qu'il publie, ni d'autre part celles de la bonne foi dont-il fait preuve dans sa publication. Les internautes dans leur majorité ne savent

⁵²⁵ Auteur : Nicole Bondois et M. Nicolas Samarcq <http://www.droit-ntic.com/news/afficher.php?id=314>

⁵²⁶ Olivier Cazeneuve, Internet et diffamation. Existe-t-il une liberté d'expression de l'internaute ? 3 novembre 2005, http://reseaudesbahuts.lautre.net/article_print.php3?id_article=152

pas ce qu'est un devoir d'enquête *a fortiori* l'internaute mineur. Comment pourraient-ils connaître le délai qu'ils ont pour prouver la véracité de ce qu'ils ont publié ?

Dans l'hypothèse où la diffamation est avérée, la personne diffamée peut solliciter un droit de réponse en ligne selon les dispositions de la loi pour la confiance dans l'économie numérique⁵²⁷. Faute de décret d'application, son applicabilité est encore sujette à caution. En principe cependant, l'absence de décret ne peut empêcher l'application d'une loi, même en matière pénale. Il n'est pas besoin d'attendre la publication d'un décret et la loi est applicable dès son entrée en vigueur (art. 1er Code civil)⁵²⁸.

Quel est le régime du droit de réponse ? Le demandeur doit simplement faire état de sa volonté d'exercer son droit de réponse. Il est maître de la teneur de sa réponse. Bien évidemment ce droit est gratuit. Le délai pour exercer un droit de réponse est de 3 mois. En effet, l'action civile ou pénale en diffamation se prescrit après 3 mois à compter de la première mise en ligne de l'écrit jugé diffamatoire. Le point de départ de ce délai est la mise à disposition au public du message justifiant la demande. Seul l'instant de la mise en ligne doit être pris en considération. Au 1er mars 2006, seuls les messages mis en ligne trois mois plus tôt étaient susceptibles de faire l'objet d'un droit de réponse. La difficulté est de déterminer avec précision cette date sur Internet ; reste à préciser quel type d'écrit doit parvenir au service de communication ? La loi ne donne pas d'indication. Il est préférable d'utiliser un courrier recommandé avec accusé de réception. En effet, la question de la preuve du respect du délai sera réglée de cette manière. Dès réception de la réponse, le directeur de la publication a trois jours pour l'insérer dans son service de communication (article 6 IV de la LCEN al. 3). La difficulté pratique est d'identifier le responsable du service de communication et son adresse postale⁵²⁹.

⁵²⁷ Depuis 2004, l'article 6 IV de la loi du 21 juin 2004 pour la confiance dans l'économie numérique fixe le cadre juridique du droit de réponse spécifique sur Internet (ci-après art. 6 IV LCEN).

⁵²⁸ Le futur décret d'application concernant le droit de réponse en ligne a été transmis à la Commission européenne. Relevant de la loi pour la confiance dans l'économie numérique, il permet aux personnes citées par un "service de communication au public en ligne" d'y publier une réponse de 200 "lignes" maximum. Les chats et forums de discussion ne font pas parti des supports concernés. La réponse doit être envoyée avant 3 mois, et doit être insérée avant 3 jours, sous peine de 3.750 euros d'amende pour le directeur de la publication. Pour le texte du Décret voir : http://www.tntlex.com/public/projet_decret_droit_reponse.pdf

⁵²⁹ Thinault Verbiest, « Droit de réponse : comment l'exercer sur le Net », 20/06/2006, voir le site Le Journal du Net : <http://www.journaldunet.com/juridique/juridique060620.shtml>

Il est nécessaire de garder une trace électronique de l'infraction avant que cette dernière ne soit effacée. Bien qu'il soit reconnu force probante à l'écrit électronique⁵³⁰, la preuve n'est pas aisée à établir. La personne dont l'écrit diffamatoire émane doit pouvoir être identifiée. Il doit être établi que cet écrit a été conservé « dans des conditions de nature à en garantir l'intégrité ».

L'enregistrement d'une page Web diffamante ne peut constituer qu'un commencement de preuve sans force probante indiscutable, car l'intégrité peut être remise en cause, la page Web enregistrée sur support électronique ou imprimée peut avoir été préalablement modifiée. Il existe une autre démarche : établir un constat par un huissier ou par un agent assermenté de l'Agence de la Protection des Programmes. Pour être reconnu comme preuve par le juge, le constat par huissier doit respecter des règles de validité : la victime de la diffamation ne doit en aucun cas intervenir lors de l'établissement du constat⁵³¹.

Bien que la diffamation apparaisse comme le délit de presse par excellence, l'injure est tout autant un délit de presse. C'est généralement un dérapage de langage, un excès constituant une catégorie résiduelle d'infractions dans le contentieux de la presse⁵³².

1-b. L'injure.

L'injure contrairement à la diffamation ne fait référence à aucun fait précis. L'injure, est un « délit ou une contravention incriminant l'emploi d'une expression outrageante termes de mépris ou invective, sans contenir d'imputation d'un fait précis »⁵³³. En pratique la diffamation et l'injure sont souvent mêlées. Ce qui permet de les différencier, c'est le fait que la diffamation suppose une imputation ou une allégation d'un fait déterminé contrairement à l'injure. L'absence de publicité fait dégénérer les délits de diffamation et d'injure en contraventions non publiques de première classe punissables de 38 euros d'amendes et

⁵³⁰ Depuis la loi du 13 mars 2000 et son décret d'application du 31 mars 2001, les preuves électroniques sont acceptées et ont la même force probante que les preuves écrites. L'article 1316-1 du code civil dispose que « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». L'article 1316-3 du code civil précise que « l'écrit sur support électronique à la même force probante que l'écrit sur support papier ».

⁵³¹ Article de Muriel Cahen, « Quelles démarches accomplir pour poursuivre l'auteur d'une injure ou d'une diffamation ? Le droit de la preuve en la matière » TGI Paris, 4 mars 2003.

http://www.murielle-cahen.com/p_forum2.asp

⁵³² Christophe Bigot, « Connaître la loi de 1881 », Guide Légipresse 2004.

⁵³³ Rémy Cabrillac, Dictionnaire du vocabulaire juridique, Jurisclasseur, Litec. – Loi du 29 juillet 1881, art. 29 al 2.

relevant du tribunal de police et régies respectivement par les articles R. 621-1 et 2 du code pénal⁵³⁴.

Si l'expression outrageante peut être une simple indécatesse, l'invective elle recouvre les termes les plus grossiers, voire les plus orduriers. La plupart du temps, le caractère injurieux des propos incriminés est d'une totale évidence⁵³⁵. L'injure tout comme la diffamation suppose l'existence d'une victime déterminée ou déterminable. « Dès lors que l'injure formulée de manière générale vise une pluralité de personnes formant un groupe restreint, chaque membre de ce groupe, atteint par l'injure, dispose d'un droit individuel à demander réparation du préjudice qui lui a été causé »⁵³⁶. L'intention coupable suppose que « l'expression outrageante, les termes de mépris ou l'invective » aient été formulés sciemment. La jurisprudence pose une présomption de mauvaise foi⁵³⁷ ; nul ne peut ignorer qu'il offense en outrageant⁵³⁸.

Il n'est pas possible en matière d'injure, et ce contrairement à la diffamation d'invoquer la bonne foi pour s'exonérer de sa responsabilité. Dans le cas l'injure une seule excuse est exonératoire : la provocation. L'article 33 de la loi de 1881 prévoit une excuse absolutoire qui entraîne le renvoi des fins de la poursuite et donc une absence totale de condamnation. Cette provocation n'est cependant définie par aucun texte. C'est la jurisprudence qui en a progressivement défini les contours et déterminé les conditions d'application. Il s'agit de tout fait ou agissement volontaire de nature à excéder sa victime et donc expliquer la réplique qu'est l'injure, il doit cependant présenter des caractères précis :

- la personne provoquée doit être celle poursuivie pour injure. Ce qui exclut que l'on puisse légitimement se porter par le verbe au secours d'un tiers qui aurait été l'objet d'une provocation,
- il faut qu'il existe un lien direct entre la provocation et l'injure. Ce qui impose que l'une et l'autre se suivent dans le temps de manière rapprochée,
- il doit exister une certaine proportionnalité entre l'attaque initiale et l'injure en réplique.

⁵³⁴ Civ. 2, 24 octobre 2002.

⁵³⁵ Philippe Bilger, Le droit de la presse, Que Sais-Je ? PUF 2003, p. 62.

⁵³⁶ Crim., 12 septembre 2000, Bull. n° 265.

<http://www.ca-bastia.justice.fr/crim120900.htm>

⁵³⁷ Crim., 18 janvier 1950 ; CA Paris, 2 mars 1995, Droit pénal, 1995-121, observations Véron.

⁵³⁸ Philippe Bilger, Le droit de la presse, op.cit., p. 66.

Il n'est pas nécessaire que la provocation ait été publique au sens de la loi de 1881. Peut-on considérer que le mineur qui a été victime de provocation est en droit de répliquer par l'injure sur Internet ? Eu égard à l'audience et à la rapidité de la diffusion sur Internet l'élément de proportionnalité est-il respecté ? Pour l'heure la jurisprudence n'a pas encore statué sur la question.

2. L'apologie des crimes contre l'humanité et leur contestation.

Les crimes contre l'humanité constituent une matière suffisamment grave et sensible, c'est pour cette raison qu'ils sont susceptibles de générer deux types de délits ; l'apologie des crimes contre l'humanité et la contestation des crimes contre l'humanité.

2-a. L'apologie des crimes contre l'humanité.

Dans son jugement dit "Aussaresses"⁵³⁹, le Tribunal de Paris a défini l'apologie des crimes contre l'humanité comme s'entendant « *du discours qui présente un crime de guerre de telle sorte que le lecteur est incité à porter sur ce crime un jugement de valeur favorable effaçant la réprobation morale qui, de par la loi, s'attache à ce crime* ». Une telle apologie est selon le Tribunal « *incriminée en ce qu'elle constitue une provocation indirecte à commettre de semblables crimes* ». Parmi les apologies de crimes prohibées et conformément à l'article 24 de la loi de 1881, il faut compter les crimes de guerre, les crimes contre l'humanité, les crimes ou délits de collaboration avec l'ennemi.

Les crimes contre l'humanité sont déterminés comme suit :

- Avant l'entrée en vigueur du nouveau Code pénal, les crimes définis par l'article 6 du statut du Tribunal militaire international dit de "Nuremberg" annexé à l'accord de Londres du 8 août 1945 étaient ceux qui avaient été commis soit par les membres d'une organisation déclarée criminelle (SS, Gestapo, SD, Corps des chefs des nazis), soit par toute personne reconnue coupable de tels crimes par une juridiction française ou internationale.
- Selon la jurisprudence, constituent des crimes contre l'humanité des actes inhumains et des persécutions qui, au nom d'un Etat pratiquant une politique d'hégémonie idéologique, sont commis systématiquement contre des personnes en raison de leur

⁵³⁹ TGI Paris 17^e chambre 25 janvier 2002, Légipresse 2002-I, p. 26, n° 190-01.

appartenance à une collectivité raciale ou religieuse, ou contre les adversaires de la politique de cet Etat.

Seuls sont concernés les crimes reconnus perpétrés pendant la Seconde Guerre mondiale par des criminels de guerre des pays européens de l'Axe, essentiellement l'Allemagne nazie, et par toute personne ayant agi pour le compte de ces Etats⁵⁴⁰.

La matérialisation d'un tel délit dans le cyberspace est liée à ses fonctionnalités. Les supports pouvant permettre la matérialisation de cette infraction sont les sites et pages personnels, les blogs, les forums de discussion organisés ou édités par des mineurs. En somme tout ce qui est axé sur la communication du mineur dans un espace public. La condition de communication publique est retenue car il ne serait pas possible à la justice de se saisir spontanément des communications privées du mineur ou des communications de ce dernier dans un espace déterminé comme privé sauf ordonnance juridique.

Depuis quelques années, on peut voir pulluler sur Internet des sites néo-nazi. Ces sites ont fait du cyberspace un terrain de recrutement et de propagande auprès des internautes de plus en plus jeunes. Des mineurs convertis à cette idéologie, se servent à leur tour d'Internet pour véhiculer cette idéologie en faisant par exemple l'apologie de crimes contre l'humanité.

2-b. La contestation des crimes contre l'humanité.

Il faut entendre par contestation des crimes contre l'humanité leur contestation ou leur négation publique.

La contestation de ces crimes est réprimée par l'article 24 bis de la loi 1881 sur la liberté de la presse⁵⁴¹. Cet article a été inséré par la loi du 13 juillet 1990 dite Loi Gayssot. Cette infraction vise tout particulièrement ceux qui, prétendant à la qualité d'historien, tendent à démontrer l'inexistence de l'holocauste nazi ou à le minimiser de manière outrancière. Aucun texte ne permettrait de sanctionner les auteurs d'écrits qualifiés révisionnistes ou négationnistes qui

⁵⁴⁰ Combattre le racisme France, France/Les lois antiracistes.

http://www.droitshumains.org/Racisme/r_france/04.htm

⁵⁴¹ « Seront punis des peines prévues par le sixième alinéa de l'article 24 ceux qui auront contesté, par l'un des moyens énoncés à l'article 23, l'existence d'un ou plusieurs crimes contre l'humanité tels qu'ils sont définis par l'article 6 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945 et qui ont été commis soit par des membres d'une organisation déclarée criminelle en application de l'article 9 dudit statut, soit par une personne reconnue coupable de tels crimes par une juridiction française ou internationale ». Cet article punit d'un an d'emprisonnement au plus et/ou une amende de 300.000 € au plus.

parvenaient à donner à leurs propos une résonance raciste. Il importe peu que cette contestation soit effectuée le cas échéant sous une forme d'insinuation comme l'a admis la Chambre criminelle de la Cour de Cassation⁵⁴². Seuls les crimes contre l'humanité définis par l'article 6 du statut du Tribunal militaire international annexé à l'accord de Londres du 8 août 1945 sont concernés. Le texte contient une référence expresse au jugement du Tribunal de Nuremberg qui vaut définition du délit de la contestation de crimes contre l'humanité.

La condition de la répression est l'existence d'une contestation publique ; l'expression de cette contestation sur Internet en a toutes les caractéristiques. Les modes de manifestation de la liberté d'expression sur Internet favorisent toutes sortes de dérapages notamment de la part des mineurs. Ces derniers même si ils mesurent parfois la gravité des propos qu'ils tiennent n'en maîtrisent pas pour autant toutes les conséquences juridiques. Dans leurs pages personnelles, leurs blogs, dans des forums, des chats ou tout autre moyen d'expression électronique, ils peuvent de leur propre fait ou en interaction avec d'autres, commettre de tels délits. Certains par ignorance et par amusement vont diffuser de tels écrits sans en connaître la portée ; d'autres vont se faire le relais d'opinions, d'idéologies haineuses, qu'ils les partagent ou non.

Il n'est pas nécessaire que le mineur soit lui-même l'auteur de cette contestation, il suffit qu'en tant qu'éditeur de contenus il aie publié ou relayé des contenus constitutifs de contestation de crimes contre l'humanité pour engager sa responsabilité.

Internet donne une telle impression de liberté d'expression, d'existence virtuelle en dehors des contingences répressives du monde réel que les dérapages sont fréquents. Les mineurs peuvent se servir de leur statut d'éditeur ou d'auteur de contenu pour nuire à la réputation et/ou l'image d'autrui. Il s'agit d'infractions par voie de presse qui sont régis par le code pénal en marge des délits de presse qu'incrimine la loi de 1881 sur la liberté de la presse.

⁵⁴² Cass. Crim 29 janvier 1998 ; Cass. Crim. 12 septembre 2000, Droit pénal, 2001, paragraphe 4, observations Véron.

B. Les infractions par voie de presse.

La loi de 1881 a conservé son statut de grande loi sur la presse ; cependant la multiplication des délits de presse en dehors de son domaine lui a fait perdre son hégémonie en la matière⁵⁴³. Il ne s'agit pas d'une loi autonome mais au contraire d'une loi « de supplément » à laquelle il ne convient de faire appel que lorsque les règles du droit commun sont insuffisantes⁵⁴⁴.

Les infractions par voie de presse sont des infractions d'origine et de nature diverses mettant en œuvre des moyens de commissions diversifiés mais présentant le point de commun de pouvoir être commises par voie de presse⁵⁴⁵. « Nombreuses sont les infractions constituées par une publication et qui ont été essayées par le législateur hors du domaine de la loi de 1881⁵⁴⁶. Le code pénal répertorie un certain nombre de ces infractions : atteintes à la vie privée (art. 226-1 à 226-9), montage de paroles et d'images (art. 226-8), provocation au suicide (art. 223-13 à 223-15), diffusion d'un message violent, pornographique ou attentatoire à la dignité susceptible d'être vu par un mineur (art. 227-24), provocations de mineurs à commettre diverses actions (art. 227-18 à 227-21), provocation à la rébellion (art. 433-10), pressions et discrédits jetés sur les décisions de justice (art. 434-16 à 434-25).

1. La rumeur.

Fondée ou pas, la rumeur ou fausse information se caractérise par sa source non officielle et le doute qu'elle génère. Dès qu'elle s'officialise, c'est pour être démentie ou confirmée : c'est la fin de la rumeur.

La facilité qu'offre Internet pour diffuser des informations au public est logiquement génératrice de dérives comme la rumeur qui est considérée comme « le plus vieux média du monde »⁵⁴⁷. Internet s'est révélé un puissant vecteur de rumeurs. Elles fleurissent dans les

⁵⁴³ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, op. cit., p. 120.

⁵⁴⁴ Sophie Martin-Valente, La place de l'article 1382 du code civil en matière de presse depuis les arrêts de l'Assemblée plénière du 12 juillet 2000 – Approche critique (2^e partie), *Légipresse* N° 203 – juillet/août 2003, p. 90.

⁵⁴⁵ M. Véron, La responsabilité pénale du directeur de la publication. Infractions de presse et infractions par voie de presse, art. op. cit.

⁵⁴⁶ A. Lepage, Les droits et libertés fondamentaux à l'épreuve d'Internet, op.cit., p. 131.

⁵⁴⁷ J.-N. Kapferer, Rumeurs. Le plus vieux média du monde, *Seuil, Points* 1995 ; *Dossier de Monde Interactif*, 23 mai 2001, p. I à III, « Rien n'arrête la rumeur sur la Toile ».

pages web et son relayées entre autres par les mails⁵⁴⁸. Nul n'est besoin de préciser que, une fois qu'une rumeur est "lâchée" dans le cyberespace, elle n'est plus contrôlable.

Internet apporte deux éléments majeurs dans la propagation de la rumeur. Auparavant la rumeur devenait publique dès lors qu'elle était relatée dans les médias. Internet permet à chacun de la rendre publique au-delà de toute proportion. De plus, l'anonymat et la possibilité de se créer de multiples identités sur Internet, permettent un relais plus aisé de la rumeur. Les internautes dans leur totalité peuvent être concernés, dans la mesure où tout internaute peut prendre part à sa propagation soit qu'il en est l'initiateur ou un des relais. La nuance quant au mineur est que l'on peut quasiment exclure l'*infans* de ce type d'infractions qui nécessite une volonté de nuisance avérée.

Un des exemples de rumeurs les plus célèbres lancées sur Internet concerne les attentats du 11 septembre, plus précisément celui commis contre le Pentagone. Les circonstances réelles, voire la réalité de cet attentat ont été remises en cause⁵⁴⁹ par des individus qui se sont servi d'Internet comme outil de propagande. En l'espace de quelques heures, la rumeur avait fait le tour de la planète amenant avec elle son cortège de soupçons et de suspicions. Dans le même genre, une rumeur concernant la ville d'Issy-les-Moulineaux a couru sur la Toile, passant de messagerie en messagerie avec pour titre « A FAIRE SUIVRE A TOUS VOS AMIS ». L'histoire concernait une femme qui se serait fait piquer par une seringue qu'un message accolé dessus disait contaminée par le virus du SIDA. Plusieurs institutions dont l'Institut Pasteur, le Commissariat de Police de la ville auraient prétendument avalisé cette rumeur en émettant des messages de prévention et d'alerte ; elles ont toutes démenties⁵⁵⁰.

On est amené à se demander si Internet n'aurait pas fait glisser le pouvoir des médias vers les particuliers. Ces derniers par manque de volonté, par malveillance ou souvent par ignorance ne se donnent pas la peine de vérifier, trier les informations qu'ils diffusent dans le cyberespace⁵⁵¹.

L'émergence des blogs a accru ce phénomène de création et de propagation des rumeurs. Les messageries instantanées, les courriers électroniques et les forums ne sont pas exclus. Tous les

⁵⁴⁸ A. Lepage. Les droits et libertés fondamentaux à l'épreuve d'Internet, op.cit., p. 68.

⁵⁴⁹ Le Monde 21 mars 2002, p. 18 et 23 ; Libération 26 mars 2002, p. 6 – 31 mars 2002, p. 4 et 6 ; Le Nouvel Observateur 28 mars et 3 avril 2002, p.68.

⁵⁵⁰ Journal Du Net, Philippe Guerrier, Issy-les-Moulineaux victime d'une rumeur sur Internet. <http://www.journaldunet.com/0102/010228issy.shtml>

⁵⁵¹ A. Cojean, « Le Monicagate, brûlot des médias américains », Le Monde, 13 février 1999, p. 15.

modes de communication sont propices à la diffusion de rumeurs. Les mineurs familiers à un monde de vérités factices (avec la vitrine des célébrités dont les fausses informations sont souvent orchestrées), sont les premiers à prendre au mot les rumeurs et à les relayer comme vraies. Ces rumeurs ne concernent pas que leur entourage ; il peut s'agir de célébrités plus ou moins connues, de personnages publics à diverses échelles, etc. C'est ainsi qu'on vu de nombreuses histoires émerger, mettant en cause leurs camarades ou le corps professoral, etc.

La victime seule peut demander l'application des règles de la responsabilité civile de droit commun sur le fondement de l'article de l'article 1382 du code civil. Pour ce faire, elle doit apporter la preuve de trois éléments : la fausse information elle-même constitutive d'une faute, le préjudice subi et le lien de causalité entre cette faute et le préjudice. Sur le plan pénal il n'existe pas de délit couvrant la création ou la diffusion de fausse information en tant que telles. Pour qu'une telle sanction soit envisagée, il faut que la création ou la diffusion de cette fausse information aboutisse à un préjudice particulier.

La particularité de la rumeur dans le cyberspace en comparaison au monde réel est que, dans le monde réel une rumeur peut cesser d'elle-même. Dans le monde virtuel cependant, elle pourra continuer d'apparaître dans les recoins du réseau, resurgir à tout moment, par le biais d'un moteur de recherche, la page personnelle d'un internaute, une sauvegarde, etc. La solution semble être un démenti juridique, pour cela la victime devra démontrer la fausse information et l'identité de son auteur⁵⁵².

Le mineur peut engager sa responsabilité en tant qu'auteur de la rumeur ou en tant que diffuseur. Sa responsabilité civile peut être engagée sur le fondement de la responsabilité civile de droit commun telle que régie par l'article 1382 du code civil. Mais, le recours à l'article 1383 du code civil⁵⁵³ est également envisageable. Le mineur bien qu'il ne soit pas l'auteur de la rumeur peut voir sa responsabilité engagée :

- si il a contribué à sa propagation bien qu'ayant conscience⁵⁵⁴ que celle-ci pouvait causer un préjudice ;
- si il n'a pas pris des précautions de texte telle que : l'emploi du conditionnel, la citation de la source ou de l'absence de source.

⁵⁵² Olivier Iteanu, Tous cybercriminels. La fin d'Internet ?, préc. p.81.

⁵⁵³ « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence ».

⁵⁵⁴ Il se repose la question de la conscience délictuelle du mineur.

La rumeur peut prendre plusieurs formes : fausses alertes aux virus, fausses chaînes de solidarité, fausses promesses, fausses pétitions⁵⁵⁵, etc.

La responsabilité pénale du mineur en tant que diffuseur peut être engagée si c'est prouvé qu'il avait conscience de rediffuser une information fausse. Responsabilité au titre de la complicité ou à titre principal.

2. Le montage de paroles et d'images.

La rumeur ne s'exprime pas uniquement par le langage, elle peut également consister en une image qui ne reflète pas l'entière réalité tel un montage d'image. On se réfère à ce type de montage sous le vocable d' "image rumorale"⁵⁵⁶. Des paroles ou des images réelles peuvent être manipulées afin de leur donner un sens, une apparence différente et non-conforme à la réalité, il s'agit également de rumeur. L'article 226-8 du code pénal régit la matière⁵⁵⁷.

La numérisation des appareils de photographies, des caméscopes et des téléphones mobiles a grandement facilité la possibilité de manipuler des images. Nul besoin de disposer de compétences pointues en technologie, pour pouvoir faire des montages. Le matériel est banalisé (par son le prix d'acquisition et l'accessibilité des techniques) et la diffusion est ouverte à tous par le biais d'Internet.

Il est arrivé que par souci de sanctionner des comportements particulièrement détestables les juges prononcent des condamnations sur le fondement de l'injure et de la diffamation en liberté avec l'interprétation stricte du droit pénal ; cela a été le cas alors même qu'il s'agissait de montages d'images⁵⁵⁸.

Le montage d'images sur Internet peut également être constitutif d'une atteinte à la vie privée, à l'image ; auquel cas, l'article 9 du code civil s'invite en la matière. Dans une affaire du 3 septembre 1997, un étudiant en informatique voulant se venger d'une petite amie avait diffusé

⁵⁵⁵ Conférence de la famille 2005, rapport sur la Protection de l'enfance et usages d'Internet remis au Ministre Philippe Douste-Blazy, préc.

⁵⁵⁶ P. Froissart, « Les images rumorales. Une nouvelle imagerie populaire sur Internet », Média Morphose, n°5, juin 2002, p. 27 et s.

⁵⁵⁷ L'art. 226-8 du code pénal punit d'un an et de 15.000€ d'amende la publication par quelle que voie que ce soit du montage réalisé avec les paroles ou l'image d'une personne sans son consentement s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou si il n'en est pas fait expressément mention.

⁵⁵⁸ TGI Meaux, 3^e ch. 19 novembre 2001 : Comm. com. électr. Février 2002, commentaire n°30, obs. A. Lepage ; D. 2002, sommaire. p. 2373, obs. C. Caron : montage et diffusion sur Internet de photographies représentant des collègues de travail dans des scènes pornographiques ou bien grimés en singes.

sur Internet depuis son ordinateur installé à son domicile, des photos à caractère pornographique la représentant. Ces clichés avaient fait l'objet de retouches numériques et étaient accompagnés de commentaires sur ses mœurs⁵⁵⁹, l'infraction de violation du droit à l'image sera retenue pour condamner l'auteur.

Certains actes nuisibles commis par le mineur dans le cyberespace sont de nature à troubler l'ordre public. Par des procédés techniques, le mineur peut mettre en péril l'équilibre du cyberespace. L'effet de ces nuisances ne se circonscrit pas uniquement au cyberespace, il peut avoir des incidences fâcheuses en dehors de cet espace.

§2. La criminalité informatique du mineur.

Le mineur est un acteur à part entière du cyberespace, dans un nombre important de cas il est même considéré comme un acteur avisé d'Internet, dans le sens où les arcanes du réseau lui sont familiers bien qu'il n'en maîtrise pas toutes les implications juridiques. L'internaute mineur dispose de compétences techniques dont-il est susceptible de faire mauvais usage, ce faisant il contribue au développement de la cybercriminalité⁵⁶⁰ en adoptant des agissements de cybercriminel.

A. Le piratage informatique.

La criminalité informatique est un phénomène ancien qui est né en même temps que l'informatique au milieu des années cinquante. Les premières attaques d'envergure de pirates informatiques avaient pour cible des centraux téléphoniques⁵⁶¹. La criminalité informatique s'adapte à son temps et aux évolutions de l'informatique. Elle a connu un

⁵⁵⁹ « Vengeances sur Internet. », http://www.murielle-cahen.com/p_vengeances.asp

⁵⁶⁰ Le terme de cybercriminalité voit le jour au milieu des années quatre-vingt-dix, avec la banalisation d'Internet. Elle couvre le même champ d'action que la criminalité informatique. Il s'agit selon Don Parker de « tout acte intentionnel associé d'une manière ou d'une autre à la technique informatique, dans laquelle une victime a subi ou aurait pu subir un préjudice et dans laquelle l'auteur a tiré ou aurait pu intentionnellement tirer profit » voire le site du ministère de l'intérieur français, www.interieur.gouv.fr. La cybercriminalité regroupe trois types d'actes : ceux qui prennent pour cible les ordinateurs ou systèmes, ceux qui utilisent les technologies comme moyen de commettre des actes délictueux de droit commun, ceux enfin qui utilisent les technologies comme vecteur de contenus informationnels illicites (pédophilie, racismes, etc.).

⁵⁶¹ Olivier Iteanu, Tous cybercriminels. La fin d'Internet ? Jacques-Marie Laffont Editeur. – L'une des plus célèbres attaques est celle de John Draper ; en 1971 il réussit à pirater des centraux téléphoniques pour réaliser des appels interurbains gratuits à l'aide d'une simple boîte de Captain Crunch dont il utilisait le sifflet qui reproduisait la tonalité exacte d'une fréquence téléphonique. Il fut arrêté et condamné à une peine de prison.

véritable essor avec l'avènement et la banalisation d'Internet. L'interconnexion des ordinateurs par le biais du réseau Internet, a amplifié la capacité de nuisances du piratage. L'accessibilité des nouvelles technologies a créé un déséquilibre entre les compétences informatiques nécessaires pour porter atteinte au réseau et l'ampleur des nuisances dont le cyberspace est victime. Il existe plusieurs formes de piratages informatiques, celles retenues pour cette étude seront le hacking et la diffusion de virus informatiques.

1. Le « hacking » et les notions voisines.

Dans l'idée commune, les hackers sont ceux qui utilisent les Nouvelles Technologies de l'Information à des fins contraires à la loi : ils se servent de leurs connaissances technologiques pour détruire, assujettir les réseaux, par cupidité ou simple malveillance. Tous les hackers sont assimilés à des terroristes du cyberspace. Cette croyance ne reflète pas l'entière réalité. Cette méconnaissance proviendrait du fait qu'il serait fait un amalgame entre la notion de hacker et des notions voisines.

1-a. Hacker.

Le terme hacker est apparu au début des années soixante quand un groupe de programmeurs du MIT (Massachusetts Institute of Technology⁵⁶²) décide de prendre ce nom. Dans un premier temps, ce terme désignait un étudiant imaginatif et audacieux, terme repris dans le jargon du Technical Model Railroad Club (TMRC)⁵⁶³. Le hacking consiste essentiellement à utiliser une machine à une autre fin que celle pour laquelle elle a été conçue à l'origine.

Le Jargon File des hackers les définit comme des « *individus qui programment avec enthousiasme et qui croient que le partage d'informations est un bien influent et positif et qu'il est de leur devoir de partager leur expertise en écrivant des logiciels libres et en facilitant l'accès à l'information ainsi qu'aux ressources informatiques autant que possible* »⁵⁶⁴. Aujourd'hui, un hacker désigne le plus souvent un spécialiste en informatique qui peut intervenir dans la programmation, l'administration ou la sécurité de systèmes et réseaux informatiques parce qu'il en connaît le fonctionnement interne. Les médias

⁵⁶² Le Massachusetts Institute of Technology (MIT) est une institution de recherche et une université américaine, spécialisée dans les domaines de la science et de la technologie. Située à Cambridge, dans le Massachusetts, à proximité immédiate de Boston, elle est considérée au XXI^e siècle comme la meilleure université occidentale en sciences et en technologies, <http://fr.wikipedia.org>

⁵⁶³ Un article de Wikipédia, Hacker., <http://fr.wikipedia.org/wiki/Hacker>

⁵⁶⁴ « Les hackers ces incompris », article publié le 24 mai 2003, http://crie-paca.org/article.php3?id_article=27

s'adressant à un large public, utilisent le terme hacker dans le sens de « hacker Black Hat » littéralement hacker à chapeau noir qui opère de façon illégale et non éthique.

L'idéologie du hacker serait de se dépasser et de trouver les failles des systèmes, sans en tirer un profit autre que celui de se voir reconnaître comme un hacker expérimenté par ses pairs. L'idéologie des hackers n'ait pas tournée sur elle-même. Toute personne même mineure qui a fait ses preuves, peut faire partie du cercle des hackers. La différence pour les mineurs se fera par leur capacité d'appréhension des risques qu'ils encourent.

En septembre 1997, l'US Air Force ayant repéré des intrusions sur certains de ses sites informatiques en provenance de la France, diligente une enquête menée par la section de la gendarmerie nationale de Paris en collaboration avec l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Cette enquête débouchera le 27 mars 1998 sur un vaste coup de filet. Parmi les personnes interpellées on compte deux mineurs et un jeune pirate. Interviewé, le père d'un des jeunes pirates Yoann, souligne le fait que son fils ne considérait pas ses activités comme délictueuses dès lors qu'elles n'étaient pas crapuleuses et ne visaient pas un profit mais plutôt la performance⁵⁶⁵. C'est un indice qui permet d'étayer ce que l'on sait de l'idéologie des hackers. Pour eux, le hacking n'est pas toujours assimilé à un crime. Yoann mis en examen pour son intrusion dans le système informatique de l'US Air Force, s'est vu ouvrir les portes d'une carrière d'informaticien avec pour seul CV cette intrusion⁵⁶⁶. Si un «heureux dénouement» est intervenu pour ce jeune hacker, il n'en demeure pas moins que l'intrusion sur un site est un délit qu'il y ait ou non détérioration et/ou vol d'informations. Un nombre croissant de génies précoces ou non en informatique utilise ce type de coup d'éclats afin de se faire remarquer par des entreprises soucieuses d'une sécurité optimale de leurs systèmes et réseaux informatiques.

Il existe une « éthique hacker » qui a été codifiée par Steven Levy⁵⁶⁷ selon les principes suivants :

- Toute information est par nature libre.

⁵⁶⁵ Le Figaro, 30 avril 1998, Christophe Doré, « Des pirates français poursuivis par les Etats-Unis ».

⁵⁶⁶ Suite à sa plus célèbre intrusion, il a été embauché par une entreprise spécialisée dans la sécurité informatique Roco Production, puis par Net Development créatrice de sites Internet et intranet, il va même écrire un livre en collaboration avec Alexandre Golovanivsky et Philippe Langlois (Chevaliers d'Internet et pirates informatiques, Editions N° 1, 239 p), Le Monde 4 mai 1999, Michel Alberganti, « Yoann, dix-sept ans, informaticien professionnel grâce au piratage ».

⁵⁶⁷ S. Levy, «Hackers: Heroes of the commuter revolution». Publié en 1984 in Garden City, New York par Anchor Press/Doubleday.

- Ne pas se fier à l'autorité, promouvoir la décentralisation.
- Les hackers peuvent se juger par leurs prouesses, non par d'autres hiérarchies sociales (ce qui permettra à un jeune prodige d'une dizaine d'années de rejoindre le groupe).
- Les ordinateurs peuvent changer et améliorer la vie.

Les premiers pirates se distinguaient par leurs dons en informatique, ils devaient tout concevoir. Ce n'est plus une donnée indispensable aujourd'hui ; Internet regorge de logiciels accessibles gratuitement et qui permettent de provoquer de sérieuses nuisances⁵⁶⁸ dans les réseaux.

A la lecture de ces éléments, les hackers sont présentés comme des « Robins des bois » du réseau. C'est l'idée qu'ils veulent véhiculer d'eux, pour enfin échappés à l'amalgame dont ils s'estiment les victimes lorsqu'ils sont identifiés à des cybercriminels. Par contre, il existe un groupe de pirates qui eux sont animés par la cupidité et la malveillance. Ils s'apparentent aux hackers, mais leur idéologie les distingue.

1-b. Les notions voisines.

Différents groupes de hackers peuvent être constitués en fonction de leur profil ou de leur idéologie ; en fonction de leur légalité ou de leur nuisance dans les réseaux informatiques.

- Les chapeaux blancs ou "white hats" sont souvent consultants en sécurité, administrateurs réseaux ou cyberpoliciers. Ils ont le sens de l'éthique et de la déontologie. Ce sont les hackers dans l'acception première de ce terme, telle qu'étudiée précédemment.
- Les chapeaux gris ou "grey hats" : bien qu'ils n'hésitent pas à pénétrer dans des systèmes sans y être autorisés, ils n'ont pas pour but de nuire. C'est souvent « l'exploit informatique » qui les motive, une façon de faire la preuve de leur agilité.
- Les chapeaux noirs ou "black hats" : créateurs de virus, cyber-espions, cyber-terroristes et cyber-escrocs, eux sont nuisibles et n'ont aucun sens de l'éthique. Ils correspondent à la définition du « pirate ». Dans cette catégorie on compte les crackers, les Script-kiddies.

⁵⁶⁸ Daniel Martin et Frédéric-Paul Martin, Cybercrime : menaces, vulnérabilités et ripostes, PUF 2001, p.75.

1.b'. Les Crackers

C'est un terme qui a été forgé en 1985 par les hackers en réponse à la mauvaise utilisation du mot hacker dans la presse. Le cracking touche le domaine de la contrefaçon. Il est quasiment né en même temps que l'informatique. Il consiste à débrider des programmes, « casser » littéralement le code d'entrée en vue d'une copie libre notamment. Il y a les crackers qui se veulent idéalistes qui s'attaquent aux grands développeurs de logiciels. Ils ont à cœur de mettre à la disposition de la communauté les logiciels ainsi récupérés sur Internet. D'autres crackers moins scrupuleux (dans leur majorité) font commerce de leurs talents au service de fabricants concurrents⁵⁶⁹. Il s'agit indubitablement d'espionnage. La catégorie la plus courante de crackers à ce jour est celle qui détournent les numéros de cartes bancaires sur Internet, ceux qui en cassent les codes ou fabriquent de fausses cartes bancaires qu'ils utilisent pour des achats en ligne. Cette catégorie de pirates, par ailleurs bannie par les vrais pirates, travaille à son compte, ou pour des entreprises et se rémunère sur ses victimes. Ces pirates se livrent grâce aux informations frauduleusement recueillies à des chantages, demandent des rançons, utilisent les cartes bancaires dont les numéros ont été interceptés, etc. Ils n'hésitent pas à détruire les logiciels et les données⁵⁷⁰ dont ils auront cassé les codes.

1.b''. Les Script-kiddies⁵⁷¹

Ils ont pour objectif de nuire par le biais de programmes dont ils ne sont pas les propriétaires, programmes qu'ils ont en général glané sur Internet. Script kiddie est un terme péjoratif désignant les pirates informatiques néophytes qui, dépourvus des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou programmes mis au point par d'autres. On pourrait traduire l'expression par « Gamin utilisateur de scripts », mais le terme « script kiddie » est le seul couramment utilisé. Malgré leur niveau de qualification faible voire nul, les script-kiddies sont parfois une menace réelle pour la sécurité des systèmes. Outre le fait qu'ils peuvent du fait de leur incompetence altérer des données de système par inadvertance, les script-kiddies sont très nombreux et sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir. Il existe plusieurs types de script-kiddies mais on retrouve chez la plupart d'entre

⁵⁶⁹ L'Hebdo n° 7 – 17 février 2000, « Pirates : Des crimes et des châtements », Cathy Macherel en collaboration avec Nicolas Willemin et Frédéric Blassel., http://www.webdo.ch/hebdo/hebdo_2000/hebdo_07/hacking5_07.html

⁵⁷⁰ Daniel Martin et Frédéric-Paul Martin, Cybercrime : menaces, vulnérabilités et ripostes, op.cit., p.76.

⁵⁷¹ Traduire kiddie de manuscrit (de temps en temps lapin de manuscrit, skidie, kitty de manuscrit, juvénile

eux un manque de reconnaissance sociale. Ils sont d'ailleurs même reniés par la plupart des communautés de pirates⁵⁷². Ces techniques sont directement nuisibles à autrui. Il existe dans le cyberespace, diverses méthodes de nuisances visant des domaines et droit variés. Le droit d'auteur fait partie des droits subissant un nombre croissant d'atteintes. Le téléchargement illégal est une des atteintes majeures à laquelle doivent faire face les auteurs et leurs représentants ou ayant-droits.

2. Le téléchargement illégal.

Le téléchargement illégal en ligne est le fait de copier et de partager illégalement des contenus protégés par des droits d'auteur à des fins commerciales ou personnelles. Cela inclut toute personne qui télécharge de la musique, des films, des jeux ou des logiciels sans autorisation du détenteur des droits et toute personne qui partage de la musique, des films, des jeux et des logiciels qui lui appartiennent⁵⁷³ certes mais dont la finalité n'est pas d'être copiés de manière illimitée en vue de distribution rémunérée ou non.

Le pionnier du téléchargement illégal est Napster⁵⁷⁴. L'ancêtre du système de peer to peer voit le jour en 1998. Le téléchargement illégal sera conforté par l'avènement du format MP3⁵⁷⁵ qui du fait qu'il allège considérablement les fichiers musicaux, en favorise le transport devenu plus aisé et rapide. Après deux ans de service, Napster sera contraint de cesser toute activité par les syndicats des éditeurs de musique américains pour cause de non respect de la législation sur les droits d'auteur. En 2002 apparaît la technique du peer to peer (P2P)⁵⁷⁶.

⁵⁷²Récupéré sur http://fr.wikipedia.org/wiki/Script_kiddie

⁵⁷³ Source Site Microsoft Sécurité ; 14 décembre 2004 ; « Eviter le piratage en ligne à la maison : Apprenez à vos enfants à ne pas télécharger ou partager de films, de musique, ni de logiciels illégalement », <http://www.microsoft.com/france/securite/gpublic/children/kidpiracy.mspx>

⁵⁷⁴ Shawn Fanning de son surnom Napster est un jeune génie américain de dix-sept ans qui dans l'idée de rendre un service à son colocataire en quête de sa musique préférée sur Internet, va créer un logiciel capable de télécharger et échanger rapidement des fichiers musicaux avec d'autres passionnés sur la toile. C'est la création du premier logiciel peer to peer c'est-à-dire de personne à personne ou de poste à poste. Cet adolescent créera par la suite avec son oncle l'entreprise Napster. Olivier Iteanu, Tous cybercriminels. La fin d'Internet ? préc., p.194-195.

⁵⁷⁵ Motion Picture Experts Group Audio Player 3, c'est un format de fixation et de compression du son.

⁵⁷⁶ Système de partage de fichiers entre internautes, grâce à ce système pas de serveur, vous accédez directement à la machine d'un autre utilisateur. En devenant client de KaZaA ou Edonkey, vous ouvrez tout ou partie de votre disque dur aux autres membres, mettant ainsi vos fichiers en réseau. Lorsque vous émettez une requête de film, chanson ou tout autre document, votre ordinateur va chercher en cascade dans les fichiers partagés par tous les clients. Il affiche alors une liste de fichiers correspondants à la demande et vous faites « votre marché » en fonction du débit et de la qualité proposée par les membres.

Autrement, le peer-to-peer est un réseau d'échange et de partage de fichiers entre internautes. Le principe du peer-to-peer (P2P) est de mettre directement en liaison un internaute avec un autre internaute qui possède un fichier convoité. Il existe 2 méthodes pour accomplir cette tâche : 1/ La méthode centralisée est basée sur un ou

Avec cette nouvelle technologie, le téléchargement illégal d'œuvres (musique, film, jeu vidéo...) prend une nouvelle dimension sur Internet. Des milliers de jeunes peu conscients des risques⁵⁷⁷, se laissent tenter à échanger pensent-ils en toute impunité des milliers de fichiers musicaux, cinématographiques, etc.

Le téléchargement illégal constitue une violation du droit d'auteur et est puni comme un acte de contrefaçon. L'article L.122-4 du code de la propriété intellectuelle énonce que : « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits ou ayants cause est illicite ». Les sanctions encourues sont lourdes et peuvent être de natures pénale et/ou civile. La loi Perben II du 9 mars 2004 a aggravé les sanctions. L'article L.335-2 prévoit une peine de 3 ans d'emprisonnement et 300.000 € d'amende. Seront punis des mêmes peines le débit, l'exportation et l'importation des œuvres contrefaites. Lorsque les délits ont été commis en bande organisée la peine est portée à 5 ans d'emprisonnement et à 500.000 € d'amende. Sur le plan pénal, le mineur doit assumer sa condamnation sauf hypothèse où le piratage s'est fait à partir d'une connexion Internet au nom de l'un des parents. Celui-ci pourrait se voir accuser d'en être l'auteur sauf à démontrer que son enfant a agi totalement à son insu⁵⁷⁸. S'agissant de la responsabilité civile, les dommages et intérêts pour réparation du préjudice sont calculés en fonction du nombre de fichiers téléchargés et/ou revendus. Pour le mineur infracteur, ce sont les parents qui devront payer, conformément à leur responsabilité civile du fait de leurs enfants mineurs.

Le délit et les peines associées s'appliquent également à celui ou celle qui a mis le fichier en partage, c'est-à-dire celui qui a mis à disposition un fichier piraté au téléchargement des internautes⁵⁷⁹.

La technique du peer to peer n'est pas *a priori* illégale. La loi est simple ; il est possible de graver un CD ou de le transformer en MP3 si et seulement si il a été légalement acheté, si les droits en ont été légalement acquis par téléchargement. Il faut préciser que cette copie ne doit

plusieurs serveurs qui possèdent la liste des fichiers partagés et qui orientent les internautes vers l'internaute possédant le fichier convoité. 2/ La méthode décentralisée utilise chaque internaute comme un mini-serveur et ne possède aucun serveur fixe. Cette méthode a l'avantage de répartir les responsabilités et d'éviter les actions en justice. Voir site Dico du Net.

<http://www.dicodunet.com/annuaire/def-464-peer-to-peer.htm>

⁵⁷⁷ Selon le Centre de recherche pour l'étude et l'observation des conditions de vie, en juin 2003 30% des internautes français auraient déjà téléchargé de la musique, des films ou des logiciels selon le mode du peer to peer : www.credoc.asso.fr

⁵⁷⁸ Source Téléchargement illégal : attention à la répression.

http://www.cyberjeune.org/ddj/44_telechargement.html

⁵⁷⁹ Olivier Iteanu, Tous Cybercriminels. La fin d'Internet ? préc., p.198-199.

être destinée qu'à un usage personnel⁵⁸⁰ et privé, c'est-à-dire que si on mettait la copie à la disposition d'autres internautes on se mettrait en situation illégale.

Lors des débats pour l'adoption de la Loi pour la confiance dans l'économie numérique on a pu croire à une légitimation, ou du moins un adoucissement des sanctions à l'encontre du téléchargement illégal. Il a été question de la licence globale que d'aucuns ont qualifié de licence de téléchargement. L'idée était de permettre un téléchargement illimité moyennant une cotisation ou une redevance mensuelle comprise dans son abonnement Internet. Cette disposition n'a pas été retenue dans la mouture finale de la loi.

L'exception de copie privée contribue à limiter la portée de l'illégalité du téléchargement. Il y a en effet une tolérance pour ceux qui copient pour un usage personnel et privé à condition qu'ils aient acquis préalablement et légalement l'œuvre copiée.

Il existe des hypothèses aggravantes à cette cybercriminalité (téléchargement illégal) : la représentation publique :

- La première hypothèse : diffuser lors d'une fête payante (par exemple) sa collection de MP3 illicite. Les mêmes textes que précédemment s'appliquent, les juges peuvent cependant les appliquer avec plus de sévérité⁵⁸¹.
- La deuxième hypothèse : revendre des CD gravés de plusieurs fichiers illicites. Dans ce cas le risque d'être poursuivi est plus grand car l'infracteur s'affranchit d'un usage privé pour réaliser un commerce. La sanction est alourdie avec de possibilité de prononciation de peines d'emprisonnement ferme.

Le fait de partager et conserver des fichiers illégaux peut être considéré comme du recel⁵⁸² puni de 5 ans d'emprisonnement et 375 000 euros d'amendes. Cette disposition est opposable au mineur qui bénéficie de téléchargements illégaux ou au parent qui l'a laissé faire en connaissance de cause.

⁵⁸⁰ Art. L.122-5-5° du Code de la propriété intellectuelle.

⁵⁸¹ Art. L.122-4 du Code de la propriété intellectuelle.

⁵⁸² Article 321-1 du code pénal, le recel est le fait de « *dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait en connaissance de cause, de bénéficier, par tout moyen d'un crime ou d'un délit* ».

La responsabilité des parents du mineur a son origine dans l'article 1384 alinéa 4 du code civil. Les parents doivent assumer l'entière responsabilité civile des dommages causés par leurs enfants mineurs. En son alinéa 7, cet article donne une possibilité aux parents de s'exonérer de leur responsabilité à l'unique condition qu'ils prouvent qu'ils « n'ont pu empêcher le fait qui donne lieu à cette responsabilité ». En l'état actuel des techniques de contrôle mises à la disposition des parents pour les activités de leurs enfants mineurs sur Internet, il leur sera quasiment impossible de s'exonérer de leur responsabilité.

L'exception de copie privée à usage personnel et dans le strict cadre familial a été invoquée comme moyen de défense pour innocenter les utilisateurs de peer to peer. Mais c'est difficilement recevable étant donné l'illicéité originelle du fichier en question. Il en est de même pour les fichiers illégalement téléchargés et stockés sur des CD audio.

S'agissant du téléchargement, deux courants s'affrontent traditionnellement ; les tenants de la légalité qui, s'appuyant sur le respect des droits d'auteurs et sur l'équilibre d'une économie artistique fustigent le téléchargement illégal. Parallèlement, les défenseurs du téléchargement illégal, considérant ce dernier comme un fait de société indépassable et qui soutiennent qu'il conviendrait de l'entériner⁵⁸³.

Un internaute sur trois fréquente les réseaux peer to peer, soit environ huit millions de personnes en France⁵⁸⁴. Julien Dourgnon le Directeur des études et de la communication de l'association de consommateur « UFC – Que Choisir ? » souligne l'ampleur de cette pratique. En guise d'exemple, elle cite une étude allemande qui révèle qu'un tiers des téléchargeurs illégaux a moins de dix-huit ans outre Rhin. Un nombre important de ces téléchargeurs sont très jeunes c'est-à-dire âgés de huit à dix ans. Le Centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC)⁵⁸⁵ en France, corrobore ces résultats en indiquant que 31% des 12-17 ans avouent avoir déjà téléchargé de la musique, des films ou

⁵⁸³ Conférence de la famille 2005, « Protection de l'enfant et usages d'Internet », Rapport de propositions remis à Philippe Douste-Blazy, par le Président du groupe de Travail Joël Thoraval (Président de la Commission nationale consultative des droits de l'homme) et le rapporteur Olivier Peraldi (Adjoint au Délégué interministériel à la famille).

⁵⁸⁴ Op. cit.

⁵⁸⁵ Le CRÉDOC, Centre de Recherche pour l'Étude et l'Observation des Conditions de Vie, est un organisme d'études et de recherche au service des acteurs de la vie économique et sociale.

des logiciels peer to peer sans préciser cependant si les téléchargements étaient ou non légaux⁵⁸⁶.

Pour résumer, l'internaute (mineur) qui télécharge et partage des fichiers illégaux est responsable de ses actes ; il pourra être poursuivi pour délit de contrefaçon, recel voire délit en bande organisée selon les circonstances.

En France jusque là, seuls les internautes tirant profit de ces téléchargements pouvaient être sanctionnés. Ceux qui se contentaient de télécharger pour leur usage personnel n'étaient pas visés par les autorités judiciaires. La donne a changé avec la décision du Tribunal correctionnel de Vannes du 29 avril 2004 qui a condamné six internautes français à des peines de prison avec sursis et des amendes de plusieurs milliers d'euros pour avoir téléchargé des films sur Internet via un réseau Peer to Peer.

Outre la responsabilité des internautes, les créateurs de logiciels peer to peer ont vu leur responsabilité engagée en matière de téléchargement illégal. Ce fut les cas pour Napster dont le logiciel reposait sur une technologie centralisée permettant le contrôle des contenus échangés. C'est sur ce fondement que Napster a été condamné aux Etats-Unis. Par contre, s'agissant de KaZaA, son système étant décentralisé, il lui est techniquement impossible de contrôler le contenu des fichiers téléchargés. C'est pour cette raison que les tribunaux néerlandais ont déclaré le 28 mars 2002 et le 19 décembre 2003 que KaZaA ne pouvait être tenu responsable des utilisations illicites qui étaient faites de son logiciel. La responsabilité retombe donc sur les internautes qui en font usage.

Le Forum des droits sur Internet en partenariat avec les ministères de la culture et de la communication et de l'éducation nationale, soutenu par l'UNAF⁵⁸⁷ et l'ADAMI⁵⁸⁸ a publié un document d'information et de sensibilisation des adolescents aux conséquences du téléchargement illégal⁵⁸⁹.

L'arsenal juridique sanctionnant le téléchargement illicite sur Internet repose sur plusieurs textes. La Loi sur la confiance dans l'économie numérique du 21 juin 2004 met l'accent sur la prévention, la cessation des comportements illicites plus que sur la sanction juridique. Cette

⁵⁸⁶ Conférence de la famille 2005, « Protection de l'enfant et usages d'Internet », op.cit.

⁵⁸⁷ Union Nationale des Associations Familiales

⁵⁸⁸ Société civile pour l'Administration des Droits des Artistes et des Musiciens Interprètes

⁵⁸⁹ *Adopte la net attitude !* Forum des droits sur Internet.

loi ordonne aux intermédiaires de procéder à des campagnes de sensibilisation en faveur du téléchargement légal ; en cas de délit, le juge pourra imposer aux hébergeurs ou aux FAI un filtrage des contenus contrefaisants, leur ordonner en urgence de prévenir ou mettre fin aux infractions. La loi du 29 juillet 2004 relative aux communications électroniques et aux services audiovisuels (LCE) prévoit par ailleurs, la possibilité pour les FAI de résilier unilatéralement le contrat d'abonnement d'une personne condamnée pour piraterie. Le téléchargement illégal est à classer dans les cyber délits qui sévissent dans le cyberespace. Les nuisances informatiques quant à elles, concernent les internautes à tous les niveaux, en tant qu'infracteur et en tant que victimes des infractions.

B. Les nuisances informatiques.

Les nuisances informatiques visent comme leur nom l'indique à générer nuisance et gêne pour les internautes. A la différence du téléchargement illégal qui vise en premier un profit personnel, les intentions à l'origine des nuisances informatiques dont il va être ici question sont purement malveillantes. C'est le cas lorsque l'on tente de paralyser une messagerie ou un système informatique par un envoi massif de messages ou, lorsque l'on crée un virus dont la seule fonction est de détruire des systèmes.

1. Le spamming et l'e-mail bombing.

D'un point de vue technique et du point de vue du résultat obtenu (le blocage d'une boîte e-mail ou d'un site Internet), ces deux procédés sont comparables. Ce qui les différencie c'est la motivation et l'objectif qui les sous-tendent. Dans les deux cas il y a une volonté de nuisance par un envoi massif de mails. L'une des méthodes a un objectif directement ou non commercial (le spamming) tandis que l'autre s'apparente plus à du terrorisme électronique (l'e-mail bombing).

1-a. Le spamming.

Spam est un acronyme qui vient de SPice hAM⁵⁹⁰ jambon en boîte vendu aux Etats-Unis dans les années soixante-dix et ayant de réputation très mauvais goût.

⁵⁹⁰ Littéralement, « jambon épice » en anglais, en français courrier non sollicité ou pourriel.

Le spamming c'est l'envoi de plusieurs milliers d'e-mails dans le but de surcharger le serveur visé. Très simple à mettre en œuvre, cette technique ne requiert que de tous petits programmes facilement accessibles. Les plus connus portent des noms éloquentes comme UNAbomber, Avalanche ou Homicide⁵⁹¹. Les particuliers ne sont pas épargnés avec comme conséquence : perte de temps, boîte à lettre électronique saturée, confusion entre les messages utiles et les messages non sollicités.

La Cnil a rendu un rapport en la matière en novembre 2002 consultable sur son site⁵⁹². Ce rapport conclut que 95% des courriers non sollicités sont en langue étrangère. Les messages à caractère sexuel constituent 42% des spams, les spams financiers constitueraient 40% des spams. La Cnil définit le spamming comme étant « l'envoi de messages électroniques à un ou plusieurs destinataires dont le nombre peut varier de quelques dizaines à plusieurs centaines de milliers, voire plusieurs millions. Il repose sur la collecte préalable d'adresses électroniques (e-mails) auxquelles seront adressés des messages électroniques ».

Une distinction doit être effectuée entre le spamming fait avec l'intention d'accéder frauduleusement à un système ou de l'obstruer et, celui qui répond à des considérations d'ordre commercial.

Le spamming qui vise l'accès frauduleux à un système ou l'obstruction de ce dernier est sanctionné pénalement par les tribunaux qui y voient un accès frauduleux dans un système de traitement automatisé ayant causé son altération (code pénal article 323-1 alinéa 2⁵⁹³), ou bien une entrave au fonctionnement d'un système de traitement automatisées des données (code pénal article 323-2)⁵⁹⁴.

On pourrait se poser la question de savoir quel rôle pourrait avoir à jouer le mineur dans cette diffusion qui semble être plus le fait de professionnels en tirant profit que de particuliers isolés. Sa responsabilité peut être engagée au titre de relais de Spam, notamment en ce qui concerne les *hoax*.

⁵⁹¹ L'Hebdo, Cathy Macherel, Nicolas Willemin, Frédéric Blassel, 17 février 2000, « Des crimes et des châtements ».

http://www.webdo.ch/hebdo/hebdo_2000/hebdo_07/hacking5_07.html

⁵⁹² www.cnil.fr

⁵⁹³ Tribunal correctionnel Lyon, 20 février 2001 : Comm. com. électr. Janvier 2002, commentaire n°5, observation Ch. Le Stanc ; JCP E 2002, p.78, observations A. Bertrand-Doulat. Il y a eu suite à cette décision une condamnation de 8 mois de prison avec sursis et une amende à l'époque de 20 000 francs.

⁵⁹⁴ TGI Paris, 12^e chambre correctionnelle, 24 mai 2002 : www.01net : 4 mois de prison avec sursis et 20 000 euros de dommages et intérêts à la partie civile.

Le **hoax** est un Spam ayant pour origine un canular. Le spammeur est généralement un de vos contacts qui a lui-même été victime dudit hoax. La méthode de diffusion est celle du *forward* (faire suivre). Ce type de Spam surfe sur la culpabilisation ou la stigmatisation par la menace de malédiction à défaut de faire suivre le message. On sollicite la naïveté des internautes. Le message prend sa pleine mesure étant donné qu'il est préconisé de l'envoyer à un maximum de personnes (minimum 5 ou 10) sous peine de malchance. Il peut être dupliqué indéfiniment par des personnes qui n'entendent pas rompre la chaîne de solidarité ou de chance, ce faisant les relayeurs contribuent à saturer votre boîte de réception électronique. La simple diffusion de messages en chaîne (quelle qu'en soit la nature) permet-elle que l'on engage sa responsabilité au même titre qu'un spammeur ? C'est peu probable. Il faut que soient remplies les conditions majeures de l'infraction :

- L'altération d'un système automatisé par un accès frauduleux. Dans la technique du "forward", il n'y a pas d'accès frauduleux, puisqu'il s'agit de réexpédier le message que l'on a soit même reçu à des personnes dont-on légalement les adresses e-mails.
- Il faut entraver le fonctionnement d'un système de traitement automatisé des données. Or chacun de nos contacts, ne recevra qu'une seule fois le message "forwardé" ; ce qui n'est pas de nature à paralyser le fonctionnement de son système.

Il est toutefois possible à l'internaute mineur, dans une démarche malveillante d'inonder la boîte de réception d'une personne physique ou morale au point de paralyser celle-ci par le procédé de l'e-mail bombing.

1-b. L'e-mail bombing.

Cette pratique consiste à envoyer un même message de manière répétée à une personne déterminée, le but étant d'inonder la boîte électronique du destinataire au point de la bloquer. A la différence du spamming souvent de nature publicitaire, l'e-mail bombing a pour unique but de saturer un serveur afin d'en empêcher le fonctionnement normal. L'article 323-2 du code pénal sanctionne cette pratique en énonçant que : « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000€ d'amende* ». Il faut s'appuyer sur l'article 1382 du code civil

pour demander réparation du préjudice lié à la perte de la messagerie, même si celle-ci est gratuite⁵⁹⁵. Le mineur auteur d'une telle infraction engage sa responsabilité pénale et civile⁵⁹⁶.

La difficulté réside dans l'identification de l'auteur de l'e-mail répété, il existe en effet des logiciels spécifiques qui permettent d'agir de manière anonyme⁵⁹⁷.

L'e-mail bombing est présenté par ses défenseurs comme un moyen de faire une "e-manifestation", de mettre en œuvre son droit de pétition et d'expression. La première décision sur l'e-mail bombing a été rendue par le premier vice-président au Tribunal de grande instance de Paris le 26 mai 2003⁵⁹⁸. Cette décision n'a pas retenu la qualification d'e-manifestation, par conséquent il n'a pas été reconnu à l'email bombing la qualité d'un exercice normal et justifié de la liberté d'expression. Ces "e-manifestations" constituent encore aujourd'hui une arme de protestation des internautes dont les cibles varient au gré de l'actualité. Toute personne ayant participé à cet envoi massif est considérée comme auteur ou coauteur de l'infraction.

Il est possible de poursuivre des internautes animés d'intention de nuire sur le fondement de l'article 323-2 du code pénal⁵⁹⁹, lorsqu'ils auront volontairement entravé le fonctionnement d'installations informatiques. C'est ainsi que le Tribunal de grande instance de Paris a condamné un internaute ayant pratiqué du « mail bombing » à 4 mois de prison avec sursis ainsi qu'à payer 20 000 euros de dommages et intérêts au fournisseur d'accès Noos dont les

⁵⁹⁵ Olivier Iteanu, Tous cybercriminels. La fin d'Internet ? préc., p.115.

⁵⁹⁶ Voir en supra les paragraphes sur la responsabilité civile du mineur ou de ses tuteurs légaux au regard des infractions que ce dernier commet.

⁵⁹⁷ TGI de Paris 12^e chambre, 24 mai 2002, un jeune technicien en informatique a été condamné à quatre mois de prison avec sursis et 20 000 euros d'amende pour avoir nui au fonctionnement du système de messagerie du fournisseur d'accès Internet Noos après avoir expédié au même internaute le même e-mail en plusieurs centaines de milliers d'exemplaires, Source ZdNet.

⁵⁹⁸ Par une ordonnance de référé du TGI de Paris du 26 mai 2003, FSU et autres c/ La Droite Libre, www.legalis.net, le Président du TGI a dit que le blocage des messageries dont il avait à connaître « caractérise une intention malicieuse » de la Droite Libre qui visait à perturber le fonctionnement des syndicats. Il en conclut que cette action ne peut se prévaloir d'un exercice normal de la liberté d'expression. Il précise que cette action, en privant « les demandeurs de l'usage des services de courrier électronique dont ils ont une possession légitime » a « constitué un trouble manifestement illicite auquel il doit être mis fin ». L'association la Droite Libre entendant réagir face aux grèves dans les Transports et l'Éducation nationale lance une e-manifestation consistant à susciter un envoi massif de messages électroniques modélisés vers une quarantaine d'adresses électroniques d'organisations et de responsables syndicaux. Il y avait eu un précédent dès la seconde fête d'Internet en mars 1999, une association d'internautes, l'ADIM aujourd'hui disparue avait lancé la première e-manifestation contre le prix trop élevé de l'accès à Internet par France Télécom.

⁵⁹⁹ Article 323-2 : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.* »

serveurs étaient restés bloqués pendant une dizaine d'heures⁶⁰⁰. De telles pratiques quoique préjudiciables n'auront en pratique pour résultat qu'un blocage momentané du système informatique ou de la messagerie. Par contre, il existe une cybercriminalité qui peut avoir des résultats plus dramatiques allant jusqu'à la destruction d'un ou de plusieurs systèmes informatiques : les virus informatiques.

2. La création et la diffusion de virus informatiques.

A la question « Quelles sont les principales menaces auxquelles vous êtes confrontés ? » Les virus sont perçus comme la menace principale à 85,5%⁶⁰¹ par les internautes. La criminalité informatique a pris un tournant avec la vulgarisation de la micro-informatique. Les premiers virus informatiques ont faits leur apparition au début des années soixante-dix. La diffusion et la propagation des virus informatiques se sont révélées être parmi les crimes informatiques les plus nuisibles du réseau informatique. Outre la nuisance pour les internautes, elles génèrent de lourdes conséquences économiques. On compterait aujourd'hui dans le monde plusieurs dizaines de milliers de virus informatiques actifs et en circulation. L'introduction de virus, vers, bombes logiques, chevaux de Troie est réprimée par l'article 323-3 du code pénal qui punit de trois ans d'emprisonnement et de 45 000 euros d'amende le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données⁶⁰².

Le virus par analogie au terme médical est un programme malicieux. Le virus informatique peut être défini comme un logiciel dont la particularité est qu'il se transmet et se reproduit ; avec le temps il mute en ver et se propage désormais par le biais de réseaux. Il comporte des fonctions nuisibles pour le système⁶⁰³. Il contamine le programme et se propage en se recopiant sur un programme pour se déclencher ensuite à la manière de la bombe logique⁶⁰⁴. Il peut être dormant ou polymorphe c'est-à-dire qu'il est capable de se mettre en sommeil pendant une durée indéterminée ou changer de forme pour tromper les défenses⁶⁰⁵. L'évolution des techniques a mis à la portée de tous, la création de virus. Il est aisé même par inadvertance de créer un virus.

⁶⁰⁰ Source : site du Forum des droits d'Internet, www.foruminternet.org, rubrique actualités 24 mai 2002.

⁶⁰¹ Olivier Iteanu, Tous cybercriminels, préc.,

⁶⁰² D. Martin et F.-P Martin, Cybercrime : menaces, vulnérabilités et ripostes, préc., p.165.

⁶⁰³ D. Martin, La criminalité informatique, PUF, 1997.

⁶⁰⁴ La bombe logique est un programme de destruction qui s'exécute lors de l'apparition ou de l'absence d'un événement. Cette application qui peut être destructrice par l'effacement d'informations ou non destructrice par l'interruption de programmes, attend généralement une date précise pour se déclencher. Pour un effet plus destructeur, la bombe logique peut être associée à un cheval de Troie »

⁶⁰⁵ Olivier Iteanu, Tous cybercriminels, préc., p.175.

La création de virus obéit à plusieurs motivations :

- Acte de revanche contre une entité dont on va tenter de détruire le système.
- Acte de revendication : sont souvent visé des groupes emblématiques dont le cybercriminel entend combattre l'idéologie ou l'hégémonie.
- Acte de défi, pour ceux pour qui la paralysie d'un système informatique vaudra un CV ; puisque après l'attaque qui n'a pour autre but que de démontrer la vulnérabilité du système, il propose la solution.
- Acte mafieux, puisque après la création et l'injection d'un virus dans un système informatique il y a réclamation d'une rançon pour remettre en état le système.

En son temps, il avait été intégré au programme de l'Université de Calgary au Canada, dans le cadre d'un nouveau cours de sécurité informatique d'apprendre à quelques étudiants à créer des virus, chevaux de Troie et d'autres applications menaçant la sécurité des réseaux, afin d'être plus aptes à les combattre⁶⁰⁶.

Qu'elle soit d'inspiration malveillante ou non, la création et la diffusion présentent pour les créateurs et les diffuseurs de virus informatiques des points communs : le défi, l'émulation résidant dans le fait d'être toujours plus performant que les autres. La compétence est le maître mot. Les créateurs de virus s'admirent et se concurrencent quelle que soit leur moralité respective, c'est la compétence indépendamment de tout autre facteur (âge, motivations, etc.) qui importe.

Le mineur est un internaute pourvu de droits et d'obligations dans de sa navigation dans le cyberspace dont-il doit répondre. Il en est un acteur à part entière, même si des aménagements sont parfois nécessaires pour prendre en considération son statut juridique. Le mineur peut se prévaloir de droits et d'obligations dans le cyberspace, dans le même temps les tiers peuvent se prévaloir de droits et obligations à son égard.

⁶⁰⁶ Cette nouvelle très critiquée, notamment par certaines compagnies d'anti-virus qui considéraient qu'apprendre aux étudiants à créer des virus, ainsi que d'autres applications potentiellement destructrices, représentait un risque inutile. Selon ces mêmes compagnies, il est tout à fait possible de combattre les virus sans jamais en avoir créé. Toutefois, le cours devait comporter un volet légal afin de responsabiliser les étudiants et les informer qu'ils risquaient des peines civiles et pénales s'ils laissaient s'échapper une de leurs créations

DEUXIEME PARTIE : LES DROITS ET OBLIGATIONS DES TIERS A L'ÉGARD DU MINEUR DANS LE CYBERESPACE.

Le développement exponentiel d'Internet s'est accompagné d'un développement quasi équivalent des délits et infractions commis dans le cyberspace. Pour lutter contre l'idée d'une impunité supposée ou avérée sur Internet, le choix a été fait d'une responsabilisation accrue de toute la chaîne des acteurs du cyberspace : de l'auteur de l'infraction aux utilisateurs victimes en passant par tous les intermédiaires. Il faut reconnaître que les conséquences des actes délictueux ne sont plus uniquement à la charge du cybercriminel⁶⁰⁷. Tout acteur de la chaîne peut engager sa responsabilité directement ou non : les parents peu regardants ou peu vigilants sur l'activité de leurs enfants mineurs sur Internet, les intermédiaires techniques et les cybercriminels.

⁶⁰⁷ Olivier Iteanu, Tous Cybercriminels. La fin d'Internet ? Préface de Daniel Hurel, Directeur général de Risc Technology France.

Titre 1. LES TUTEURS LÉGAUX RESPONSABLES DES MINEURS.

Le mineur est un sujet de droit. En tant que tel il dispose de droits et devoirs juridiques inhérents à ses activités. Pour autant, la particularité de sa personnalité juridique fait qu'il doit bénéficier d'une protection accrue tant de ses tuteurs légaux que de la loi⁶⁰⁸. Il ne s'agit pas de le déresponsabiliser, mais simplement de le protéger parfois par devers lui, d'infractions dont il pourrait être la victime ou l'auteur dans le cyberspace. Pour assurer la sécurité du mineur dans le cyberspace il y a un certain nombre de mesures de protection à mettre en œuvre pour protéger ce dernier dans le cyberspace. En plus de ces mesures de protections, les parents ou tuteurs légaux du mineur peuvent personnellement voir leur responsabilité engagée pour ou à cause de la protection du mineur.

⁶⁰⁸ Le mineur comme le rappelle la définition est « une personne physique qui n'a pas atteint l'âge de la *majorité* légale et que la loi en raison de son jeune âge place sous un régime de protection et prive de la possibilité d'exercer elle-même ses droits (c'est-à-dire qui est frappé d'une incapacité d'exercice) », Dictionnaire du vocabulaire juridique sous la direction de Rémy Cabrillac, Juris classeur, Litec.

Chapitre 1. LES MOYENS DE PROTECTION DU MINEUR DANS LE CYBERESPACE.

La protection de l'enfance est un objectif politique majeur commun à toutes les démocraties. En 1924, la déclaration de Genève marque la première tentative de codification des droits fondamentaux des enfants. En 1989, la Convention internationale sur les droits de l'enfant consacre l'enfant comme personne spécifique à protéger⁶⁰⁹. Ces textes révèlent la volonté des Etats signataires de mieux organiser la protection des mineurs. Le monde virtuel ne fait pas exception à cette volonté. La banalisation d'Internet a mis en lumière la nature et l'ampleur des dangers courus par les mineurs surfant dans le cyberespace. Force est de constater la portée limitée des réglementations organisant la protection des mineurs dans le cyberespace. Les justifications sont nombreuses et tiennent pour l'essentiel à la nature et au fonctionnement du cyberespace :

- la mutation continue et rapide des technologies d'Internet que les réglementations et les organismes de répression ont du mal à suivre ;
- l'adaptabilité des cybercriminels qui eux n'ont aucun mal à s'approprier les évolutions de la technologie d'Internet au service de leurs crimes ;
- l'immatérialité, la volatilité et la nature transfrontalière des contenus du cyberespace qui rendent le travail des enquêteurs et des juges difficile, etc.

La protection des mineurs doit faire intervenir tous les acteurs directs ou indirects du cyberespace (les parents et/ou tuteurs légaux, les intermédiaires, etc.). Cette intervention doit idéalement survenir avant la commission des infractions par ou contre le mineur. La protection des mineurs ne peut pas être du seul ressort du législateur ou de la justice dont l'intervention ne survient qu'après la commission des infractions. Pour être efficace, la protection des mineurs dans le cyberespace doit mobiliser tous les moyens et acteurs avant et après la commission des infractions dans le cyberespace.

⁶⁰⁹ Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur Internet. Publication 11.02.2004.

§1. La protection *a priori* du mineur dans le cyberspace.

Il est indubitable que la protection des mineurs dans le cyberspace suppose une bonne connaissance de l'outil qu'est Internet et des dangers qu'il présente pour eux. Le handicap avéré des tuteurs du mineur, est pour certains une connaissance superficielle d'Internet. Le premier pas vers une protection optimale des mineurs passe par une sensibilisation sur Internet dans toutes ses facettes. Cette sensibilisation doit viser conjointement les mineurs qui bien que maîtrisant les fonctionnalités d'Internet n'en appréhendent pas toujours très bien les dangers et les implications juridiques et leurs tuteurs légaux. Il s'agit de réconcilier les familles autour de l'utilisation d'Internet. Pour ce faire de grandes campagnes de sensibilisation se déclinant sous plusieurs formes se sont mises en place et prennent progressivement de l'ampleur grâce à un intérêt public accru et à une meilleure structuration.

A. La sensibilisation.

Une grande majorité de parents de jeunes internautes admet volontiers ne pas maîtriser l'outil Internet aussi bien que leurs enfants⁶¹⁰. Ils souhaitent avoir la meilleure information sur les moyens de sécuriser la navigation de leur enfant sur la Toile⁶¹¹ sans toujours savoir où l'obtenir.

La logique de la sensibilisation à Internet s'articule sur deux axes principaux : d'une part la détermination de la cible des acteurs d'Internet demandeurs et nécessitant de l'information; d'autre part l'adaptation du discours de sensibilisation aux différents auditoires.

1. Les cibles de la sensibilisation.

La sensibilisation aux dangers du cyberspace vise d'une part les mineurs, et d'autre part leurs parents et/ou tuteurs légaux.

⁶¹⁰ Selon le rapport rendu au Ministre Philippe Douste-Blazy suite à la Conférence de la Famille 2005 : « Protection de l'enfant et usages d'Internet » en 2001, 72% des parents avaient le sentiment que leur enfant connaissait mieux Internet qu'eux même.

⁶¹¹ 55% selon le rapport ci-dessus cité.

1.a. La sensibilisation des mineurs aux dangers du cyberspace.

Lorsqu'il s'est agi de sensibiliser sur les dangers du cyberspace, il a été logique de commencer par les principaux intéressés par les mesures de protection des mineurs. Le discours adopté a d'abord été général, destiné à tous les acteurs d'Internet, puis il a été affiné afin de cibler spécifiquement les mineurs.

Les lieux principaux où les mineurs sont susceptibles de naviguer sur la Toile sont le domicile et l'école. Il existe cependant d'autres lieux où leur fréquentation bien qu'épisodique reste porteuse de risques pour eux : il s'agit des cybercafés, des navigations chez des tiers, etc. Nous ne retiendrons pour notre étude que les lieux de navigations les plus significatifs pour les mineurs : le domicile (du tuteur légal) et l'école. Dans ces lieux la navigation du mineur se fait sous la responsabilité d'un tuteur ou d'un représentant légal.

De nombreux organismes gouvernementaux et associatifs, ont pris l'initiative de lancer des campagnes de sensibilisation vers les mineurs internautes⁶¹² : des campagnes ponctuelles et/ou pérennes. Pour atteindre directement les mineurs, il existe des sites qui leur sont dédiés et qui leur donnent des astuces et des règles pour savoir surfer en évitant les dangers. Il peut s'agir de sites axés exclusivement sur une sensibilisation à la sécurité des mineurs⁶¹³ dans le cyberspace, ou de sites généralistes leur ménageant un espace. Outre la sensibilisation par les médias, les organismes de protection des mineurs organisent des rencontres (conférences, salons, etc.), se rendent dans des établissements avec des mallettes pédagogiques afin de sensibiliser les mineurs aux dangers d'Internet⁶¹⁴. La première initiative menée par la

⁶¹² Il y a les associations de protection de l'enfance telles que : Innocence en danger (<http://www.innocenceendanger.org>); E-enfance (<http://www.e-enfance.org>) qui vise essentiellement une protection dans le cyberspace. Il y a aussi l'action gouvernementale par le biais d'organismes et d'institutions telles que la Délégation aux Usages d'Internet (DUI voir : <http://www.delegation.internet.gouv.fr>), OCLCTIC (Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication), le Défenseur des enfants (<http://www.defenseurdesenfants.fr>).

⁶¹³ Par exemple le site d'Internet sans crainte leur réserve une rubrique qui se présente sous la forme d'une série réalisée avec l'aide du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche : "Vinz et Lou sur Internet" voir : <http://www.internetsanscrainte.fr/article.php?rubrique=juniors&menu=false> ou <http://www.vinzetlou.fr> ; L'Association du Multimédia jeunesse participe au programme Confiance, Plan d'action national de sensibilisation aux enjeux et aux risques d'Internet voir : <http://www.adelouzes.fr/?wpid=12299> , Ouvert en décembre 2003, le site mineurs.fr est animé par la Délégation aux usages d'Internet. Il recense les différentes possibilités qui existent pour protéger les mineurs contre les contenus illicites d'Internet, que ce soit dans le cadre familial ou à l'école. Il met l'accent également sur la responsabilisation et l'éducation des enfants aux règles et usages du net. Un espace s'adresse directement aux juniors, <http://www.internet.education.fr/mineurs/juniors.htm>

⁶¹⁴ Action Innocence, dans le cadre de sa mission de prévention, réalise des interventions de prévention en milieu scolaire et associatif : primaires, collèges, lycées, associations de parents d'élèves, cyber-centres, municipalités, etc. L'objectif est de sensibiliser les enfants et leurs parents à un usage prudent, éthique et citoyen d'Internet,

Délégation aux Usages d'Internet dans ce cadre de la sensibilisation fut « le Tour de France des collègues ». Des journées de sensibilisation furent à cette occasion proposées aux établissements scolaires dans le but d'informer les enfants, les parents et les enseignants des risques liés à l'utilisation d'Internet tant à l'école que dans les foyers

1. b. La sensibilisation des parents et/ou tuteurs légaux aux dangers du cyberspace.

Les parents sont autant concernés que leurs enfants par les mesures de sensibilisation en vue de la protection de ces derniers⁶¹⁵.

En matière de connaissance du cyberspace, tous les parents ne sont pas logés à la même enseigne. Un certain nombre de parents maîtrisent parfaitement cet outil et connaissent les dangers du cyberspace de même que les mesures nécessaires à la protection des mineurs dans le cyberspace. D'autres connaissent l'outil sans en maîtriser toutes les fonctionnalités et les dangers⁶¹⁶. Certains enfin, ne s'y connaissent absolument pas et sont complètement dépassés par cette technologie⁶¹⁷. Au regard de ces disparités dans la maîtrise d'Internet, un discours adaptable à tous est nécessaire. Pour certains la sensibilisation ne visera qu'une mise à jour des évolutions technologiques d'Internet ; tandis que les autres nécessiteront un apprentissage de débutant afin de pouvoir appréhender au mieux la réalité de l'outil. L'objectif étant de comprendre et prévenir au mieux les risques encourus par les mineurs.

avec des contenus et conseils différents selon les tranches d'âge. Pour répondre à une demande de plus en plus fréquente, deux nouveaux modules ont été créés en 2007 :

- un module enfant pour les 6-8 ans, qui s'ajoute aux modules 9-12 ans, 13-17 ans,
- un module spécial « interactivité numérique » autour des blogs, happy slapping, webcams.

<http://www.internetsanscrainte.fr/article.php?rubrique=actu&id=36&month=7&year=2007>

⁶¹⁵ En 2001, selon un sondage SoFres tiré de la Conférence de la Famille 2005. Protection de l'enfant et usages d'Internet, 72% des parents avaient le sentiment que leur enfant connaissait mieux Internet qu'eux-mêmes. En selon une étude du CREDOC (centre de recherche pour l'étude et l'observation des conditions de vie) et de l'ART (Autorité de Régulation des Télécom), 87% des 12-17 ans se déclarent familiarisés avec Internet contre 45% d'adultes.

⁶¹⁶ Selon un sondage Eurobarometer, voire Forum des Droits sur Internet, 55% des parents de jeunes internautes souhaitaient disposer d'une meilleure information sur les moyens de sécuriser la navigation de leur enfant sur la toile.

⁶¹⁷ Le risque avec cette dernière catégorie de parent est de laisser les enfants livrés à eux-mêmes, livrés aux excès d'un monde virtuel peu ou pas policé, qui peut être générateur de traumatismes bien réels par l'exposition à des contenus violents, à des agressions de tous sorts : commerciales pour l'enfant consommateur, anticiviques (racisme, antisémitisme, apologie du suicide, de l'anorexie...), à des agressions sexuelles (pornographiques ou pédopornographique, dialogues non modérés, prises de contacts dangereuses...).

Les parents à l'instar de leurs enfants peuvent être atteints par les campagnes de sensibilisation destinées au grand public par le biais des médias, ou rechercher dans des sites spécialisés l'information qui leur manque⁶¹⁸.

L'obligation de vigilance des parents et tuteurs légaux à l'égard des mineurs est posée dans le préambule de la Convention internationale des droits de l'enfant. Il y est souligné l'obligation d'assurer aux enfants « une aide et une assistance spéciales du fait de leur manque de maturité physique et intellectuelle » au regard de l'intérêt supérieur de l'enfant⁶¹⁹. Cette vigilance doit s'appliquer à tous les aspects de la navigation de l'enfant sur Internet afin de prévenir les délits commis par le mineur ou contre le mineur.

1. c. La sensibilisation des éducateurs aux dangers du cyberspace.

Les éducateurs sont formés au maniement et à la maîtrise des outils qu'ils sont amenés à utiliser avec les élèves. Ils reçoivent des mises à jour des technologies s'agissant de la protection des mineurs sur Internet. Ils ne maîtrisent pas tous pour autant Internet. Ils doivent être à même d'inculquer aux mineurs les règles de sécurité sur Internet. EPSIDOC⁶²⁰ est un site destiné au corps enseignant et regroupant des liens de ressources documentaires et pédagogiques ; il y a notamment une rubrique « côté profs – usage et sécurité Internet ». Il y est rassemblé conformément à l'esprit du site, des liens susceptibles de fournir des éléments d'informations au corps enseignant dans l'optique d'une meilleure sensibilisation des mineurs à leur sécurité dans le cyberspace.

Les éducateurs des mineurs ne sont pas laissés pour compte par les campagnes de sensibilisation. Ils sont au contraire mis à contribution dans les campagnes de sensibilisation destinées aux mineurs et qui sont organisées au sein de leurs établissements scolaires⁶²¹. Ils y participent activement, puisqu'ils doivent contribuer à véhiculer le message de prévention auprès des mineurs. S'agissant de l'initiative prise par la Délégation des Usages d'Internet : « Le Tour de France des collèges », les éducateurs doivent avoir une démarche volontaire pour que les journées de sensibilisation proposées aux établissements scolaires dans le but

⁶¹⁸ <http://www.internetsanscrainte.fr>, un site Créé à l'initiative du Ministère de la famille, ce site vise à sensibiliser les parents à Internet et favoriser le dialogue avec leurs enfants, www.famille.gouv.fr/fam_lign/index.htm, Le Forum des Droits sur Internet, le Ministère de la Famille et la Délégation aux Usages d'Internet ont conçu deux guides pratiques : un pour sensibiliser les jeunes adolescents aux pratiques et aux lois d'Internet, l'autre pour mieux informer les parents, www.droitdunet.fr

⁶¹⁹ Voir article 18 de la Convention internationale des droits de l'enfant de 1989.

⁶²⁰ <http://www.epsidoc.net/eprofs/secunet.htm>

d'informer les enfants, les parents et les enseignants des risques liés à l'utilisation d'Internet tant à l'école que dans les foyers, se tiennent dans leur enceinte.

Les parents comme les éducateurs doivent être en mesure de pallier les lacunes des mineurs, leur apporter l'assistance technique et psychologique nécessaire à l'utilisation d'Internet. Ils doivent être à même de prévenir au mieux l'exposition des mineurs dont ils ont la charge à des contenus inconvenants. A défaut de pouvoir prévenir toutes les expositions inconvenantes, ils doivent apporter un soutien psychologique au mineur en lui expliquant comment se comporter en pareille circonstance ou comment éviter de se trouver confronté à certains dangers.

2. La nature et la forme de la sensibilisation.

La sensibilisation sur les dangers et la protection des mineurs est devenue l'affaire de tous. Le gouvernement, les associations, les fournisseurs d'accès, les personnes privées, etc. Tout le monde s'y est mis pour tenter de faire d'Internet un endroit plus sûr pour les enfants. Ce fut notamment de cas des associations de protection de l'enfance telle : Innocence en danger. Elle a mis noir sur blanc, les règles de bases pour naviguer sereinement et en sécurité dans le cyberspace⁶²².

La sensibilisation prend plusieurs formes. Elle se présente sous forme de campagnes ponctuelles sur le thème de la protection des mineurs. La traditionnelle fête annuelle d'Internet est toujours l'occasion de rappeler les règles "du bien surfer" sur la toile en toute sécurité. Il peut arriver que des organismes, des associations, des administrations individuellement ou en collaboration, organisent des campagnes ponctuelles, à des échelles

⁶²² Ces règles de bases sont applicables pour toute utilisation d'Internet, dans les forums et les « chat », navigation, échanges de mails, visites de sites etc.

- ne jamais utiliser son vrai nom, prénom
- ne jamais donner d'informations privées (email, téléphone, adresse...)
- ne jamais accepter de recevoir ou d'envoyer des photos ou de brancher votre Webcam à la demande d'un inconnu
- ne jamais ouvrir des emails dont la provenance est inconnue, ils peuvent contenir des images choquantes ou des virus
- les enfants ne doivent pas surfer seuls
- l'ordinateur devrait toujours être placé dans une pièce commune
- les parents ne doivent pas s'imaginer qu'Internet peut remplacer une nounou
- tout tuteur doit prendre le temps d'apprendre à utiliser un ordinateur, au moins les bases lui permettant d'accéder à Internet
- il est vivement recommandé d'installer des logiciels de protection tout en ayant conscience qu'ils ne sont pas infaillibles et ne remplacent pas la vigilance d'un adulte
- les parents doivent prendre le temps de surfer avec leurs enfants pour connaître les sites qu'ils visitent

diverses sur les dangers du cyberspace où différents supports sont visés. Selon qu'il s'agisse de campagnes ponctuelles ou pérennes, les supports et les formes de sensibilisation seront différents.

- Les campagnes de sensibilisation ponctuelles sollicitent souvent les médias traditionnels par le biais de spots télévisés ou radiodiffusés, d'articles de presse, de campagnes d'affichages⁶²³. Ces campagnes visent une grande visibilité. Elles souhaitent bousculer le public afin d'éveiller ou de réveiller leur conscience sur les dangers que courent le mineur dans le cyberspace. Elles ne se réalisent pas dans la durée.
- Les campagnes pérennes se font plus à l'écart des médias et se caractérisent par leur durée dans le temps ou leur caractère quasi permanent. Elles se font par des tracts ou brochures d'information, des conférences-débats, des interventions en milieu scolaire ou plus généralement éducatif (bibliothèque, lieux de rencontre des mineurs après l'école...). Elles visent un travail de fonds au plus près des acteurs principalement concernés par la sécurité des mineurs dans le cyberspace.

La sensibilisation tend à se pérenniser dans la forme, ce qui est vivement encouragé dans le sens où la sécurité des mineurs dans le cyberspace est entrée dans un processus de responsabilisation de tous les acteurs à tous les échelons y compris les prestataires techniques. Il s'agit pour les intermédiaires techniques et les professionnels du cyberspace, de prévoir dans leurs sites, leurs forums, chats etc., des avertissements attirant l'attention des internautes sur les règles "du bien surfer" en sécurité. Il peut également s'agir de sites Internet spécialisés et/ou institutionnels qui ont pour but principal de prodiguer conseils, recommandations et mises en garde aux parents et enfants⁶²⁴.

⁶²³ L'ONG Action Innocence a lancé une Campagne de sensibilisation contre les dangers d'Internet pour les enfants. Une première vague a été lancée novembre 2005 en télévision, presse, cinéma, Internet sur le thème "le Masque". Dans le cadre de sa mission de contribution à préserver la dignité et l'intégrité de l'enfant sur Internet Action Innocence réalise des campagnes de sensibilisation du grand public. Depuis le 7 août 2006, c'est en affichage sur les réseaux Avenir et JC Decaux que sont diffusés ces messages de sensibilisation, avec 6000 affiches réparties sur toute la France...et toujours le même leitmotiv : « un pseudo peut cacher n'importe qui, soyez vigilants sur Internet ».

<http://www.actioninnocence.org/france/campagnelemasque.asp?page=1&navig=20>

⁶²⁴ Les ministères de l'Intérieur, de la Défense, Emploi et famille en accord avec la Cnil ont créé un site qui a pour ambition de lutter contre le crime, en même temps qu'il fournit les principaux textes législatifs référence, des conseils pratiques pour les parents et les enfants : <https://www.internet-mineurs.gouv.fr>

La sensibilisation peut se décliner sous la forme d'un programme ou d'une directive politique. On a pu voir l'Union européenne prendre une position active par la voix de ses institutions⁶²⁵. De nombreux organismes internationaux, tels que l'Unesco ont une politique spécifique en la matière. L'Unesco organise périodiquement des conférences sur le thème de la protection de l'enfance sur Internet. Par le biais d'associations créées sous son égide ou qu'elle parraine, l'Unesco relaie sa politique à différentes échelles. Les associations se chargent de faire un travail de fond au quotidien⁶²⁶ en mettant en œuvre les lignes directrices de l'Unesco. Le G8 n'a pas échappé à cette ligne directrice. Ce combat est devenu une véritable priorité d'ordre public.

Il est une autre forme de sensibilisation qui table sur une véritable formation du mineur. Cette formation est sanctionnée par une reconnaissance : le brevet informatique et Internet qui engage le mineur dans la voie de la responsabilisation.

Le brevet informatique et Internet⁶²⁷ est désormais obligatoire pour les écoliers et les collégiens. Il s'agit d'un apprentissage des règles de bonne conduite sur Internet. Le brevet atteste que l'élève utilise de manière autonome et raisonnée les technologies de l'information

⁶²⁵ Le Parlement européen avait défini une politique sous forme d'une action communautaire en vue d'une utilisation plus sûre d'Internet. Il s'agissait précisément d'une « Proposition de décision du Conseil adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation sûre d'Internet » [COM(97)582 présentée en novembre 1997]. Le plan d'action proposé couvrait une période de quatre ans et visait à créer un environnement favorable à l'émergence de l'industrie liée à Internet. Le plan contenait quatre lignes d'actions : créer un environnement sûr, développer les systèmes de filtrage et classification, encourager les actions de sensibilisations et des actions de soutien. Source, Europolitique 4 juillet 1998.

⁶²⁶ Ces associations qui ont souvent une double envergure occupent le terrain national et par le jeu d'antennes ou de représentations dans plusieurs pays assurent ainsi un relais international. Ces associations travaillent en amont dans le cadre de la prévention et la sensibilisation dans les écoles, et partout où c'est possible, auprès des gouvernements, elles s'invitent ou sont invitées dans les débats sur des projets d'amélioration des dispositions législatives. Elles travaillent en aval également dans l'accompagnement psychologique et juridique des victimes et de leur famille.

⁶²⁷ Le Brevet informatique et Internet (B2i) a été mis en place par un texte du Ministère de l'Éducation Nationale n° 2000-206 du 16-11-2000. L'objectif de ce brevet est de spécifier un ensemble de compétences significatives dans le domaine des technologies de l'information et de la communication et d'attester leur maîtrise par les élèves concernés. Les compétences correspondant à chacun de ces niveaux feront l'objet de réajustements ultérieurs prenant en compte l'évolution des technologies, des pratiques et des contenus d'enseignement. Bulletin Officiel du ministère de l'Éducation Nationale et du ministère de la Recherche N°42 du 23 novembre 2000.

<http://www.education.gouv.fr/bo/2000/42/encart.htm>

Connaissances et capacités exigibles pour le B2i. Arrêté du 14-6-2006, JO DU 27-6-2006, Bulletin Officiel n°29 du 20 juillet 2006, Vu code de l'éducation, not. articles L. 122-1-1, L. 311-1, L. 311-2, L. 311-3, L. 312-9 et L. 337-4 ; A. du 25-1-2002 not. annexe V ; N.S du 16-11-2000 ; avis du CSE du 18-5-2006 ;

<http://www.education.gouv.fr/bo/2006/29/MENE0601490A.htm>

et de la communication disponible à l'école et au collège pour lire et produire des documents, rechercher des informations qui lui sont utiles et communiquer au moyen d'une messagerie⁶²⁸.

Une charte de bonne conduite. L'Education nationale recourt systématiquement à des « chartes d'utilisation » signées par l'administration, les professeurs et les élèves. Ces chartes peuvent être intégrées aux règlements intérieurs des établissements. Elles équivalent à un engagement contractuel des signataires à utiliser les Techniques d'Information et de Communication en milieu scolaire en respectant les droits et les obligations de chacun.

Il existe un projet en France animé par le CLEMI (Centre de Liaison et de l'Enseignement et des Médias d'Information⁶²⁹) qui est soutenu par la Commission européenne dans le cadre du plan d'action « safer Internet » et du projet Educaunet. C'est un programme d'éducation critique des risques liés à Internet et, qui entend agir par une double approche centrée sur les parents et les enseignants, comme relais d'une éducation des enfants et des jeunes. Le projet prévoit des outils et modèles adaptés spécifiquement à trois tranches d'âge : 8-11 ans, 12-15 ans et 16-18 ans⁶³⁰. Tous ces enseignements sur la sécurité du mineur dans le cyberespace doivent servir prioritairement à accroître la vigilance des parents sur les connexions de leurs enfants mineurs dans le cyberespace.

B. Le contrôle parental pour la sécurité du mineur dans sa navigation dans le cyberespace.

Les mesures de sensibilisation des parents et des mineurs ne résolvent pas totalement la question de la sécurité des mineurs dans le cyberespace. Une efficacité optimale supposerait que tous les mineurs aient suivi et compris les campagnes de sensibilisation, et qu'ils appliquent les mesures de sécurité préconisées. Reste la question des contenus inconvenants qui continuent à être accessibles pour tous que la démarche d'y avoir accès soit ou non volontaire. Le moyen le plus efficace consisterait en l'accompagnement physique des parents pendant le temps de connexion du mineur sur Internet. Cette présence représenterait le double avantage de permettre d'une part une réaction prompte du parent face à la survenance impromptue de contenus inconvenants lors de la navigation du mineur ; d'autre part elle aurait

⁶²⁸ <http://www.educaunet.org/sommaire-fr.php3/>

⁶²⁹ Organisme qui conçoit et développe des programmes d'éducation aux médias ; il est dépendant du ministère de l'éducation nationale.

⁶³⁰ http://www.educaunet.org/sommaire-fr.php3

un effet dissuasif sur les mineurs qui seraient autrement tentés d'avoir des comportements à risque et/ou préjudiciables sur Internet. En pratique cependant, les parents ne peuvent en permanence être présents auprès de leurs enfants pendant leurs connexions sur Internet. Il en ressort la nécessité d'envisager des méthodes supplémentaires et complémentaires pour perpétuer la sécurité des mineurs dans le cyberspace même en l'absence de leurs parents. Ces modes de prévention des mineurs contre les dangers d'Internet, doivent être utilisés de manière conjointe pour une plus grande efficacité.

Les mesures privilégiées par les parents traduisent leur volonté de renforcer la protection de leur enfant. Ainsi, plus des deux tiers des parents (68 %) déclarent avoir déjà installé l'ordinateur dans un lieu ouvert. A un moindre degré, 44 % ont déjà limité l'accès de leur enfant à Internet. En revanche, ils ne sont que 11 % à s'être déjà procuré un guide d'information. 34 % ont déjà eu recours aux services du fournisseur d'accès et 32 % ont installé un logiciel de contrôle parental. Pour ce qui concerne l'action publique de protection de l'enfance, les attentes des parents placent trois pistes d'action sensiblement au même niveau de priorité.

1. Une présence physique et dissuasive lors de la navigation.

Le premier pas vers une présence physique des parents passe par une mise à disposition familiale d'Internet. Il est recommandé de ne pas mettre un ordinateur relié à Internet dans la chambre d'un enfant, dans une pièce privée où la vigilance parentale sera très limitée : le contrôle du temps et de la nature de la connexion de l'enfant serait illusoire. Le conseil est de mettre l'ordinateur dans un lieu de vie familiale où l'enfant ne sera pas isolé. Cela aura la vertu de dissuader l'enfant d'aller sur des sites illégaux ou de commettre des actes ostensiblement délictueux, par la seule crainte d'être surpris.

Il ne s'agit pas pour autant de créer un régime de peur et de suspicion. L'idéal serait d'instaurer un climat de confiance qui pousserait l'enfant à laisser l'adulte interférer de manière non intrusive dans son univers cybernétique. Cela suppose une bonne communication avec lui et le respect de son espace privé.

Outre la présence dissuasive des parents ou de tout autre adulte lors de la navigation du mineur, les enfants attendent surtout une assistance psychologique lorsqu'ils sont confrontés à des contenus inconvenants ou à des interlocuteurs indéclicats. Le parent ou tuteur légal doit

être en mesure d'apporter une réponse prompte et adéquate. Il devra lui rappeler la démarche à suivre : ne pas communiquer de données personnelles identifiantes sur Internet, se déconnecter (d'un site, d'un forum, chat) chaque fois que les propos de ses interlocuteurs deviennent inconvenants ou qu'il se trouve face à des contenus choquants, signaler tout incident au médiateur ou modérateur s'il y en a un et en parler à un adulte afin que ce dernier effectue un signalement dans un point de contact.

Le rôle des parents est de plus en plus mis en avant en matière de protection des mineurs contre les contenus choquants. Le devoir parental prime sur toute autre disposition visant la protection du mineur dans le cyberspace⁶³¹. La Commission européenne, dans le Livre vert sur la protection des mineurs et la dignité humaine dans les services d'information, s'était prononcée sur une autorégulation impliquant les parents. Leur contrôle devait s'appuyer sur une vigilance de leur part de même que sur des outils techniques appropriés⁶³².

Cette prise de position qui semble évidente, ne l'est pourtant pas pour tous les parents ayant des enfants en âge de naviguer sur Internet. Lors d'une enquête d'Ipsos, réalisée en partenariat avec *Libération* et *La Cinquième*, en novembre 2000, 40 % de parents ont répondu qu'il arrive que leur enfant surfe seul. Si 62 % affirment être préoccupés par l'utilisation que fait ou pourrait faire leur enfant du net, 36 % ne le sont pas. Par ailleurs, 49 % pensent qu'il n'est pas indispensable d'être à côté de son enfant lorsqu'il surfe, estimant qu'il suffit de lui dire quelles sont les choses qu'il ne faut pas faire⁶³³.

L'autonomisation de l'enfant devant l'ordinateur, préfigure souvent de son autonomisation au sein de sa famille. La trop grande confiance des parents qui peut s'apparenter à un déficit de vigilance envers leurs enfants, crée un vide dans le quotidien de l'enfant facilement comblé par le Web. Sur le Net, l'enfant est certain de trouver une activité, une occupation, des

⁶³¹ Selon un rapport du Conseil de l'Etat sur Internet et les réseaux numériques, la protection et donc la moralité du mineur sont avant tout un devoir parental. Bien qu'affirmé comme tel dans l'article 371-2 du code civil, sa mise en œuvre apparaît en pratique difficile eu égard à la diversité des contenus circulant sur le réseau ; Frédéric-Jérôme Pansier et Emmanuel Jez, *La criminalité sur Internet*, Que-Sais-Je ? PUF, p.76-92.

⁶³² La Commission européenne avait estimé qu'il convient « dans tous les cas d'identifier les moyens qui permettront raisonnablement de s'assurer que des mineurs n'auront pas accès à des contenus susceptibles de nuire à leur épanouissement physique ou mental, tout en permettant l'accès des adultes qui le souhaitent à ces contenus ». Voir J.-M. Orion, *Le livre vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information* : Légipresse, juin 1997, II-72.

⁶³³ Enquête : Les enfants et le net, Ipsos/Libération /La Cinquième, auprès de 952 parents d'enfants âgés de 3 à 18 ans.

interlocuteurs auxquels il s'identifie parfois, des interlocuteurs avec qui il peut parler de tout sans contraintes ni tabous.

Le 24 septembre 1998, le Conseil européen a adopté une Recommandation concernant le développement de la compétitivité de l'industrie européenne des services audiovisuels et d'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de protection des mineurs et de la dignité humaine⁶³⁴. Le Conseil précisait à cette occasion que l'objectif de ces codes devait être de « permettre aux mineurs d'utiliser de manière responsable les services en ligne et d'éviter qu'ils accèdent, sans l'accord de leurs parents ou de leurs éducateurs, à des contenus légaux susceptibles de nuire à leur épanouissement physique, mental ou moral.

Dans la foulée, le Parlement européen et le Conseil par une décision du 25 janvier 1999, ont adopté un « plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux »⁶³⁵. Dans la continuité, le Parlement européen a adopté le 11 avril 2002 une proposition de résolution⁶³⁶. A cette occasion, les députés ont tenu à rappeler que la protection des mineurs face aux contenus choquants relevait essentiellement de la vigilance des parents et plus généralement des tuteurs légaux.

Toutes ces dispositions démontrent que, les parents ou tuteurs légaux ne peuvent se décharger sur autrui de leur devoir de vigilance envers le mineur s'agissant de la sécurité de ce dernier sur Internet. Quelles seraient les conséquences juridiques d'un défaut de vigilance avéré des parents ou tuteurs légaux envers leurs enfants internautes ? Pour l'heure les juges n'ont pas encore eu à connaître de tels litiges.

Dans la mise en avant de la vigilance des parents ou tuteurs légaux du mineur, l'accent est toujours mis sur la nécessité pour eux de disposer d'outils techniques appropriés, pour compléter leur vigilance physique. D'aucuns y voient un repli sur la technique, révélateur des lacunes de la sécurisation de la navigation des mineurs dans le cyberspace. Ces lacunes

⁶³⁴ JOCE n° L 270, 7 octobre 1998, p.48 ; Légipresse, novembre 1998, IV-99.

⁶³⁵ Décembre n° 276/1999/CE, 25 janvier 1999 du Parlement européen et du Conseil : JOCE n° L33, 6 février 1999, p.1 ; Légipresse, mars 1999, IV-29. Ce plan qui devait se dérouler entre le 1^{er} janvier 1999 et le 31 décembre 2002, faisait apparaître la conviction selon laquelle face aux contenus choquants pour les enfants, le recours à la technique était la parade ultime à défaut d'être infaillible.

⁶³⁶ Adoption suite au rapport d'évaluation de la Commission sur la protection des mineurs et de la dignité humaine.

tiennent pour partie au fait que le cyberspace étant un lieu où s'entrechoquent liberté des adultes et protection des intérêts des mineurs⁶³⁷, la crainte d'une politique toute entière tournée vers la protection des mineurs contre tout ce qui leur est préjudiciable avec pour résultat de restreindre considérablement des comportements même légaux.

2. L'utilisation de la technologie pour la prévention.

Eu égard à la recrudescence des contenus illicites sur la toile et aux limites humaines des parents et/ou tuteurs légaux, l'utilisation de la technologie en renfort de la vigilance parentale s'est imposée comme indispensable dans la lutte pour un Internet plus sûr pour les enfants.

Sous couvert de la sécurité du mineur sur Internet, il ne s'agit pas pour autant de promouvoir des mesures liberticides pour ce dernier. Il faut trouver un juste milieu entre les mesures de sécurité et la liberté de l'enfant. Pour ce faire, il faut adapter les mesures prises à l'âge et la maturité de l'enfant. Il convient d'aménager à l'enfant une sphère privée d'expression en lui faisant confiance pour surfer seul, tout-en conservant un contrôle sur sa navigation dans le cyberspace.

Idéalement, la meilleure protection pour l'enfant serait par l'information, de le prémunir des dangers d'Internet. Cela supposerait qu'il puisse faire preuve d'une réelle capacité de compréhension et de vigilance, qualités dont tous les adultes ne peuvent eux-mêmes se targuer. Avec les pop-ups, les Spam et autres contenus impromptus et ne nécessitant aucune manifestation volontaire de l'internaute de les consulter, la nécessité du recours aux logiciels de filtrage s'impose comme partie intégrante de la sécurité des mineurs dans le cyberspace.

Le filtrage doit toujours se faire de manière claire et sans qu'il soit pour autant question de concertation avec l'enfant, il doit lui être expliqué. Il doit en outre être adapté à l'âge et à la maturité de ce dernier⁶³⁸.

⁶³⁷ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.203-204.

⁶³⁸ Contrôle parental sur Internet : www.teteamodeler.org/conditionstravail/encadrement/controparent.htm

2-a. Les logiciels de filtres parentaux.

Créés pour empêcher l'accès des mineurs aux contenus obscènes, choquants et inconvenants, les logiciels de filtres parentaux sont loin de faire l'unanimité auprès des divers acteurs et intervenants du cyberspace. Leur fiabilité est sujette à caution, et ils ne règlent pas la question fondamentale de la responsabilisation des utilisateurs ou de leurs tuteurs légaux dans le cas des mineurs⁶³⁹.

Il y a un préalable à l'utilisation et donc à l'efficacité des logiciels de filtres parentaux : il faudrait que le mineur soit identifiable comme l'utilisateur d'Internet pour une meilleure efficacité. C'est dans cet esprit qu'en date du 29 janvier 2003, l'Observatoire des Droits d'Internet a émis, un avis à l'adresse du gouvernement fédéral belge, relatif à la protection des mineurs sur Internet. Cet avis complétait un autre avis rendu en septembre 2002 par la Commission pour la protection de la vie privée. Selon l'Observatoire, l'identification est un axe prioritaire pour préserver la dignité humaine et la loyauté dans la société de l'information au profit de certaines catégories d'utilisateurs vulnérables et notamment les mineurs. C'est un moyen approprié pour assurer le contrôle et la sécurité des relations sur Internet. L'objectif est de créer un espace sécurisé et loyal sur Internet.

Il existe différents types de logiciels de filtrage parentaux avec divers niveaux de filtrage qui se veulent aussi novateurs les uns que les autres. Ils ont tous l'objectif commun de créer un cyberspace plus propre pour les mineurs. Tout le monde convient que ces programmes peuvent empêcher un jeune enfant de tomber par hasard sur des contenus indésirables mais qu'ils ne suffisent pas pour arrêter un adolescent décidé à consulter ce type de contenus⁶⁴⁰.

Les filtres parentaux sont de petits programmes qui se mettent à fonctionner automatiquement dès que vous accédez à Internet. La majorité d'entre eux s'activent sur toutes les fonctionnalités d'Internet : recherche de sites, newsgroups, réseaux de discussion en ligne, etc.⁶⁴¹. Ces programmes de filtrage couvrent des aspects différents de la sécurisation de la navigation du mineur sur Internet.

⁶³⁹ John Schwartz, Votre Internet avec ou sans filtre ? Courrier International n° 455 du 22 au 28 juillet 1999, p.34.

⁶⁴⁰ Ibid.

⁶⁴¹ Contrôle parental sur Internet : www.teteamodeler.org/conditionstravail/encadrement/controparent.htm

- Ils peuvent délimiter le temps d'accès du mineur en définissant des plages horaires pendant lesquelles le mineur pourra avoir accès à Internet.
- Ils peuvent bloquer tout accès à certaines fonctionnalités comme le chat ou la messagerie instantanée.

Ces programmes ont une liste de sites bannis (listes noires), ou autorisés (listes blanches) ; des mots clés prohibés rendant l'accès à certains sites impossibles. Il est possible de configurer plusieurs niveaux d'utilisateurs, chacun disposant de son propre mot de passe.

2.a'. Les listes noires et les listes blanches

i. Le filtrage par liste blanche

Ce procédé suppose qu'un travail de veille soit fait en amont sur les milliers de pages que compte le cyberspace. Cette veille peut être l'œuvre du fournisseur d'accès ou des concepteurs du logiciel de filtrage. Les parents n'auront ensuite qu'à entériner ces listes ou y ajouter des critères plus restrictifs.

Le principe du filtrage par liste blanche consiste en une présélection de sites que l'enfant pourra ou non consulter. Cette liste est établie sur la base de différents critères dont le plus usité est celui de la classification. Il appartient à un organisme plus ou moins indépendant (fournisseur d'accès, fournisseur du logiciel...) de "scanner" de manière continue le cyberspace afin de classer les différents sites référencés selon un degré de nocivité pour l'enfant en vue d'en bloquer ou non l'accès.

ii. Le filtrage par liste noire.

Les organismes de référencement ont quasiment toute latitude pour empêcher l'accès à des sites qui leur semble préjudiciables ou inadéquats pour l'enfant. Les sites qui seront référencés dans la liste noire ne seront pas accessibles au contraire de ceux de la liste blanche. Ce système s'apparente à de l'auto-labellisation. Par ce système, les fournisseurs de contenu attachent une étiquette à leur contenu. Les parents utilisent ensuite les caractéristiques de leur logiciel de navigation pour entériner ou affiner les critères qui leurs ont été fournis.

Dans ce système, la présélection de listes est souvent fonction de la culture et des pratiques du pays dans lequel elle est mise en œuvre. La liste peut être très restrictive ou assez permissive en fonction de ces critères. En France il a été mis sur pied une structure nationale, au niveau

interministériel chargée de coordonner et de centraliser l'offre de "listes noires". Les partenaires en sont : le ministère de la Justice, le ministère de l'Intérieur, le ministère de la Famille et de l'Éducation nationale. Ils contribuent dans leur domaine respectif à améliorer et pérenniser cette liste⁶⁴².

Ils existent des logiciels permettant d'adapter la liste noire en fonction du pays d'origine.

Le filtrage par liste blanche ou noire connaît des limites. La première limite tient au caractère restrictif de l'accès à l'information, ces systèmes créent *de facto* une inégalité face à la recherche et l'obtention d'information. D'un pays à l'autre et selon les us et coutumes du pays où le filtrage est mis en place, l'internaute mineur n'aura pas accès à la même information. Considérant le volume exponentiel des contenus et du nombre de pages du cyberspace, de leur volatilité, il est presque certain que l'autorité en charge de la labellisation ne sera pas à même de suivre ou d'examiner toutes les pages du cyberspace en temps réel afin de les référencer selon leur degré de nocivité.

2.a". Les filtres basés sur certains mots clefs.

A l'instar des listes noires d'url (informellement appelées adresses web), les éditeurs utilisent des listes de mots à bannir pour restreindre les risques d'accès à des contenus inconvenants pour le mineur. Ils sont détectés soit dans l'url du site soit à l'intérieur de la page. Certains logiciels peuvent les détecter dans les moteurs de recherche, les mails, les newsgroups, etc. Dès lors, le mot interdit est remplacé par des caractères de substitution⁶⁴³, le reste du contenu n'est cependant pas bloqué. Il existe toutefois la possibilité de bloquer la page ou le service contenant un mot clé interdit.

Le filtrage par mots clés présente l'inconvénient de bloquer parfois l'accès à des sites dont le contenu n'est en rien préjudiciable. Par exemple, une demande de filtrage fondée sur le mot « sein » pourra bloquer l'accès à des sites médicaux ou à des pages contenant l'expression « en son sein ».

⁶⁴² Protection et éducation des mineurs à la maison, <http://delegation.internet.gouv.fr>

⁶⁴³ Pour le logiciel de contrôle Cybersitter, le mot interdit sera remplacé par des blancs, pour Net Nanny il s'agira de dièses ; Protection des mineurs, Les tests des logiciels de filtrage, voire sur le site Délégation aux usages d'Internet.

2.a'''. Le filtrage des intermédiaires du cyberspace.

i. Le filtrage PICS⁶⁴⁴ des navigateurs.

Les principaux navigateurs proposent une fonction de filtrage des contenus à partir du poste de l'utilisateur dans des espaces réservés aux enfants. Le navigateur affiche ou non une page à l'écran en fonction d'une évaluation des sites réalisée par les concepteurs même de la page. Ce filtrage n'est contrôlé par aucun organisme extérieur et laisse donc une part importante à la subjectivité du navigateur. Cette classification n'est pas adaptée aux services de messagerie, de transfert de fichiers, de chat, ce qui l'a rend finalement assez limitée. Difficulté supplémentaire, peu de sites sont à ce jour classifiés et l'utilisation d'Internet pour les mineurs s'en trouve limitée d'autant.

ii. Le filtrage des fournisseurs d'accès.

Légalement (et cela a été renforcé par la loi pour la confiance dans l'économie numérique), les fournisseurs d'accès sont tenus de proposer un dispositif de filtrage pour l'accès à Internet⁶⁴⁵. Ils proposent des logiciels gratuits ou payants qui bloquent l'accès aux sites en référençant des mots-clés ayant trait à des contenus inconvenants pour les enfants comme la pornographie, ou illicites comme ceux ayant trait à la pédophilie. Ce procédé de filtrage dont-il a déjà été question en *supra* leur permet de se passer d'une classification des pages *a priori* en utilisant une analyse générale du site.

Les fournisseurs d'accès ont créé une organisation "Inhope" qui est soutenue par l'Union européenne. Leur but est de lutter contre les contenus illégaux sur Internet. L'intérêt véritable réside dans le fait que l'appartenance au réseau "Inhope" permet d'accélérer de façon significative le traitement d'une réclamation concernant un contenu hébergé à l'étranger. Une

⁶⁴⁴ La plate-forme PICS : Platform for Internet Content Section. Il s'agit d'un langage commun pour décrire le contenu. Elle a été élaborée en 1995 par le World Wide Web Consortium

⁶⁴⁵ Article 43-7 de la loi relative à la liberté de communication n° 86-1067 du 30 septembre 1986 : « les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autre que des correspondances privées sont tenus, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens »

réclamation parvient en quelques secondes dans le pays où le contenu est hébergé et peut donc être supprimé⁶⁴⁶.

Ce système permet de modifier l'accès en fonction de l'adresse e-mail qui est entrée. Seule l'identité principale (l'adresse e-mail principale) permet une modification des choix d'accès. Il est possible de paramétrer les critères de sélection en les adaptant à chaque enfant.

2.a'''. Les logiciels dédiés ou le filtrage basé sur les données.

i. Le filtrage basé sur les données : l'exemple du filtre mis sur pied par l'association Innocence en danger.

L'association Innocence en danger a parrainé la conception d'un logiciel de filtrage parental appelé LCPA (logiciel de contrôle parental d'activité). Ce logiciel de contrôle parental a pour vocation une action double. Lors de discussions de l'enfant dans des forums, chats ou messageries instantanées, le logiciel doit pouvoir empêcher la communication par l'enfant de mots ou informations personnelles prohibées par les parents, avec saisie écran. Dans le même temps, il va délivrer des messages d'alertes et de rappel à l'enfant, des restrictions programmées par les parents pour assurer sa protection durant la navigation. Les parents peuvent consulter (comme c'est le cas pour de nombreux autres outils de contrôle parental) l'historique de la navigation de l'enfant⁶⁴⁷ et voir les saisies écrans montrant les tentatives faites par les enfants de communiquer des informations personnelles prohibées.

ii. Le logiciel Logprotect.

Ce logiciel est parrainé par la Secrétaire d'Etat aux droits des victimes avec le soutien de l'AFA (association des fournisseurs d'accès). C'est un logiciel gratuit qui doit être téléchargé et paramétré par les parents. Ils devront à cette occasion déterminer les informations qui ne devront pas être communiquées par leurs enfants lors de leur navigation. Il s'agit d'empêcher l'enfant connecté de communiquer toute information sensible concernant sa taille, son âge, l'adresse familiale, son école, ou toute autre coordonnée personnelle susceptible d'aboutir à son identification. S'il venait à taper une de ces informations, non seulement celle-ci ne sera pas envoyée mais un message de mise en garde apparaîtra à l'écran. Tout incident de ce type

⁶⁴⁶ Ce point sera étudié en infra dans le point concernant la responsabilité des intermédiaires. Pour ce faire voir le site suivant : <http://www.inhope.org/french/index.htm>

⁶⁴⁷ Rapport de propositions remis à Philippe Douste-Blazy sous la Présidence de Joël Thoraval, Protection de l'enfant et usages d'Internet, Conférence de la famille 2005, p. 74

est enregistré par le logiciel et accompagné d'une copie d'écran qui pourra être consultée par les parents. Ce logiciel a une vertu préventive et éducative⁶⁴⁸.

2.a'''''. Les filtres d'analyse des contenus et des images.

S'agissant des filtres basés sur l'analyse des contenus ; il s'agit d'une technologie rarement employée car difficilement transportable sur un PC. Il s'agit pour ces moteurs d'analyser le contenu de la page et les associations de mots pour décider si la page doit être transmise ou non au navigateur⁶⁴⁹.

L'illicéité des contenus et des données diffusées sur Internet constitue l'objet d'une jurisprudence particulièrement récente et progressive. Hormis la pédophilie, les juridictions françaises ont eu entre 1996 et 2003 à se prononcer sur une vingtaine d'affaires particulièrement repoussantes. Ca été le lieu de discuter la définition qui devait être donnée à la notion de contenu illicite.

2.a'''''. Les filtres de contrôle d'applications.

Il s'agit en l'hypothèse de filtrer voire de bloquer l'accès aux newsgroups, aux Chats et aux sites de Peer to Peer.

La qualité des logiciels existants est très variable. Certains vont interdire l'accès à des sites inoffensifs. Des farouches défenseurs de la liberté d'expression s'opposent à toute initiative visant à limiter l'accès à l'information disponible sur le Net, même si les parents en sont à l'origine. D'autres groupes ne s'y opposent pas mais, refusent l'idée d'une législation rendant obligatoire dans les écoles et les bibliothèques subventionnées par l'Etat (fédéral dans le cas des États-Unis)⁶⁵⁰ de logiciels de contrôle parental.

Face à la multitude de logiciels proposés sur le marché, il est très difficile pour les parents de s'y retrouver. Certes, des initiatives existent tel le banc d'essai des vingt-cinq principaux

⁶⁴⁸ www.logprotect.net

⁶⁴⁹ C'est le cas du logiciel PureSight d'Incognito ; il filtre en dynamique les sites inappropriés sans avoir recours à une liste d'URL préétablies. Il fait intervenir un « algorithme utilisant les techniques d'intelligence artificielle » qui permet d'analyser le contenu de la page demandée.

⁶⁵⁰ Le Children's Internet Protection Act signé par le Président alors sortant Bill Clinton, obligeait les écoles et les bibliothèques publiques recevant les des E-rate funds (subventions publiques reliées à des programmes d'intégration d'Internet) à utiliser un logiciel pouvant filtrer le contenu de sites Web aux mœurs douteuses. Les administrateurs des institutions visées étant libres de choisir leur système de filtrage en tenant compte des sensibilités locales de leur communauté ; Charles Perreault, Logiciels de filtrage : pour ou contre ? Infos rapides sur Juriscom.net le 26 janvier 2001 : <http://www.juriscom.net/actu/achv/200101.htm>

logiciels de contrôle parental présents sur le marché assuré par l'association Action Innocence. Les logiciels sont notés en fonction de leurs capacités de blocage et de leur facilité d'utilisation⁶⁵¹. L'évaluation de ces logiciels est actualisée sur une base trimestrielle.

L'Institut national de la consommation (INC), à la demande de la Délégation interministérielle à la famille, de la Délégation aux usages d'Internet et de la Direction du développement des médias a également réalisé un essai comparatif de quinze logiciels de contrôle parental en mai 2004. L'enquête a montré qu'il existait de bons outils de filtrage selon l'usage que l'on veut en faire⁶⁵².

Le choix du logiciel de contrôle revient entièrement aux parents ; leur tâche n'est pas aisée surtout si ils n'ont pas de réelles connaissances et compétences en informatique et sur Internet. Comment pourraient-ils s'y retrouver, d'autant que la liste des logiciels est longue et que leurs fonctionnalités sont diverses, avec une efficacité variable. Certains ne sont pas suffisamment fiables, soit parce qu'ils n'identifient qu'un nombre restreint de sites, ou au contraire en retiennent trop ; soit parce qu'ils sont fastidieux à installer pour les parents ou trop aisés à désactiver par l'enfant. De fait, il n'existe pas de logiciel parfait malgré les progrès technologiques.

En matière de filtrage, il est impossible qu'une liste d'adresses soit à la fois pertinente et exhaustive et que cela perdure en dépit des évolutions du cyberspace. Des sites apparemment inoffensifs peuvent être bloqués par un filtrage trop strict. Certains logiciels de contrôle parental se désactivent très facilement en utilisant, par exemple, la fonction de désinstallation « Ajout/Suppression de programme » ou par un simple raccourci clavier, voire une case à décocher. Résultat, un enfant malin et averti trouvera rapidement comment passer outre (à l'insu de ses parents) cet outil de contrôle⁶⁵³.

Certaines astuces permettent également à des jeunes de contourner facilement certains logiciels de filtrage. Ainsi, les « serveurs d'anonymisation » ou « anonymizers » servent de paravent entre l'ordinateur de l'internaute et le site visité. Il est quasiment impossible de vous identifier aucune adresse ou donnée personnelle n'apparaissant. De fait, la page souhaitée

⁶⁵¹ Pour une évaluation des logiciels voir le site www.actioninnocence.org

⁶⁵² Voir le rapport, Protection de l'enfant et usages d'Internet, préc.

⁶⁵³ Ibid.

s'affiche dans celle de l'anonymiseur et peut être consultée par l'enfant en dehors de tout contrôle⁶⁵⁴.

Autre limite à l'efficacité des filtres et autres logiciels de contrôle, ils ne peuvent s'appliquer que dans la mesure où il est possible d'identifier l'internaute comme étant mineur. Dès lors, se pose la question de l'identification du mineur en ligne, mais également celle du respect des libertés fondamentales du mineur comme : sa liberté d'expression, son droit à sa correspondance privée, etc., qui peuvent être malmenées par la consultation par ses parents de l'historique de sa navigation. Les données retenues par les filtres permettent au parent un contrôle *a posteriori*. Ce contrôle qui peut se révéler d'un intérêt double : d'une part réajuster les paramètres des filtres parentaux et/ou adapter le discours de prévention fait au mineur.

Dans le registre des moyens techniques de prévention pour le mineur dans le cyberspace, les certificats numériques ont un rôle important à jouer, quoiqu'ils ne soient pas encore vulgarisés.

2-b. Les certificats électroniques.

La surveillance et l'identification sont contraires au droit au respect de la vie privée qui est un droit fondamental reconnu par l'article 8 de la Convention européenne des droits de l'homme. Afin de permettre une identification fiable qui soit également respectueuse de la vie privée des internautes, l'Observatoire propose la création d'un statut juridique spécial pour des tiers de confiance qui seraient chargés d'attribuer des codes adultes après vérification de l'âge des requérants, aux fins de consultation de sites interdits ou inappropriés aux mineurs.

Le législateur a statué en la matière à l'occasion de la réglementation sur la signature électronique par la loi du 13 mars 2000 transposant la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. Il a apporté des précisions sur les certificats électroniques dans le chapitre III du décret 2001-272 du 31 mars 2001.

Un certificat électronique est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique. L'autorité de certification fait foi de tiers de confiance

⁶⁵⁴ Ibid.

et atteste du lien entre l'identité physique et l'entité numérique⁶⁵⁵. Un certificat électronique doit être qualifié ; pour ce faire il doit comporter certains éléments et être délivré par un prestataire de services de certification électronique.

Pour être qualifié un certificat doit comporter :

- une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
- l'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;
- le nom du signataire ou son pseudonyme, celui-ci devant être identifié comme tel ;
- le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
- les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
- l'indication du début et de la fin de la période de validité du certificat électronique ;
- le code d'identité du certificat électronique ;
- la signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
- le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé⁶⁵⁶.

La délivrance d'un certificat numérique suppose un processus complexe et fiable de vérification de l'identité du demandeur. Il existe plusieurs types de certificats en fonction du niveau de sécurité⁶⁵⁷. Pour les plus fiables, cela suppose la confrontation physique du demandeur avec l'un des agents auxquels l'autorité délègue le pouvoir d'attester son identité⁶⁵⁸. La limite d'une telle procédure tient à son coût et sa complexité. Ces deux

⁶⁵⁵ http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique

⁶⁵⁶ Article 6-I, chap. III du décret 2001-272.

⁶⁵⁷ On recense 4 types de certificats, répartis en classe :

- classe 1: adresse e-mail du demandeur requise;
- classe 2: preuve de l'identité requise (photocopie de carte d'identité par exemple);
- classe 3: présentation physique du demandeur obligatoire.
- classe 3+: identique à la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, ou carte à puce; exclut donc les certificats logiciels)

http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique

⁶⁵⁸ Liste des autorités de certifications et des certificats électroniques reconnus par le Ministère de l'Économie en France se trouve sur le site dudit ministère : <http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html>

éléments sont de nature à limiter le nombre d'utilisateurs majeurs et/ou mineurs d'Internet pouvant en bénéficier⁶⁵⁹.

Dans la même logique il existe en Grande-Bretagne la Citizen Card que propose la société Interactive Age Check (IAC)⁶⁶⁰ et que semble soutenir la Home Office. Elle propose la délivrance au terme d'une procédure simplifiée de codes et certificats d'identités utilisables sur Internet. Tout membre d'une profession assermentée (référént de police, juge, médecin, enseignant, ministre du culte, fonctionnaire élu, etc.) peut se substituer à l'autorité de certification et garantir l'identité du requérant⁶⁶¹. La difficulté tient à l'élargissement du nombre de personnes pouvant faire œuvre de certification, cela ne fragilise t-il pas l'authentification et sa probité ?

Aux Etats-Unis, le législateur par le biais de la Child Online Protection Act impose aux sites proposant des contenus nuisibles aux enfants d'en restreindre l'accès en vérifiant l'âge des visiteurs. L'un des moyens est le certificat digital : c'est un certificat électronique délivré par des autorités de certification dans le cadre de la signature électronique. Il existe deux méthodes pour déterminer l'âge et l'identité de l'internaute ; une méthode directe par la carte de crédit et une méthode indirecte par la poste⁶⁶². S'agissant de la carte de crédit, le postulat est que seules des personnes majeures peuvent en disposer. Pour ce qu'il est de la poste, l'internaute envoie copie d'un document d'identité (permis de conduire, certificat de naissance, etc.) en retour il se voit délivrer un ID (une identité) plus un mot de passe⁶⁶³.

En France en mars 2000, la Poste et Sagem ont créé une nouvelle société : Certinomis dirigée par Inès Sen. Sa mission était d'élaborer une puissante autorité de certification. Cette société devait proposer une gamme de services de certificats destinés aux particuliers et aux entreprises. Certinomis devait émettre des certificats électroniques faisant le lien entre l'identité de l'internaute et des clefs cryptographiques⁶⁶⁴. Pour bénéficier d'un certificat, il était envisagé que l'internaute se présente au guichet d'une agence de La Poste avec des pièces d'identité et quittances. En échange et pour une cotisation annuelle à déterminer,

⁶⁵⁹ Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur Internet, préc.

⁶⁶⁰ www.citizencard.com

⁶⁶¹ Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur Internet, préc.

⁶⁶² www.cyberverify.com

⁶⁶³ Maximilien Amégée, La protection des mineurs sur Internet. La problématique de la pornographie.

⁶⁶⁴ Eric Mugnere, 2 mars 2000, A la Poste, le certificat numérique fera foi : <http://www.transfert.net/a520>

Certinomis lui délivrait via Internet un passeport stocké sur son disque dur ou sur une carte à puce en théorie infalsifiable grâce à l'usage de la cryptographie.

Lorsque l'internaute voudra accéder à un site, celui-ci devrait vérifier le certificat automatiquement et refuser ou non l'accès en fonction de la nationalité ou de l'âge du visiteur. L'accès pouvant être bloqué en l'absence du certificat.

Les entreprises désireuses de sécuriser leurs échanges avec d'autres entreprises ont montré les premières un intérêt vif. Inès Sen, alors Présidente de Certinomis avait souligné que « le développement des certificats vers le grand public sera très long ». En 2003 Certinomis détenue à 100% par la Poste se recentre sur son offre « institutionnelle » de délivrance de certificats d'identité électronique à des personnes (particuliers⁶⁶⁵, professions libérales, représentants d'entreprises, de collectivités, etc.) ou à des machines (serveurs, marchand, etc.)⁶⁶⁶.

Il est toujours fait référence aux particuliers qui peuvent bénéficier des services de certification de Certinomis. Cependant, force est de constater que la banalisation de ces certificats numériques vers grand public n'est pas encore effective. Une orientation vers la certification envers les professionnels est très marquée dans la politique de Certinomis⁶⁶⁷.

Les certificats électroniques pourront peut-être devenir à terme la solution à l'identification des mineurs en ligne et de toutes les difficultés qui en découlent, mais en l'état actuel de la technologie ou plutôt des services fournis, il n'est pas possible d'en faire un moyen incontournable de la protection des mineurs dans le cyberspace. C'est pour cette raison qu'il a fallu prévoir des méthodes palliatives en amont comme en aval de l'utilisation de la toile par le mineur pour le protéger parfois malgré lui.

⁶⁶⁵ Sur son site Certinomis expose les conditions d'obtention des certificats électroniques pour les particuliers. http://www.certinomis.com/certificats_particuliers.php

⁶⁶⁶ Fédération Nationale des Tiers de Confiance (fntc), Certinomis se repositionne sur son métier de Certification et nomme sa nouvelle Présidente : http://www.fntc.org/articles/article.php3?id_article=28

⁶⁶⁷ « Certinomis fournit des certificats permettant de sécuriser et de signer électroniquement les échanges dématérialisés entre les entreprises (B to B), les administrations (A to A) ou entre les entreprises et les administrations », Communiqué de presse du 6 octobre 2004, Certinomis élargit ses prestations de services autour des certificats d'organisation. Nulle mention n'est faite des prestations délivrées aux particuliers. http://www.fntc.org/articles/article.php3?id_article=75

§2. La protection *a posteriori* du mineur dans le cyberspace.

Les atteintes dont sont victimes les mineurs dans le cyberspace sont d'une gravité telle que tous les moyens sont mobilisés dans la lutte contre cette cybercriminalité. La prévention de la survenance de la cybercriminalité a montré ses limites. La vigilance active des tuteurs légaux et/ou l'utilisation des moyens technologiques ne garantissent pas un succès absolu, eu égard à la capacité de contournement de ces mesures par le mineur. Il a fallu penser des méthodes supplémentaires de contrôle s'opérant certes *a posteriori*, mais visant les interventions à venir du mineur dans le cyberspace. Ces méthodes supposent une atteinte (justifiée ?) aux droits du mineur et une participation active dans la sécurisation du cyberspace notamment grâce à la dénonciation de comportements et de contenus inconvenants pour le mineur.

A. Une « atteinte justifiée » aux droits du mineur.

Le mineur est titulaire de droits fondamentaux qui doivent être respectés. Le droit à la liberté d'expression et le droit à la correspondance privée en font partie. Les articles régissant ces droits prévoient une possibilité de restriction de leur exercice par l'autorité publique, à condition que cette ingérence soit légale et nécessaire. Nulle mention n'est faite de la légitimité et des conditions d'ingérence des particuliers en l'occurrence les parents du mineur. Dans la pratique, il est admis que les parents puissent restreindre la liberté d'expression et le droit à la correspondance privée de leur enfant mineur selon les circonstances. Cette tolérance s'insère dans une idée de protection du mineur par devers lui-même. Cette ingérence ne doit pas être constitutive d'une atteinte arbitraire aux droits fondamentaux du mineur que sont sa liberté d'expression et son droit à la correspondance privée.

1. Atteinte à la liberté d'expression du mineur.

Le mineur a droit à sa liberté d'expression, cette liberté ne peut cependant en aucun cas être absolue. Cette liberté souffre des limitations du fait de la nécessité de l'exercice normal d'autres droits et libertés⁶⁶⁸. Des restrictions liées à sa minorité sont également à prendre en

⁶⁶⁸ Selon l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 « la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire librement sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi.

compte. La liberté d'expression du mineur est régie par les articles 12 et 13 de la Convention internationale des droits de l'enfant de 1989⁶⁶⁹.

La Convention européenne en son article 10 §2 prévoit que, la liberté d'expression puisse être limitée par la loi en vertu de « mesures nécessaires, dans une société démocratique [...] à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale... ». Les limites qui sont opposées à la liberté d'expression ont vocation à s'appliquer à Internet.

La limitation de la liberté du mineur dont-il s'agit ici est subjective et n'est pas clairement régie par la loi. Aucune norme et aucune jurisprudence n'a posé à ce jour de cadre à la limitation parentale de la liberté d'expression du mineur dans le cyberspace. Les moyens de cette limitation ne sont pas objectivement répertoriés. Les méthodes varient selon les personnes concernées et l'ampleur du but visé.

La liberté d'expression du mineur trouve à s'exercer sur différents supports : les forums de discussion, les chats, les blogs, les webzines, les pages ou sites personnels, etc. Les tuteurs peuvent interdire tout accès du Net au mineur. Mais à moins de l'enfermer également, il existe plusieurs lieux où le mineur peut naviguer dans le cyberspace : à l'école, chez des tiers, dans des cybercafés, etc. Le danger dans ces cas est encore plus grand dans la mesure où aucun adulte n'est désigné pour assurer une navigation sereine du mineur. Le mineur n'est quasiment soumis à aucun contrôle (sauf hypothèse de navigation chez des amis dont les parents sont vigilants). Le mineur laissé à lui-même donne libre cours à sa liberté d'expression ce d'autant qu'il peut avoir un sentiment d'impunité à l'égard de ses parents ou tuteurs légaux absents.

Les tuteurs du mineur peuvent utiliser la technologie, tels les logiciels de contrôle interdisant au mineur l'accès aux forums, chats, etc. Dans ce contexte, la limitation se veut totale. Le mineur ne pouvant pas accéder à ces fonctionnalités du réseau, il ne pourra être confronté aux

⁶⁶⁹ Article 12 alinéa 1 de la Convention Internationale des droits de l'enfant de 1989 : « Les États parties garantissent à l'enfant qui est capable de discernement le droit d'exprimer librement son opinion sur toute question l'intéressant, les opinions de l'enfant étant dûment prises en considération eu égard à son âge et à son degré de maturité » et Article 13 de la même convention « 1. L'enfant a droit à la liberté d'expression. Ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen du choix de l'enfant.

2. L'exercice de ce droit ne peut faire l'objet que des seules restrictions qui sont prescrites par la loi et qui sont nécessaires :

a) Au respect des droits ou de la réputation d'autrui ; ou
b) À la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques.

contenus inconvenants qui y circulent. Cette méthode a une portée limitée et peut avoir un effet pervers : la portée est limitée car ces outils peuvent être désactivés, l'efficacité de ces outils peut être contournée par des enfants qui iront se connecter ailleurs ; l'effet pervers réside dans le fait que les parents pensant avoir trouvé la solution à la sécurité de leurs enfants mineurs ne seront pas conscients de son inefficacité et le mineur sera encore plus exposé car livré à lui-même.

Le tuteur peut faire preuve d'une omniprésence pendant la navigation du mineur afin de contrôler en temps réel ce que fait ce dernier sur la Toile. Mais cette situation n'est pas tenable à long terme pour le mineur comme pour le tuteur. Elle est matériellement difficile à mettre en œuvre. Cela suppose que l'ordinateur soit disposé dans un lieu de passage, que le mineur navigue sur Internet avec son parent. Selon l'âge du mineur la méthode sera ou non attentatoire à sa liberté d'expression. Pour un mineur de moins de 10 ans dont l'autonomie envers ses parents est faible, il est tout à fait envisageable qu'il navigue avec ses parents. Entre 11 et 13 ans on peut envisager qu'une présence parentale soit nécessaire, sans intrusion, au-delà on est confronté à des adolescents dont l'autonomie est plus grande et dont le besoin d'intimité ne se satisferait pas d'une ingérence intrusive. Ces classes d'âge n'ont pas les mêmes activités dans le cyberspace. La première tranche sera plus portée vers des activités ludiques (recherche d'information sur les héros de dessins animés, de séries télévisées, de stars, etc.), que tournée sur la communication avec autrui dans le cyberspace. La deuxième tranche commence à s'ouvrir sur les modes de communications virtuelles mais reste encore sur une utilisation ludique des ressources d'Internet. La dernière tranche est internaute à part entière, et fait un usage optimal de toutes les fonctionnalités du cyberspace. Sa liberté d'expression s'est d'intervenir dans des forums et des chats, de créer des blogs, d'échanger des dossiers (musique, film, jeux vidéos, etc.), d'échanger des messages via le courrier électronique et plus encore par le biais de la messagerie instantanée.

Les parents, par le biais de logiciels de contrôle ne peuvent restreindre leur accès dans la même mesure. Autant il est compréhensible qu'ils bloquent tout accès aux forums de discussion et aux chats pour les plus jeunes, autant une telle mesure pour la dernière tranche peut être jugée excessive sauf en l'existence de raisons concrètes justifiant une telle décision.

La solution sera plus dans le dialogue, l'explication et la confiance mutuelle que dans la technique ou l'autoritarisme. Le danger identifié avec les forums et les chats réside dans

l'inconnu : le principe de ces espaces est de dialoguer avec des inconnus difficilement identifiables car s'abritant derrière des pseudonymes. Dans le "monde réel", la première chose que les parents apprennent à leurs enfants c'est de ne pas s'adresser aux inconnus ; les parents adoptent le même principe pour le cyberspace ce, d'autant plus que ce dernier est victime d'une réputation largement entachée par la cybercriminalité. On pourrait penser que puisque "l'inconnu" est l'élément qui motive les craintes des parents et les conduit à limiter la liberté d'expression de leurs enfants par un accès inexistant ou restreint aux espaces publics du cyberspace (chats et forums), la liberté d'expression du mineur dans ces espaces peut souffrir de graves restrictions du fait de leur parent.

2. Atteinte aux droits à la vie privée et à la correspondance privée du mineur.

Le mineur a droit au respect de sa vie privée et de sa correspondance privée. Le courrier électronique en tant qu'il correspond aux critères d'une correspondance privée permet au mineur de faire valoir son droit au respect de sa correspondance privée électronique.

Il ne peut être fait atteinte à ce droit conformément à plusieurs dispositions juridiques concordantes : la Convention internationale des droits de l'enfant adoptée par l'Assemblée Générale de l'ONU le 20 novembre 1989 et entrée en vigueur le 2 septembre 1990. Elle pose en son article 16 que «1) *Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* 2) *L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* », l'article 8 de la Convention européenne des Droits de l'Homme, article 12 de la Déclaration Universelle des Droits de l'Homme de 1948, la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances par voie électronique et l'article 9 du code civil protègent également ce droit à la correspondance privée du mineur.

La loi prévoit de manière restrictive des interceptions de correspondances privées à certaines conditions strictement déterminées. L'article 3 de la loi du 10 juillet 1991 relative au secret des communications émises par voie de télécommunications prévoit que le Premier ministre peut autoriser de telles interceptions afin de permettre l'obtention de renseignements relatifs à

la sécurité nationale, la prévention du terrorisme, etc.⁶⁷⁰. Par ailleurs, les articles 100 et 100-7 du Code de procédure pénale prévoient des interceptions sur l'ordre de l'autorité judiciaire. Nulle mention n'est faite du cas spécifique de la correspondance privée du mineur, seule la Convention internationale des droits de l'enfant s'y réfère précisément.

La violation du secret des correspondances est pénalement sanctionnée par l'article 226-15 du code pénal. Cette violation consiste dans « *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ». Peut-on envisager que cette sanction puisse être invoquée contre un parent qui intercepte le courrier électronique de son enfant mineur. On pourrait alléguer que, n'ayant pas fait preuve de mauvaise foi *a priori* dans cette interception, mais plutôt d'une volonté de protéger son enfant par devers lui, il pourrait bénéficier d'une tolérance.

A l'heure où on invoque de plus en plus la responsabilité des parents dans le cadre de la protection de leurs enfants contre des contenus choquants dans le cyberspace, il semble logique que les mesures de protections dont ils disposent puissent être étendues ou du moins envisagées de manière extensive.

Il est admis en France que les parents ont le droit de prendre connaissance de la correspondance adressée à leurs enfants mineurs. Cette « tolérance » française⁶⁷¹ en contradiction avec l'article 16 de la Convention internationale des droits de l'enfant qui interdit les « ingérences arbitraires ou illégales dans la correspondance de l'enfant » se justifie uniquement par la vulnérabilité des mineurs susceptibles d'être confrontés jusque dans leur messagerie personnelle (par le biais des Spam notamment) à des contenus illicites. Cette tolérance ne fait pour l'heure l'objet d'aucune réglementation. Aucune juridiction n'a eu à connaître à ce jour d'un litige opposant un mineur à ses parents coupables d'interception de sa

⁶⁷⁰ A. Lepage, Liberté et droits fondamentaux à l'épreuve de l'Internet, préc. P.40.

⁶⁷¹ Marie-Pierre Fenoll-Trousseau et Gérard Haas, Internet et protection des données personnelles, p. 64

correspondance privée en contradiction avec la Convention internationale sur les droits de l'enfant.

L'interception de la correspondance privée du mineur peut être faite à plusieurs niveaux. En concordance avec les définitions faites de la correspondance privée, l'interception concerne toutes les formes de la correspondance privée du mineur : le courrier électronique, la messagerie instantanée. Il n'y a pas de méthode intangible du contrôle parental de la correspondance privée électronique du mineur.

Les parents épurent-ils la messagerie de leur enfant des contenus indésirables préalablement à sa lecture par ce dernier ? Si tel est le cas il existe un risque de dérive interventionniste qui pourrait les conduire à censurer tout message qui ne leur conviendrait pas, que le contenu en soit ou non illicite. Le contrôle pourrait s'effectuer de concert avec le mineur titulaire de la messagerie électronique. Il y aurait une dimension pédagogique dans laquelle l'accent serait mis sur le dialogue entre le mineur et ses parents. Cela n'est possible que dans la mesure où le mineur accepte comme légitime l'ingérence parentale dans sa sphère privée. Pour que l'intervention parentale soit possible, il faut que le code secret d'accès à la messagerie soit communiqué par son détenteur volontairement ou non.

L'interception de la correspondance privée dans la messagerie ne peut se faire qu'*a posteriori*. Quelle que soit la nature de l'intervention des parents dans la messagerie électronique du mineur, elle ne pourra intervenir qu'après réception du message, sauf à bloquer l'arrivée de message provenant de certaines adresses répertoriées comme indésirables.

Face à l'ampleur de la tâche de la protection des mineurs dans le cyberspace, tous les moyens et toutes les volontés se mobilisent pour ce combat titanesque. Après un appel à la vigilance physique, à la prévention technologique, on fait également appel au sentiment citoyen des internautes. On leur donne la possibilité de participer au combat contre la cybercriminalité envers les mineurs par un système de dénonciation de contenus choquant et délictuels.

B. La dénonciation pour un cyberspace plus propre.

Dans la lutte contre la prolifération des contenus choquants et de la cybercriminalité contre les mineurs, tous les internautes sont mis à contribution. On les incite vivement à faire œuvre citoyenne en contribuant à rendre le cyberspace plus propre et plus sûr pour les enfants. Pour ce faire, on a mis une série de mesures à leur disposition. Ils peuvent dénoncer les contenus illicites dans des points de contact prévus pour ; ils peuvent de manière plus personnelle s'engager en constituant ou en adhérant à une association de défense de l'enfance dans le cyberspace.

1. Les points de contacts généraux et spécifiques.

Un point de contact est un site qui recueille les signalements faits par les internautes de contenus choquants rencontrés au cours de leur navigation dans le cyberspace. Un formulaire en ligne leur permet de décrire le contenu d'un site, d'un chat ou d'un forum délictueux et d'en indiquer les coordonnées. Ce type d'initiative visait à faciliter les procédures, mais surtout à mettre sur pied des mesures appropriées à la spécificité des infractions commises sur Internet permettant de déjouer la volatilité des contenus dans le cyberspace. Il est possible de faire un signalement anonyme, bien que les sites incitent fortement au contraire dans l'hypothèse où un complément d'informations serait nécessaire.

L'association des fournisseurs d'accès et de service Internet (AFA) a créé en 1998 le Point de contact⁶⁷². Il est destiné à recevoir les signalements de contenus impliquant la pornographie infantile et l'incitation à la haine raciale. Le signalement est anonyme si l'internaute le souhaite. Il peut dénoncer un site web, un newsgroup, un courriel non sollicité, etc. Le site du Point de contact propose un formulaire en ligne ainsi que des modèles de courriers dans plusieurs langues à adresser au Point de contact et aux fournisseurs de service impliqués ou encore aux autorités compétentes. Selon le cas, le Point de contact transmet les signalements reçus aux fournisseurs concernés, aux autorités compétentes ou à son correspondant étranger si le dossier le requiert⁶⁷³. Le point de contact a également pour mission d'informer

⁶⁷² www.pointdecontact.net

⁶⁷³ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p.68.

l'internaute sur les textes pénaux applicables en matière de contenus choquants et illégaux pour les mineurs (pédophilie et incitation à la haine raciale)⁶⁷⁴.

Le 9 novembre 2001 le gouvernement français lance un site Web permettant de signaler et de dénoncer des sites à caractère pédophile⁶⁷⁵ ; les internautes témoins de propagation d'images ou de textes avilissant les enfants peuvent désormais alerter les autorités via un site gouvernemental. En France l'Office central de lutte contre les crimes liés aux technologies de l'information et de la communication (OCLCTIC) réceptionne les renseignements collectés lors de ces signalements. Des formulaires sont proposés en ligne, et peuvent également être rempli anonymement. La Cnil a donné son feu vert à la mise en place de ce fichier⁶⁷⁶. Le site énonce également les principaux textes législatifs de référence, des conseils pratiques pour les parents et les enfants.

Il n'existe pas d'obligation générale de surveillance à la charge des fournisseurs d'accès et d'hébergement ; voulant compenser cette absence, les parlementaires français leur ont imposé de « mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de contenus⁶⁷⁷ ».

La faculté de dénonciation est ouverte à tous et non réservée aux associations de lutte contre le racisme ou de défense des mineurs constituées depuis au moins cinq ans au jour du signalement⁶⁷⁸. Faudrait-il y voir un premier pas vers le développement d'une citoyenneté numérique qui donne une portée nouvelle à l'obligation de dénoncer tous crimes et certains délits en train de se commettre (code pénal article 434-1 et suivants).

Les réserves que l'on peut avoir sur cette mesure tiennent aux risques accrus de dénonciations calomnieuses. A la différence de la notification abusive d'une demande de suspension adressée à un fournisseur d'hébergement⁶⁷⁹, le signalement effectué de mauvaise foi par un internaute n'est pas précisément sanctionné par la Loi pour la confiance dans l'économie numérique. Cependant, le recours à un tiers de bonne foi (le fournisseur d'accès ou d'hébergement) pour transmettre une information inexacte à l'autorité compétente n'empêche

⁶⁷⁴ Le Forum des droits sur Internet, « Assurer la protection de l'enfant sur Internet » 05/09/2001, http://www.foruminternet.org/documents/en_pratique/lire.phtml?id=118

⁶⁷⁵ <https://www.internet-mineurs.gouv.fr/>

⁶⁷⁶ Le Figaro 17 novembre 2001, Marie Sigaud, « Mineurs : un site pour les protéger ».

⁶⁷⁷ Cf. infra la responsabilité des intermédiaires dans le cyberspace.

⁶⁷⁸ Légipresse n°214 – septembre 2004, p. 93, Emmanuel Dreyer, « La responsabilité des internautes et éditeurs de sites à l'aune de la loi pour la confiance dans l'économie numérique ».

⁶⁷⁹ Art. 6-1, 4° de la LCEN.

pas la sanction de la dénonciation calomnieuse⁶⁸⁰. Cette infraction suppose que le fait dénoncé ait été imputé directement ou non à une personne déterminée. Du fait de l'anonymat ambiant dans le cyberspace, il sera difficile de reprocher à l'auteur du signalement d'avoir agi dans le but de nuire à autrui en l'exposant injustement à une sanction⁶⁸¹. Le cas échéant, on pourra retenir l'infraction de dénonciation mensongère prévue à l'article 434-26 du code pénal. Ce texte pose une incrimination de portée limitée. Il punit de six mois d'emprisonnement et de 7 500 € d'amende «*le fait de dénoncer mensongèrement à l'autorité judiciaire ou administrative des faits constitutifs d'un crime ou d'un délit qui ont exposé les autorités judiciaires à d'inutiles recherches*». Ce texte tend plus à protéger l'autorité de justice d'engorgements par des plaintes imaginaires ou délibérément inexacts. Pour que l'infraction soit qualifiée, il faut que le signalement ait été suffisamment convaincant pour entraîner des investigations inutiles⁶⁸².

Il subsiste des limites à l'efficacité des signalements.

- Extrêmement volatile, un signalement fait à un moment précis risque de perdre toute valeur juridique si les photos ou les contenus incriminés sont supprimés du serveur avant que l'autorité saisie ne les aie elle-même constatés. Dans l'hypothèse même où l'autorité saisie aura effectué un constat de contenus illégaux apparaissant sur des serveurs anonymes de pays étrangers (dont la législation diffère de la culture juridique française et européenne) quels sont ses pouvoirs ?
- En ce qui concerne la convention internationale de lutte contre la cybercriminalité, les pays européens ont tout tenté pour inclure un article visant à lutter contre les sites à contenu xénophobe ou raciste. Mais ils se heurtent au refus des Etats-Unis qui invoquent le premier amendement de leur Constitution. Ils invoquent également le premier amendement s'agissant de la représentation de pornographie infantile virtuelle.
- Les mesures liées à la cryptographie et au contrôle des fichiers de connexion des fournisseurs d'accès à Internet, posent quant à elle le problème des libertés individuelles et du respect de l'anonymat. Les projets actuels risquent de surtout

⁶⁸⁰ Philippe Conte, Droit pénal spécial, Litec, 2003, p.286, n°495. Compétences en matière médicale : Crim. 22 octobre 2002, Bull. n° 199.

⁶⁸¹ Crim. 17 mai 1994 : Bull. n° 184.

⁶⁸² Crim. 10 octobre 2000 : Droit pénal 2001, p.16, n°2 observations M. Véron.

pénaliser les internautes ordinaires sans atteindre les cybercriminels qui gardent souvent une longueur d'avance en termes d'ingéniosité et d'innovation technologique⁶⁸³.

Le signalement de contenus illégaux, s'adresse à tous dans l'optique d'un cyberspace citoyen où tous œuvreraient pour un espace convivial et sûr pour tous notamment pour les internautes les plus vulnérables que sont les mineurs. Dans cette continuité, la constitution en associations qui militent et se battent pour un Internet approprié aux mineurs est un élément de poids dans la recherche d'un cyberspace plus propre.

2. La constitution en association.

Les parents, les tuteurs légaux et de manière générale les acteurs d'Internet militant pour un Internet plus propre et plus sûr pour les enfants s'associent parfois de manière plus ou moins formelle afin de mener ensemble ce combat contre la cybercriminalité dans le cyberspace.

A la suite de la multiplication des initiatives nationales tendant à dénoncer les contenus pédopornographiques dans le cyberspace, Childnet International⁶⁸⁴ a proposé en 1997 aux différentes hotlines de travailler ensemble. Pour ce faire, elle a obtenu des fonds européens (Daphne Programme) pour établir un forum européen. Le 23 novembre 1999, ce forum est devenu l'association Inhope de droit hollandais. A ce jour onze hotlines en sont membres, plus un membre provisoire et trois membres associés. L'action de l'association consiste à supprimer les contenus de pornographie enfantine d'Internet et à protéger les enfants des contenus et des usages illégaux d'Internet. L'association organise des échanges d'expertise, soutient les nouvelles hotlines, assure l'interface avec des initiatives analogues hors de l'Union européenne et organise des campagnes d'information à destination des décideurs pour les sensibiliser à cette problématique. Lorsqu'une dénonciation implique plusieurs pays, il

⁶⁸³ La cybercriminalité intéressera-t-elle les candidats aux présidentielles ? Par Carlo Revelli Président Directeur Général de Cybion (Société pionnière dans l'intelligence économique et stratégique sur Internet, Cybion propose depuis 1996 une gamme de services pour vous accompagner dans la maîtrise de l'information disponible sur Internet. Avec nos prestations, adaptées à vos besoins, vous disposez de données stratégiques immédiatement exploitables, Tribune publiée dans les Echos.net du 11/02/02

http://www.cybion.fr/pages/presse/carlo_cybercriminalite.html

⁶⁸⁴ Childnet International est une association à but non lucratif localisée à Londres. Elle a été créée en 1995 avec comme mission la promotion des intérêts des enfants dans les communications internationales.

peut transmettre au membre concerné les signalements qu'elle reçoit pour le matériel localisé dans son pays⁶⁸⁵.

De nombreuses associations interviennent dans le cyberspace. Il est possible de se joindre à leur action de diverses manières : en y adhérant ou en leur apportant une contribution pécuniaire. Leurs actions s'exercent dans et en dehors du cyberspace.

Par exemple, l'association Innocence en Danger dont la présidente est Homayra Sellier, a été créée pour appliquer le Plan d'Action, rédigé à l'issue de la réunion d'experts des 18 et 19 janvier 1999 tenue à l'UNESCO, sur le thème de « l'Exploitation des enfants, la pornographie impliquant des enfants et la pédophilie sur Internet : un défi mondial ». Elle est présente dans 27 pays. Innocence en Danger regroupe des militants, des spécialistes d'Internet, des juristes, des décideurs du monde politique, économique, médiatique dans le but de sensibiliser l'opinion mondiale sur le problème croissant que constitue la pédocriminalité. Elle se veut une force d'actions, de sensibilisation, de propositions, d'éducation et d'informations auprès des organisations gouvernementales ou non, des instances européennes et internationales, des entreprises et de la population (écoles, collectivités locales, groupes de jeunes). Innocence en danger travaille à mobiliser le maximum des ressources :

- Ressources humaines : policiers, magistrats, législateurs, journalistes, médias, institutions, ONG, médecins et professionnels de l'enfance pour leur pouvoir de décision, d'information et de dénonciation. Elle en appelle également à toute personne souhaitant participer à leurs actions pour un Internet plus sûr pour les mineurs.
- Les ressources financières par les contributions des personnes morales ou physiques, organisations publiques, institutionnelles ou privées.
- Les ressources technologiques : professionnels de l'informatique pour leur créativité et la mise au point de logiciels permettant de contrecarrer les actions des pédocriminels sur le Web et l'élaboration des outils destinés à protéger les jeunes internautes

En 2004, Innocence en danger a lancé le premier logiciel de Contrôle parental d'activité LCPA. Depuis 2006 ils sont partenaires et recommandent le logiciel "Kidz CD" la Surf Station pour votre enfant et adolescent, gratuit et téléchargeable sur ce site⁶⁸⁶.

⁶⁸⁵ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, préc., 84.

L'association e-enfance dont la présidente est Christine du Fretay, a pour ambition d'aider les enfants à tirer le meilleur parti des nouvelles technologies : Internet, téléphone mobile et jeux en réseau⁶⁸⁷.

L'association Droit @ l'enfance dont la présidente est Marie-Pia Hutin-Houillon, a été Créée le 8 mars 2006. Cette association est composée de bénévoles ayant une expérience de terrain de plusieurs années dans le monde associatif. Elle lutte contre tout type de trafic et de maltraitance des enfants, notamment sexuelle (inceste, pédocriminalité) et contre les dangers qui menacent les enfants, des plus jeunes jusqu'aux adolescents, surtout lorsqu'ils surfent sur Internet (via un ordinateur ou un téléphone mobile)⁶⁸⁸.

Il existe de nombreuses autres associations qui ont en commun l'objectif de faire du cyberspace un endroit plus sûr pour les mineurs. Ces associations sont ouvertes à tous ceux qui, internautes ou non souhaitent contribuer à la réalisation de l'objectif d'un Internet plus sûr. Ces associations ont toutes une représentation sur Internet qui rend plus aisée leur contact.

La sécurisation d'Internet est un projet vaste qui nécessite la mobilisation de tous les moyens nécessaires : les moyens humains, techniques, normatifs, etc. s'agissant des ressources humaines (notamment les parents) qui sont sollicitées, la moindre défaillance est sanctionnée civilement ou pénalement.

⁶⁸⁶ <http://www.innocenceendanger.org>

⁶⁸⁷ <http://www.e-enfance.org>

⁶⁸⁸ <http://www.droitlenfance.com/>

Chapitre 2. LA RESPONSABILITÉ DES TUTEURS LÉGAUX DU FAIT DES MINEURS.

Le mineur est apte à répondre de sa responsabilité pénale et/ou civile, et ses parents sont dans une certaine mesure solidairement responsables des infractions qu'il commet. Les parents sont placés au cœur du système de responsabilité qui régit les actes d'un mineur et Internet n'échappe pas à la règle. L'autorité parentale implique des droits et des devoirs pour les parents. Le respect des droits de l'enfant s'effectuant sous la responsabilité de ses responsables légaux, il reste à déterminer au cas par cas l'existence et l'étendue de la responsabilité du parent solidairement avec celle du mineur. La responsabilité civile du mineur entraîne quasi automatiquement la responsabilité solidaire du tuteur légal sauf à prouver que le mineur est titulaire d'un patrimoine propre. Il n'existe en principe pas de responsabilité solidaire pénale.

§ 1. La responsabilité civile des tuteurs légaux du mineur.

La responsabilité civile, c'est l'obligation pour une personne de réparer le préjudice qu'elle a causé à autrui par sa faute, par le fait ou la faute d'une autre personne ou par le fait d'un bien qu'elle a sous sa garde. La réparation se fait par équivalent. Elle consiste dans le paiement d'un capital dit " dommages-intérêts".

A. Les conditions de la mise en cause de la responsabilité civile des tuteurs légaux.

En vertu de l'article 1384 alinéa 4 du code civil « le père et la mère, en tant qu'ils exercent le droit de garde, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux ». En cas de séparation, c'est le parent qui a la garde du mineur qui assume cette responsabilité⁶⁸⁹.

⁶⁸⁹ Selon l'article 1384 du code civil, les père et mère en tant qu'ils exercent l'autorité parentale sont solidairement responsables de tous les dommages causés par leurs enfants mineurs habitant avec eux. Le parent

Il va de soi que la responsabilité des parents ne joue que si l'enfant, auteur du dommage est mineur. Il est exigé une obligation de cohabitation. Le caractère non fautif du dommage ne suffit pas à exonérer les parents de leur responsabilité ni sur l'absence d'une faute d'éducation ou de surveillance de leur part.

1. Une responsabilité objective.

Le droit fait peser sur les parents une responsabilité du fait de leurs enfants mineurs ; il s'agit d'une obligation de plein droit⁶⁹⁰. *A contrario* dès que l'enfant a atteint l'âge de 18 ans ou qu'il a été émancipé à 16 ans⁶⁹¹, la responsabilité des parents n'est plus en cause. Tous les parents sont concernés, qu'ils soient légitimes, naturels ou adoptifs.

Le mineur peut voir sa responsabilité civile personnellement engagée lorsqu'il possède un patrimoine propre et distinct de celui de ses parents. Le mineur et notamment le jeune enfant étant ordinairement insolvable. Pour cette raison, il sera plus intéressant pour la victime de recourir contre les père et mère en vertu de l'article 1384 alinéa 4 qui établit une responsabilité du fait d'autrui (en présument la faute des parents pour insuffisante surveillance ou mauvaise éducation du mineur). En son alinéa 7, l'article 1384 permettait aux parents de s'exonérer de leur responsabilité en prouvant qu'ils n'avaient pas commis de faute ni dans l'éducation, ni dans la surveillance de leur enfant mineur. En 1997, la Cour de cassation leur a retiré cette faculté d'exonération ; leur responsabilité est devenue objective et se fonde désormais sur le risque.

La responsabilité des tuteurs découle d'une obligation de garantie. L'article 1384 alinéa 4 exige seulement que le mineur « ait commis un acte qui soit la cause directe du dommage invoqué par la victime »⁶⁹². La faute de l'enfant n'est pas une condition d'application de l'article 1384. Les tuteurs du mineur peuvent être responsables en dehors de toute faute⁶⁹³, simplement parce qu'il existe un fait dommageable dont l'enfant est l'auteur. S'agissant de la

chez qui le mineur a sa résidence légale peut être tenu de payer les dommages et intérêts pour réparer le préjudice commis par son enfant.

⁶⁹⁰ Cass. 2^{ème} civ. 19 février 1997, Bertrand.

⁶⁹¹ Le code civil répertorie deux hypothèses d'émancipation : l'article 482 énonce que « le mineur émancipé cesse d'être sous l'autorité de ses pères et mères », le mineur est également émancipé de plein droit par le mariage selon l'article 476.

⁶⁹² Cour de cassation Assemblée plénière 9 mai 1984, Fullenwarth c/ Felten, Dalloz 1984.525.

⁶⁹³ Cour de cassation 10 mai 2001 ; Cour cassation Assemblée plénière 13 décembre 2002 ; Cour de cassation 20 octobre 2005.

responsabilité d'un instituteur du fait de ses élèves, peut-on considérer qu'un mineur qui engage sa responsabilité civile pour des actes commis dans le cyberspace alors qu'il était sous la surveillance d'un enseignant engage la responsabilité de ce dernier ? Selon l'article 1384-5 il est possible que l'enseignant engage sa responsabilité du fait du mineur bien qu'il ne soit pas fait mention du cyberspace. Les hypothèses varient selon qu'il s'agit de l'enseignement privé ou public :

- Pour l'enseignement public, on a substitué la responsabilité de l'Etat à celle des enseignants. Seul l'Etat peut être assigné en responsabilité devant un tribunal administratif. Cette responsabilité exige que l'on prouve une faute de l'enseignant dans sa mission de surveillance, un dommage doit être survenu et qui implique un élève (commis ou subi par un élève).
- Pour l'enseignement privé : la responsabilité de l'enseignant peut être engagée sur le fondement des articles 1382 et 1383 pour les dommages causés par un élève ou à un élève. Il faut prouver que l'enseignant a commis une faute de surveillance ou d'enseignement.

La responsabilité d'un enseignant ne peut être engagée que si la faute de ce dernier a été la cause exclusive du dommage. Il pourra s'exonérer en prouvant la faute de la victime ou l'existence du fait d'un tiers qui dans les deux cas revêtent les caractéristiques de la force majeure.

La responsabilité civile du mineur se décompose en responsabilité contractuelle et en responsabilité délictuelle. Lorsque le mineur a manqué à ses obligations issues d'un contrat qu'il a valablement conclu dans le cyberspace et qu'il en découle un préjudice pour autrui, se sont ses tuteurs légaux qui vont se substituer à lui non plus pour respecter ses obligations, mais pour en assurer une compensation par équivalent. Pour ce qui est de la responsabilité délictuelle, si le mineur commet dans le cyberspace un délit porteur de préjudice pour autrui, il appartient à ses tuteurs légaux de s'acquitter des dommages-intérêts qui en résultent.

2. La cohabitation, condition de la légitimité de la responsabilité civile du tuteur légal du mineur.

La Cour de cassation considère qu'une responsabilité de plein droit pèse sur les père et mère dès lors qu'ils détiennent l'autorité parentale et que l'enfant cohabite avec eux⁶⁹⁴. La notion de cohabitation prime en la matière sur l'autorité parentale. Pour les parents vivant ensemble, la cohabitation avec leurs enfants n'est qu'un des éléments de leur autorité parentale qui leur octroie un droit de garde, de surveillance et d'éducation ; en contrepartie, les parents sont solidairement responsables des faits de leurs enfants. Par contre pour les parents séparés, même exerçant conjointement l'autorité parentale, le parent responsable est celui qui exerce le droit de garde au moment du dommage.

La cohabitation de l'enfant avec ses parents visée par l'article 1384 alinéa 4 résulte de la résidence habituelle de l'enfant au domicile des parents ou de l'un d'eux⁶⁹⁵.

La cohabitation n'est pas considérée comme rompue lorsque l'enfant est confié à un institut médico-éducatif⁶⁹⁶, lorsque le dommage est causé à l'école⁶⁹⁷ et même lorsque le mineur est scolarisé en internat⁶⁹⁸. La cohabitation ne cesse pas lorsque l'enfant est confié à un centre de vacances éloigné du domicile⁶⁹⁹. Les parents ne peuvent s'exonérer de leur responsabilité civile lorsque la cohabitation avec leur enfant n'a pas cessé pour une cause légitime comme une fugue de l'enfant par exemple⁷⁰⁰.

Même lorsque l'enfant est confié à un service éducatif et qu'ils ne sont plus civilement responsables, les parents doivent être convoqués devant le Tribunal saisi d'une action en responsabilité contre leur enfant, et cela en tant qu'administrateurs légaux et représentants de leur enfant⁷⁰¹ et ce conformément aux articles 375-7 et 389-2 du code civil.

⁶⁹⁴ Cour de cassation, 2^{ème} civile 19 février 1997, Bertrand.

⁶⁹⁵ Cour de cassation, 2^e chambre civile, 20 janvier 2000 <http://www.huyette.com/civ200100.htm>

⁶⁹⁶ Cour de cassation 9 mars 2000 <http://www.huyette.com/crim090300resp.htm>

⁶⁹⁷ Cour de cassation 20 avril 2000 <http://www.huyette.com/respexoparCiv200400.htm>

⁶⁹⁸ Cour de cassation 16 novembre 2000 <http://www.huyette.com/civ161100cohab.htm> ; Cour de cassation 29 mars 2001 <http://www.huyette.com/civ290301.htm> ; Arrêt du 25 septembre 2002 <http://www.huyette.com/crim250902.htm> ; Arrêt du 7 janvier 2004 <http://www.huyette.com/civ070104.htm> ; Arrêt du 18 mai 2004 <http://www.huyette.com/crim180504.htm>

⁶⁹⁹ Cour de cassation 29 octobre 2002 <http://www.huyette.com/crim291002.htm>

⁷⁰⁰ Cour de cassation 28 juin 2000 .

⁷⁰¹ Cour de cassation 18 novembre 1986 <http://www.huyette.com/respminciv181186.htm>

B. Les exceptions à l'engagement de la responsabilité civile des père et mère du mineur.

Le principe veut que les parents voient leur responsabilité civile engagée pour les préjudices commis contre autrui par leurs enfants mineurs. Mais ce principe souffre des exceptions. Il est déjà admis que le parent responsable du mineur est celui qui en a légalement la garde ; en cas de rupture (judiciairement prononcée) de la cohabitation des mineurs avec ses parents, la responsabilité civile de ces derniers ne sera pas engageable. Par ailleurs, la faute de la victime est exonératoire de la responsabilité civile des parents du mineur.

1. La rupture de la condition de cohabitation avec les parents : le placement judiciaire du mineur.

Lorsque le mineur est placé au titre de l'ordonnance du 2 février 1945 :

- Dans un établissement relevant d'une personne publique (Etat, Conseil général) : la responsabilité sans faute de l'Etat est engagée sur le fondement du risque spécial que créée pour les tiers le recours à des « méthodes libérales de rééducation »⁷⁰².
- Dans un établissement relevant d'une personne privée (association) : la responsabilité de plein droit de l'association est engagée sur le fondement de l'article 1384 du code civil⁷⁰³. La responsabilité sans faute de l'Etat pour risque spécial peut également être recherchée⁷⁰⁴.

Lorsque le mineur est placé au titre de l'assistance éducative :

- Dans un établissement relevant d'une personne publique : la responsabilité de l'administration est engagée sur le fondement de la faute prouvée⁷⁰⁵.
- Dans un établissement relevant d'une personne privée : la responsabilité de plein droit de l'association est engagée sur le fondement de l'article 1384 du code civil⁷⁰⁶.

⁷⁰² Conseil d'Etat 3 février 1956 Thouzellier, Rec., p. 49 ; AJDA 1956, II, 96, chronique Gazier.

⁷⁰³ Cass. Crim. 10 octobre 1996 Gaz. Pal. 1997 I Chr. I 4°, D. 1997, p. 309 - 26 mars 1997. voir commentaire de l'arrêt <http://www.huyette.com/commCrim260397.htm>

⁷⁰⁴ Conseil d'Etat 19 décembre 1969, Epoux Delannoy, p. 595.

⁷⁰⁵ Conseil d'Etat 11 avril 1973, Département de la Marne.

⁷⁰⁶ Cass. Crim. 10 octobre 1996 et Cass. Crim. 26 mars 1997, op. cit.

La notion de cohabitation est une notion juridique. Seul un placement judiciaire peut exonérer les père et mère de leur responsabilité de plein droit. Lorsque les mineurs résident chez un tiers sur la seule décision des parents ceux-ci restent pleinement responsables, y compris lorsque ce tiers est un organisme de vacances qui n'est pas chargé d'organiser et de contrôler à titre permanent le mode de vie de l'enfant⁷⁰⁷.

Un service éducatif privé qui accueille un mineur confié par un Juge des enfants est civilement responsable des dommages causés par ce mineur en application de l'article 1384 alinéa 4 du code civil⁷⁰⁸. Le service éducatif à qui le mineur est confié reste civilement responsable, même lorsque celui-ci habite avec ses parents ce, tant qu'aucune décision judiciaire n'a suspendu ou interrompu cette mission éducative⁷⁰⁹. La responsabilité du service gardien subsiste même lorsque le mineur, bien que confié judiciairement au service vit en permanence au domicile de ses parents⁷¹⁰. Dans un tel cas cependant, la responsabilité pour faute du parent qui héberge le mineur peut être recherchée.

2. La faute exonératoire de responsabilité de la victime.

Bien que les père et mère du mineur aient une obligation objective de répondre civilement des dommages causés à autrui par le mineur, il existe des cas de figure qui leur permettent de s'exonérer de cette responsabilité.

La faute de la victime peut exonérer le père ou la mère de leur responsabilité civile encourue de plein droit du fait des dommages causés par leur enfant habitant avec eux⁷¹¹. Il n'est pas nécessaire que la faute de la victime ait un caractère volontaire pour exonérer partiellement les parents de leur responsabilité⁷¹².

⁷⁰⁷ Cass. crim. 29 octobre. 2002, Dalloz 2003, IR, p. 41. arrêt in Responsabilité civile assemblée 2003, com. n°29.

⁷⁰⁸ Cour de cassation du 10 octobre 1996, Dalloz 1997 jurisprudence, p.309.

⁷⁰⁹ 3 arrêts du 6 juin 2002 de la Cour de cassation, Dalloz 2002, jurisprudence p. 2750.

⁷¹⁰ Cour de cassation 15 décembre 2005, n° 23, jurisprudence, article 38287, 9, p. 1924-1928..

⁷¹¹ Civ. 2eme, 16 mai 1988, Gaz. Pal. 1989, 2 sommaire. 371 ; Cour de cassation 20 octobre 2005 ; Cour de cassation 28 juin 2000.

⁷¹² Cour de cassation 29 avril 2004 ; Cour de cassation 10 novembre 2005. Cour de cassation Civ. 2, 20 octobre 2005

La force majeure ou la faute imprévisible et irrésistible de la victime peuvent exonérer totalement les parents de leur responsabilité civile⁷¹³.

Le mineur peut commettre des délits dans le cyberespace dont il doit répondre en justice. Quel est le rôle est réservé à ses tuteurs légaux lorsqu'il engage ainsi sa responsabilité pénale.

§2. La responsabilité pénale des tuteurs légaux du mineur.

En principe, sur le plan pénal, seul l'enfant peut être condamné pour les actes qu'il a lui-même commis. Son parent ou tuteur légal ne peut être reconnu coupable que si sa complicité est démontrée dans la commission de l'infraction⁷¹⁴. Le code pénal prévoit tout de même une peine d'emprisonnement pour le parent jugé négligent quant à la sécurité du mineur⁷¹⁵.

A. La responsabilité pénale pour des faits commis par le tuteur légal en complicité avec le mineur.

Les enfants sont responsables de leurs actes, pour autant, les parents peuvent être reconnus coresponsables en cas de complicité ou de recel.

1. Responsabilité selon le critère de la complicité.

Le complice est une « personne dont la participation à la commission d'une infraction ne réunit pas tous les éléments constitutifs de cette infraction, mais qui, dans des conditions déterminées légalement, provoque, incite, assiste ou aide à la préparation ou à la consommation de cette infraction par une action volontaire, au côté de l'auteur principal »⁷¹⁶. Pour qu'un parent puisse être reconnu coupable d'une infraction commise par le mineur, il faudrait que soit démontrée sa complicité dans l'infraction commise par le mineur.

La complicité suppose donc une volonté de participer à la commission de l'infraction par l'auteur principal, avant, pendant ou après la commission de ladite infraction. La complicité

⁷¹³ Cour de cassation 12 octobre 2000 ; Cour de cassation 18 mai 2000 ;

⁷¹⁴ Céline Halpern, Droit et Internet, Guide juridique et pratique, Editions de Vecchi 2003, page 53.

⁷¹⁵ Article 227-17 du code pénal, punit de deux ans de prison et de 30 000 € d'amende le fait pour le père ou la mère de se soustraire à ses obligations légales, notamment d'éducation et de surveillance, au point de compromettre la sécurité, la moralité ou l'éducation de son enfant mineur.

⁷¹⁶ Dictionnaire du vocabulaire juridique, sous la direction de Rémy Cabrillac ; article 121-6 et 121-7 du code pénal.

peut s'entendre ici de plusieurs manières : il peut s'agir d'une association de malfaiteurs ou d'une complicité par une abstention coupable des parents à intervenir pour empêcher la commission d'une infraction par le mineur dans le cyberspace. La complicité du tuteur dans la commission d'un délit pénal peut être ou non volontaire. L'exemple que l'on va retenir c'est celui du téléchargement illégal. Le mineur qui fait du téléchargement illégal se rend coupable au pénal, de contrefaçon (par exemple s'il copie des morceaux téléchargés sur des CD et qu'il les revend) et encourt une peine pouvant aller jusqu'à trois ans d'emprisonnement et 300 000 € d'amende. Dans ce cas, ses tuteurs légaux ne peuvent être reconnus coupables que si ils ont été complices de cette infraction, même un mineur. Un juge pourrait estimer que les tuteurs sont complices dès lors qu'ils ont laissé, en toute connaissance de cause, l'enfant continuer à télécharger, graver et dupliquer des CD contrefaits.

1-a. La complicité par un acte volontaire des parents du mineur infracteur.

Cela signifie qu'il a eu connaissance de la commission de l'infraction, qu'il n'a pas essayé de l'empêcher ou au contraire qu'il y a contribué. Le parent peut se rendre complice des activités frauduleuses du mineur en lui fournissant du matériel pour faire prospérer l'entreprise illégale de son enfant (exemple achat de CD vierges) ou en l'encourageant (par des demandes personnelles et explicites de téléchargement illégal). La complicité peut consister à aider le mineur à optimiser le téléchargement illégal en contribuant à la recherche des meilleurs sites de téléchargements. Il peut augmenter son débit connexion Internet pour optimiser les téléchargements. Plus directement encore, le parent peut prendre part à l'entreprise de commercialisation, en procédant lui-même à la distribution rémunérée ou non des œuvres téléchargées. Les circonstances sont similaires à une association de malfaiteurs. Le tuteur peut être retenu comme complice du mineur alors qu'il n'a posé aucun acte volontaire dans la commission de l'infraction pénale.

1-b. La complicité objective des parents du mineur infracteur.

Un juge pourrait estimer que le parent est complice dès lors qu'il laisse en toute connaissance de cause, son enfant continuer à télécharger et distribuer des œuvres illégalement téléchargées⁷¹⁷.

⁷¹⁷ Céline Halpern, *Droit et Internet*, préc., p.54.

Conformément à l'article 227-17 du code pénal, il est puni de deux ans d'emprisonnement et de 30 000 € d'amende le fait pour le père ou la mère de se soustraire à ses obligations légales, notamment d'éducation et de surveillance, au point de compromettre la sécurité, la moralité ou l'éducation de son enfant mineur. Cet article sanctionne la négligence coupable du parent à l'égard du mineur. On peut tout à fait imaginer que l'on puisse invoquer cet article, pour engager la responsabilité pour abstention ou négligence coupable du parent. Ce dernier est devant la loi, le garant de la sécurité et de la morale du mineur. Le fait que le mineur se livre devant son tuteur légal à des activités illégales sans que ce dernier ne l'en dissuade ni ne l'empêche est assimilable à de la négligence et/ou de la complicité. Le fait qu'il n'ait apporté aucune aide matérielle à son enfant dans la commission de l'infraction, ne suffit pas à le disculper du délit de complicité objective. La loi du 1er août 2006 renforce l'obligation de surveillance des parents à l'article L. 335-12 du code de la propriété intellectuelle: « Le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation des titulaires des droits prévus aux livres Ier et II, lorsqu'elle est requise, en mettant en œuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du chapitre I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique».

Ces moyens de sécurisation sont les logiciels de contrôle parental qui vous sont proposé par votre fournisseur d'accès à Internet. On vise une action du tuteur légal avant la commission de l'infraction par le mineur.

Pourrait-on imaginer que l'on retienne contre eux le seul fait qu'ils aient mis à la disposition de leur enfant mineur le matériel qui lui a permis de commettre des infractions. On entend par matériel, une connexion Internet (qui lui aura permis de télécharger illégalement des œuvres pourtant protégées par le droit d'auteur), un ordinateur doté d'un graveur (qui lui aura permis de fixer sur un support les œuvres illégalement acquises). Cette hypothèse semble avoir été confirmée par la loi pour la confiance dans l'économise. A la suite de la promulgation de la LCEN, une Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique a été conclue entre l'industrie du disque et l'association des fournisseurs d'accès (AFA) le 2 juillet 2004 en en présence de M. Nicolas Sarkozy, ministre d'Etat, ministre de l'économie, des

finances et de l'industrie, M. Renaud Donnedieu de Vabres, ministre de la culture et de la communication, et M. Patrick Devedjian, ministre délégué à l'industrie⁷¹⁸.

Cette charte s'articule en deux volets :

- Le premier volet, préventif, permet aux majors de communiquer aux fournisseurs d'accès Internet (FAI) les adresses IP des internautes soupçonnés de piratage. Les FAI informent ensuite automatiquement leurs abonnés que leurs téléchargements ont été repérés.
- Le second volet, répressif, devrait généraliser les résiliations des contrats d'accès Internet des personnes condamnées pour piratage, « *y compris en référé ou sur requête* » dans le cadre de procédures aux fins d'identification ou de résiliation/suspension de leur abonnement. Les FAI devront également généraliser les clauses de résiliation et de suspension de leurs contrats en cas de violation des droits de propriété littéraire et artistique de leurs abonnés.

Dans cette hypothèse le fournisseur d'accès Internet va fournir les coordonnées de son client (le parent) alors même que ce dernier n'est pas l'auteur des téléchargements illégaux. Cette infraction lui sera pourtant imputable puisque et toujours selon la Loi pour la confiance dans l'économie numérique, le fournisseur d'accès se réserve le droit de résilier unilatéralement l'abonnement de la personne jugée responsable des téléchargements illégaux. On retient une complicité objective de tuteur légal en l'absence de comportements fautifs de sa part dans la commission de l'infraction sauf à receler les produits de cette infraction.

2. Le recel.

Le recel est le fait de dissimuler, détenir, transmettre ou faire office d'intermédiaire afin de transmettre une chose que l'on sait provenir d'un crime ou d'un délit, ou de bénéficier sciemment du produit d'un crime ou d'un délit⁷¹⁹. Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, article 321-1 du code pénal. Et selon l'article 321-2 en cas de recel aggravé la peine d'emprisonnement passe à dix ans et 750 000 euros d'amende. Il faut tout de même noter que ces peines seront fixées en adéquation avec

⁷¹⁸ http://www.minefi.gouv.fr/presse/communiqués/charte_musique_en_ligne.pdf

⁷¹⁹ Article 321-1 et s., article 434-6 du code pénal ; Dictionnaire du vocabulaire juridique, sous la direction de Rémy, Cabrillac, préc.

les peines fixées pour l'infraction initiale. On peut donc difficilement envisager que le receleur soit puni de peines plus importantes que celle de l'auteur de l'infraction pour laquelle il a fait du recel (une particularité est à retenir en matière de condamnation pénale, le mineur ne peut écopier de plus de la moitié de la peine encourue par un majeur ; la peine du majeur complice sera alignée sur la peine initialement prévue pour l'infraction ou sur la peine prononcée contre le mineur ?).

On peut retenir la qualification de receleur pour le parent qui bénéficie directement du produit du téléchargement illégal de son enfant. Il est receleur quand il détient et/ou vend les produits les produits du téléchargement illégal (CD gravés) en connaissance de cause. Il y a recel par la détention de la chose provenant d'un crime ou d'un délit et recel par le profit d'un crime ou d'un délit. Le tuteur engage sa responsabilité lorsqu'il s'est abstenu d'un acte qui aurait pu garantir la non commission d'une infraction par ou contre le mineur.

B. La responsabilité pour abstention du tuteur légal.

Au regard des risques encourus par le mineur lors de sa navigation, la responsabilité parentale a été étendue pour assurer une protection optimale au mineur. Les parents sont mis à contribution ; on attend d'eux qu'ils s'engagent physiquement et matériellement dans la protection du mineur dans le cyberspace.

1. La négligence préjudiciable au mineur.

Le code civil comme le code pénal régissent l'obligation parentale de protection et de surveillance envers le mineur. Le code civil en son article 371-1 met à la charge des parents la responsabilité de « *protéger l'enfant dans sa sécurité, sa santé et sa moralité* ». Cette disposition du code civil ne paraît pas devoir s'appliquer dans le cas des parents négligeant de surveiller par exemple, la navigation de leur enfant sur Internet, l'élément d'intentionnalité ne pouvant être démontré. L'article 227-17 du code pénal dispose que « *le fait par le père ou la mère légitime, naturel ou adoptif, de se soustraire, sans motif légitime, à ses obligations légales au point de compromettre la santé, la sécurité, la moralité ou l'éducation de son enfant mineur est puni de 2 ans d'emprisonnement et de 30.000 € d'amendes* ». Cet article

s'applique également lorsque la jeune victime a été exposée au spectacle de la luxure d'autrui⁷²⁰.

La responsabilité pénale des parents ou tuteurs légaux du mineur peut aisément être engagée du fait de leur négligence envers ce dernier. Cette négligence peut être assimilée à de la maltraitance. Le droit commun s'appliquant à Internet ; cette application pourrait nécessiter des adaptations propres à la spécificité de la matière. Quelles sont la nature et l'étendue des obligations légales des parents ou tuteurs légaux pour assurer la santé, la sécurité, la moralité et l'éducation du mineur sur Internet. *A contrario*, quels sont les comportements des tuteurs pouvant être considérés comme préjudiciables à la santé, la sécurité, la moralité et l'éducation du mineur au point d'engager leur responsabilité pénale ? Le législateur n'a pas apporté de réponse à ces interrogations. On peut aisément s'imaginer qu'il reviendra aux juges de procéder à une appréciation au cas par cas, quant ils auront à connaître de tels litiges. Par leur jurisprudence, ils pourront établir progressivement une liste non exhaustive des comportements préjudiciables à la santé, la sécurité, la moralité et l'éducation du mineur qui sont imputables à leur parent.

La non utilisation d'un filtre sur l'ordinateur familial serait-elle de nature à justifier la condamnation des parents qui laisseraient consciemment leurs enfants accéder à des contenus choquants sans restriction. Il subsiste une infraction d'abandon moral dont les termes apparaissent d'autant plus larges qu'il n'est plus nécessaire que l'abstention des parents ait nui « gravement » à la moralité ou l'éducation de leur enfant⁷²¹.

En se référant au chapitre portant sur les moyens de protection du mineur dans le cyberspace⁷²², on a pu voir un faisceau de comportements que l'on attend des parents et tuteurs légaux pour assurer la protection des mineurs contre la cybercriminalité dont ces derniers peuvent être les auteurs et/ou les victimes dans le cyberspace. La famille est remise au centre du débat, il lui est dévolu un rôle central à jouer pour éviter la démission de certains parents devant les évolutions et les compétences technologiques de leurs enfants mineurs.

⁷²⁰ CA Colmar, 6 décembre 1957, Dalloz 1958, jurisprudence p.357, note P. Bouzat.

⁷²¹ Légipresse N° 214-septembre 2004, Emmanuel Dreyer (Maître de conférences à la Faculté de droit de l'Université de Rennes 1), La responsabilité des internautes et éditeurs de sites à l'aune de la loi pour la confiance dans l'économie numérique, p.92.

⁷²² Cf. dans la 2^e Partie, Titre 1, chapitre 2.s

La responsabilité des parents ou tuteurs légaux du fait des mineurs, suppose qu'ils aient commis des actes illégaux. Ils peuvent également voir leur responsabilité engagée en l'absence de négligence ou d'abstention fautive de leur part.

2. La charge morale des parents à l'égard des enfants mineurs.

On a pu parler à plusieurs reprises de la de responsabilité morale du parent pour son enfant mineur. Cet aspect moral est transversal dans la mesure où il touche tous les aspects de la navigation du mineur dans le cyberspace. C'est un aspect important qui joue un rôle essentiel dans la sécurité et la protection du mineur sur Internet par devers lui-même. La charge morale des parents suppose qu'ils aient une capacité d'anticipation et de prévention sur tout ce qui est susceptible d'entacher la moralité du mineur. Parallèlement, le parent doit s'assurer que le mineur ne soit ni la victime ni l'auteur d'actes immoraux.

Le mineur ne doit pas être l'auteur d'actes immoraux. Le parent du mineur doit mobiliser tous les moyens personnels, physiques et techniques pour prémunir son enfant de commettre des actes illégaux dans le cyberspace. De manière générale, tout parent est censé inculquer à son enfant la notion de ce qui est légal ou non, ou plus prosaïquement la notion du bien et du mal. Le postulat de départ étant que « nul n'est censé ignorer la loi », on attend des parents qu'ils en soient conscients et qu'ils pallient les lacunes de leurs enfants mineurs. Les parents doivent faire preuve d'une bonne connaissance du cyberspace et de ses applications pour prétendre prévenir l'activité illicite de leur enfant. Cela vaut surtout pour la cybercriminalité. Dans ce cas de figure, la charge morale du parent ne peut s'exercer que de manière préventive, on imagine mal un parent livrer son enfant infracteur à la justice. Tout au plus pourrait-il appliquer des punitions à l'échelle familiale. Les enjeux sont encore plus importants lorsqu'il s'agit pour le parent de protéger son enfant contre autrui.

Le mineur ne doit pas être victime d'actes immoraux. Le parent doit dans le même esprit que précédemment mettre en œuvre tous les moyens possibles pour protéger l'intégrité physique et morale de son enfant. Pour ce faire il peut utiliser la pédagogie, sa présence physique et/ou des outils techniques. Internet est entré dans les mœurs, il est légitime qu'il soit intégré dans le processus d'éducation des enfants en milieu familial comme en milieu scolaire. Cela suppose que l'on attire leur attention sur les dangers auxquels ils pourraient être confrontés. Comme on apprend la sécurité routière à un enfant, on doit lui apprendre la sécurité de

navigation dans le cyberspace. Il ne s'agit pas pour autant d'en faire des paranoïaques. Les parents se doivent d'être présents autant que faire se peut auprès de leurs enfants dans leur navigation. Ils doivent compléter leur action par des dispositifs techniques dont il a déjà été question dans les précédents développements. L'action des parents doit être préventive, mais également répressive ; ils doivent au nom de leur charge morale viser comme objectif que les cybercriminels s'en prenant à leurs enfants mineurs soient traduits en justice et condamnés. Dans cette optique, ils doivent contribuer à la recherche et à la sanction de tous les responsables des infractions commises à l'encontre des mineurs dans le cyberspace.

Titre 2. LES RESPONSABLES DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE.

Les mineurs sont confrontés au meilleur comme au pire dans le cyberespace. La cybercriminalité connaît en même temps que le cyberespace un développement exponentiel. Les mineurs font partie d'une catégorie d'internautes cristallisant les attentions et les mesures de protection de tous les acteurs du cyberespace. La volonté prépondérante de créer un cyberespace sûr pour les mineurs a eu une grande influence dans la réglementation de la responsabilité de la cybercriminalité contre les mineurs. C'est ainsi que, peuvent être tenus responsables de cette cybercriminalité des tiers autres que les cybercriminels.

La responsabilité pour les actes commis contre les mineurs va s'articuler essentiellement sur deux axes :

- Une responsabilité indirecte ne visant pas directement les cybercriminels mais plutôt ceux qui ont leur servi de relais technique pour la commission et la diffusion de contenus illégaux dont les mineurs sont les victimes.
- Une responsabilité directe des cybercriminels dont les mineurs sont les victimes dans le cyberespace.

Chapitre 1. LA RESPONSABILITÉ DES INTERMÉDIAIRES DU FAIT DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE.

Internet est un support propice à la commission de délits et d'infractions tels que l'atteinte à la vie privée, la diffamation, les propagandes révisionnistes, la diffusion de la pornographie, les réseaux pédophiles, etc. Ce n'est pour autant pas une zone de non-droit où tout serait autorisé. Ses acteurs sont soumis à des règles de droit, donc ils peuvent engager leur responsabilité.

Entre l'auteur d'un contenu illicite et l'internaute qui en prend connaissance, il existe une série d'intermédiaires relayant ce contenu pour le mettre à disposition : ce sont les fournisseurs de contenus, les fournisseurs d'accès, les fournisseurs d'hébergement, etc.⁷²³. En matière de régulation d'Internet, une des questions importantes concerne le régime de la responsabilité des prestataires techniques c'est-à-dire les intermédiaires qui transmettent ou hébergent des informations émanant de tiers.

La question du régime de la responsabilité des prestataires techniques s'est posée dans les années quatre-vingt-dix avec des affaires concernant les mannequins Lynda Lacoste et Estelle Halliday dont des photographies non autorisées furent diffusées sur le réseau. Si l'on s'accorde le plus souvent à retenir la responsabilité de l'éditeur du contenu, la question est plus controversée pour les fournisseurs dont le rôle est de transmettre ou d'héberger des informations⁷²⁴. Il est rare que la responsabilité du prestataire technique soit recherchée pour un préjudice qu'il a causé directement lui-même⁷²⁵.

La jurisprudence française, en l'absence d'un régime clairement défini de responsabilité des intermédiaires techniques dans le cyberspace, a du apporter des éléments de réponses lors de litiges en la matière. Le premier texte à avoir marqué une avancée significative est un texte

⁷²³ Christiane Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve d'Internet*, Dalloz-Dunod, 3^e édition 2002, p.127.

⁷²⁴ Ibid.

⁷²⁵ Jacques Larrieu, *Droit d'Internet*, Paris Ellipses 2005, p.111.

américain : le « Digital Millenium Copyright Act » signé par Bill Clinton le 28 octobre 1998. Ce texte prémunit les fournisseurs contre certaines actions en contrefaçon. Il inspirera les rédacteurs de la directive européenne sur le commerce électronique du 17 juillet 2000⁷²⁶. La loi du 1^{er} août 2000 modifiant la loi du 30 septembre 1986 relative à la liberté de communication a confirmé la mise en place d'un système de limitation de la responsabilité de certains prestataires techniques. Cette loi fut vidée d'une part substantielle de ses dispositions jugées inconstitutionnelles. Il faudra attendre la loi du 21 juin 2004 dite Loi pour la confiance dans l'économie numérique pour que ce vide soit comblé.

A l'occasion de litiges ayant marqué la jurisprudence, la question du régime de responsabilité des prestataires techniques a ressurgi : il s'agit de l'affaire Estelle Halliday et de l'affaire Yahoo. Fallait-il légiférer ou laisser libre cours à l'autorégulation ?

Les prestataires techniques peuvent engager leur responsabilité pour les contenus qu'ils véhiculent. Ils peuvent aussi bien engager leur responsabilité civile que pénale. S'agissant de la responsabilité civile, on a escamoté la réflexion sur l'alternative entre responsabilité pour faute et la responsabilité sans faute⁷²⁷.

§1. Le régime de responsabilité de droit commun des intermédiaires techniques du cyberspace.

Sous le terme d'intermédiaire technique, le droit a tenté de classer tous les métiers liés à Internet se caractérisant par l'accomplissement d'une tâche technique. Le trait commun de tous ces intermédiaires est de ne pas exercer de droit de regard sur l'information qu'ils relaient⁷²⁸.

La responsabilité de l'éditeur d'un contenu fait l'objet d'un consensus. Par contre la responsabilité des intermédiaires reste une question controversée, généralement liée au débat

⁷²⁶ Directive 2000/31/CE, JOCE 17 juillet 2000, n° L 178, p. 1 et s. ; voir également Légipresse 172-IV, p. 51.

⁷²⁷ André Lucas, La responsabilité des différents intermédiaires d'Internet, Université Paris-I Panthéon-Sorbonne Ecole Doctorale de droit public et de droit fiscal sous le patronage du Sénat, du Ministre des Affaires étrangères, du Ministère de l'Education nationale, du Ministre de la Recherche et de l'Académie des Sciences Morales et Politiques. http://droit-internet-2000.univ-paris1.fr/di2000_19.htm

⁷²⁸ La responsabilité des intermédiaires techniques. <http://www.educnet.education.fr/legamedia/juriscol/fiche08.htm>

sur le contrôle des informations diffusées sur Internet⁷²⁹. C'est sur le fondement de la responsabilité de droit commun que la jurisprudence a condamné à plusieurs reprises des fournisseurs de service sur Internet⁷³⁰.

A. La détermination des intermédiaires techniques responsables dans le cyberspace.

A la différence de la loi américaine, la directive européenne et la loi française du 21 juin 2004 dite Loi pour la confiance dans l'économie numérique (LCEN) ne visent que quatre catégories d'intermédiaires techniques : les opérateurs de télécommunications, les fournisseurs d'accès, les caches et les hébergeurs. Une ligne de partage a été tracée entre ceux qui stockent l'information et ceux qui ne font que la transmettre⁷³¹. La durée de la relation rendant possible le contrôle justifierait une mise en cause plus naturelle de la responsabilité des premiers⁷³². Dans le cadre de l'étude du régime de droit commun de la responsabilité des intermédiaires techniques nous allons retenir cinq catégories d'intermédiaires : les fournisseurs de contenu, les fournisseurs d'hébergement, les fournisseurs d'accès les exploitants de forums de discussion et les fournisseurs de moteurs de recherche.

1. Les fournisseurs de contenu.

Le fournisseur de contenu est défini comme la « personne physique ou morale introduisant directement ou indirectement des informations disponibles à travers un des services Internet »⁷³³. C'est l'intermédiaire entre l'éditeur du contenu d'un site web et l'internaute qui consulte ce site⁷³⁴. Il peut s'agir d'un particulier comme d'un professionnel. L'éditeur de site peut être ou non distinct de l'auteur du contenu. La personne ayant mis une information en ligne en est « responsable au premier chef »⁷³⁵.

⁷²⁹ Valérie Sédallian, La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique. <http://www.juriscom.net/pro/1/resp19990101.htm>

⁷³⁰ Cass. Crim., 15 novembre 1990, Ulla ; Cass. Crim. 17 novembre 1992 PPX et Neron, Rapport du Conseil d'état « Internet et les réseaux numériques », La Documentation Française, 1998, p.177, également disponible sous : <http://www.internet.gouv.fr/francais/index.htm>

⁷³¹ Jacques Larrieu, Droit d'Internet, préc., p.112.

⁷³² Article 6, I, 8 loi du 21 juin 2004.

⁷³³ A. Latreille, Dictionnaire juridique des termes techniques.

⁷³⁴ Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, op.cit., p.128.

⁷³⁵ Isabelle Falque-Pierrotin, Internet. Enjeux juridiques, op.cit., p.83.

L'une des premières difficultés dans la mise en œuvre de la responsabilité des fournisseurs de contenus tient à leur anonymat ou à leur insolvabilité⁷³⁶. Pour pallier cette difficulté, la Cour d'appel de Versailles, préalablement à la législation avait enjoint à l'hébergeur de proscrire l'anonymat et la non identification⁷³⁷. Les juges ont quant à eux enjoint l'hébergeur, sur le fondement de l'article 10 du code civil⁷³⁸, de mettre à la disposition de la victime l'identité du créateur du site au contenu litigieux⁷³⁹. L'article 43-9 inséré à la loi du 30 septembre 1986 par la loi du 1^{er} août 2000 impose aussi bien aux fournisseurs d'hébergement qu'aux fournisseurs d'accès de « détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu relayé par des services dont [ils] sont prestataires »⁷⁴⁰. Ces données ne peuvent être mises à la disposition du public conformément aux articles 226-17, 226-21 et 226-22 du code pénal. Un juge doit en autoriser la communication au demandeur⁷⁴¹. Par ailleurs l'article 43-10 de la loi du 30 septembre 1986, oblige l'éditeur de site à tenir à la disposition du public ses nom, prénom ou domicile ; dans le cas d'une personne morale : sa dénomination et sa raison sociale ainsi que son siège social, le nom du directeur, du codirecteur de la publication ou du responsable de la rédaction ainsi que les coordonnées de son hébergeur.

2. Les fournisseurs d'hébergement.

Ils sont définis⁷⁴² comme « les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles » par les services de communication autres que des correspondances privées. Ils sont également définis comme étant des prestataires de services assurant le lien entre les fournisseurs de services et les internautes. Ce sont des intermédiaires techniques qui n'ont pas à se soucier du contenu de

⁷³⁶ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.281.

⁷³⁷ CA Versailles, 12^e ch., 8 juin 2000 : JCP E 2000, p.1858, obs. N. Mallet-Poujol et M. Vivant ; Comm. com. électr. Juillet-août 2000, commentaire. n° 81, obs. J.C. Galloux ; Légipresse, sept. 2000, p.139, note C. Rojinsky.

⁷³⁸ « Chacun est tenu d'apporter son concours à la justice en vue de la manifestation de la vérité ».

⁷³⁹ Tribunal commercial. Paris, réf., 29 juin 2000 : Comm. com. électr. Sept. 2000, commentaire. n° 91, obs. J.C. Galloux.

⁷⁴⁰ TGI Paris 6 février 2001 : Comm. com. électr. Mai 2001, commentaire. n° 50, obs. Ch. Le Stanc.

⁷⁴¹ Loi du 30 septembre 1986, article 43-9 al. 2 ; TGI Paris 6 février 2001 : Comm. com. électr. Mai 2001, commentaire. n° 50, obs. Ch. Le Stanc. – TGI Paris 20 septembre 2000 : Comm. com. électr. Déc. 2000, commentaire. n° 131, obs. J.C. Galloux.

⁷⁴² Article 43-8 de la loi du 30 septembre 1986, issu de la loi du 1^{er} août 2000.

l'information mais de son formatage en vue de sa diffusion. Ils ne doivent pas être considérés comme auteur principal de l'infraction⁷⁴³.

Ils sont souvent mis en première ligne dans les procès et se sont retrouvés au cœur d'une controverse sur la portée qu'il convenait de donner à leur responsabilité⁷⁴⁴.

Les fonctions d'hébergeur et de fournisseur d'accès peuvent être cumulées ou séparées. Elles peuvent s'assimiler à celle d'imprimeur dans le domaine de la presse écrite.

3. Les fournisseurs d'accès.

A la lecture de l'article 43-7 de la loi du 30 septembre 1986, ce sont les personnes physiques ou morales « dont l'activité est d'offrir un accès à des services de communication en ligne autre que de la correspondance privée ». Leur rôle est important mais purement technique. L'article 12 de la directive commerce électronique du 8 juin 2000 exclut en principe leur responsabilité, à condition qu'ils ne soient pas à l'origine de la transmission, qu'ils ne sélectionnent pas le destinataire de celle-ci et qu'ils ne sélectionnent ni ne modifient les informations faisant l'objet de la transmission. La loi du 21 juin 2004 les définit comme « les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne »⁷⁴⁵.

Comme l'hébergeur, ils sont tenus de conserver les données de nature à permettre l'identification du fournisseur de contenu⁷⁴⁶. Ils sont également tenus d'informer leurs abonnés « de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner ; d'autre part de leur proposer au moins un de ces moyens⁷⁴⁷ ».

4. Les exploitants de forums de discussion et les fournisseurs de moteurs de recherche.

Les exploitants des forums de discussion sont comme leur nom l'indique, chargés de la gestion des systèmes de messageries instantanées et autres types de newsgroup.

⁷⁴³ Céline Halpern, Droit et Internet, préc., p.11.

⁷⁴⁴ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p. 282.

⁷⁴⁵ Article, 6, I, 1 LCEN.

⁷⁴⁶ Article 43-9 de la loi du 30 septembre 1986, issu de la loi du 1^{er} août 2000.

⁷⁴⁷ Article 43-7 de la loi du 30 septembre 1986, issu de la loi du 1^{er} août 2000.

Les fournisseurs de moteurs de recherche sont quant à eux, les personnes qui mettent à disposition un « logiciel d'exploration appelé "robot", qui visite en continu les pages web et les indexe de manière automatique dans une base de données, en fonction des mots-clés qu'ils contiennent »⁷⁴⁸.

Ces deux groupes d'intermédiaires ont en commun de ne pas avoir de régime de responsabilité spécifique. On a pu noter parfois une assimilation discutable de l'exploitant d'un forum de discussion à un hébergeur⁷⁴⁹. La loi du 1^{er} août 2000 n'a envisagé ni le cas particulier de l'exploitant du forum de discussion, ni celui du fournisseur de moteurs de recherche. La directive du 8 juin 2000 et la Loi pour la confiance dans l'économie numérique n'ont pas précisé leur régime de responsabilité.

Les forums de discussions du fait du caractère instantané des messages peuvent connaître des dérapages difficiles à contenir en temps réel malgré la présence d'un modérateur. Les forums de discussion s'attachent à afficher une charte de participation, à mettre en place une modération et gérer les litiges qui peuvent survenir. En cas de délits dans un forum de discussion, engage sa responsabilité :

- l'auteur direct du message incriminé (il est parfois difficile à identifier⁷⁵⁰) ou toute personne ayant effectivement participé à la création dudit contenu,
- le modérateur qui en modifiant la teneur d'un message lui a conféré un caractère illicite ou préjudiciable qu'il ne présentait pas originellement (ce cas de figure se présente surtout dans la modération *a priori* : le modérateur intervient avant que le message ne soit publié pour le modifier si nécessaire)⁷⁵¹.

La question de la responsabilité de l'exploitant du forum de discussion n'a pas été traitée par le législateur avant 2004. Le sujet n'était que de peu d'intérêt pour la doctrine ; des décisions des juges du fond ont tenté de répondre à cette question⁷⁵² en assimilant l'exploitant de forum

⁷⁴⁸ Th. Verbiest et Etienne Wéry, La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés : Légipresse, mai 2001, II-49.

⁷⁴⁹ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p. 291.

⁷⁵⁰ TGI Paris, 17^e ch., 26 mars 2002 : Comm. com. électr. Mai 2002, commentaire. n°78, obs. A. Lepage.

⁷⁵¹ Le Forum des droits sur Internet, Rapport d'activité 2003, La documentation française, Michel Elie (Observatoire des usages d'Internet) « Quelle responsabilité pour les organisateurs de forums de discussion sur le web ? Recommandation adoptée le 8 juillet 2003, p.262 ; - Dossier du forum des droits sur Internet, 18 juillet 2002, « Les responsabilités liées à l'activité des forums de discussion, Légipresse n°194, septembre 2002 IV 75, Foruminternet.org, <http://www.foruminternet.org/publication/lire.phtml?id=358>

⁷⁵² TGI Paris, réf., 18 février 2002 : Comm. com. électr. Juillet.-août 2002, commentaire. n°102, obs. L. Grynbaum. – Tribunal correctionnel Rennes, 27 mai 2002. – TGI Lyon, 28 mai 2002 : Comm. com. électr.

à un hébergeur. Ainsi envisagé, il se voit appliquer le régime favorable de responsabilité prévu à l'article 43-8 de la loi du 30 septembre 1986, issu de la loi du 1^{er} août 2000⁷⁵³.

La question de la responsabilité des fournisseurs de moteurs de recherche dans le cas de référencement de contenus jugés illicites. Une décision du Tribunal de grande instance de Paris en date du 4 janvier 2002⁷⁵⁴ s'est montrée particulièrement sévère à l'égard d'une société d'édition dont une publication avait méconnu les droits de la personnalité d'une célébrité. Bien qu'ayant supprimé les contenus incriminés suite à une condamnation, ces informations continuaient d'être accessibles grâce à un important moteur de recherche. La société a été condamnée sur le fondement des articles 9 et 1383 du code civil à payer un euro symbolique à la victime de l'atteinte. Les juges ont estimé que la société avait fait preuve d'une « négligence certaine », en ne jugeant pas « utile de s'assurer qu'un important moteur de recherche ne permettait pas aux internautes de continuer à y avoir accès ». Cette solution a consacré la responsabilité du fait d'autrui. Le flou persiste cependant ; la vigilance réclamée de l'éditeur ne vaut-elle qu'à l'égard des « importants » moteurs de recherche, et si tel est le cas, selon quels critères les distingue-t-on de ceux qui ne le sont pas⁷⁵⁵ ?

B. La nature de la responsabilité des intermédiaires techniques.

Conformément au droit commun de la responsabilité, les intermédiaires sont amenés à répondre de leur responsabilité civile ou pénale pour les actes qui leurs sont directement ou indirectement imputables.

1. La responsabilité civile des intermédiaires techniques.

Avant l'entrée en vigueur de la loi du 1^{er} août 2000, la responsabilité de l'hébergeur était recherchée sur le terrain du droit de la communication. Pour ce faire, il était assimilé à un producteur au sens de la loi du 29 juillet 1982 sur la communication audiovisuelle. Ce fondement n'a pas été retenu dans la durée⁷⁵⁶. A défaut de régime légal spécifique, la responsabilité des intermédiaires techniques (dont les hébergeurs) a été recherchée sur le

Décembre 2002, obs. A. Lepage. – TGI Toulouse, réf., 5 juin 2002 : Comm. com. électr. Septembre 2002, obs. L. Grynbaum.

⁷⁵³ TGI Paris, réf., 18 février 2002, préc.

⁷⁵⁴ TGI Paris, réf., 4 janvier 2002 : Comm. com. électr. Juin 2002, commentaire., n°93, obs. A. Lepage ; Légipresse 2002, n°190, III-63, note C. Rojinsky ; D. 2002, sommaire., p.2299, obs. C. Caron.

⁷⁵⁵ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.280.

⁷⁵⁶ TGI Puteaux, 28 septembre 1999, Axa/Infonie, www.legalis.net; Cass. Crim. 8 décembre 1998, Expertises juillet 1999, p.234.

fondement de la responsabilité civile de droit commun. La responsabilité civile des intermédiaires peut être engagée sur le fondement d'un acte ou d'un manquement fautif qui leur serait imputable, ou encore pour les actes fautifs d'autrui.

1-a. La responsabilité sans faute.

La responsabilité sans faute des intermédiaires techniques peut être engagée à l'encontre des intermédiaires alors même qu'il ne peut leur être imputé aucun acte fautif. L'arrière-pensée est de permettre aux usagers d'Internet s'estimant lésés ou victimes de comportements répréhensibles de toujours pouvoir avoir un responsable vers qui se tourner. La responsabilité de l'hébergeur peut être engagée en l'absence de faute avérée de sa part. Le responsable à titre principal reste l'auteur du contenu incriminé. Ce n'est qu'à titre subsidiaire ou en raison de son refus de communiquer l'identité de l'auteur que le fournisseur d'hébergement peut être sanctionné comme ce fut le cas dans l'affaire Estelle Halliday⁷⁵⁷.

La loi du 1^{er} août 2000 et la Loi pour la confiance dans l'économie numérique prévoient que le fournisseur d'accès comme l'hébergeur ne sont pas soumis à une obligation générale de surveillance. Selon une jurisprudence de 2000 dite affaire Front 14⁷⁵⁸, les juges s'en sont tenus à une conception minimale de la responsabilité du fournisseur d'accès. Dans une autre affaire où il était demandé à des fournisseurs d'accès de procéder au filtrage de sites racistes hébergés aux Etats-Unis, le juge des référés⁷⁵⁹ a rappelé qu' « en l'état actuel de notre droit positif, les fournisseurs d'accès n'ont (...) aucune autre obligation que celle de fournir à leurs clients des outils de filtrage ». Ce faisant, le juge leur a laissé « le soin de déterminer librement les mesures qui leur apparaîtront nécessaires et possibles en l'état des moyens techniques existants, dans le prolongement de [son] constat du caractère illicite du site portail Front 14 »⁷⁶⁰. Dans cette affaire, un site hébergé aux Etats-Unis regorgeait d'injures et de propos racistes. Des associations antiracistes ont saisi la justice française. Au regard de la non coopération de la société américaine d'hébergement, elles ont assigné les fournisseurs d'accès

⁷⁵⁷ CA Paris 14^e ch. A 10 février 1999, Estelle Halliday / Valentin Lacambre, décision et commentaires sous : http://www.legalis.net/jnet/internet_illicites.htm voir également Gazette du Palais, 5-6 avril 2000, jur., p.19, not Christophe Caron ; JCP éd G, 1999, II, 10-101, note Eric Babry et Frédéric Olivier ; voir encore Légipresse n° 160, III, p.52 ; voir aussi Dalloz 1999, jur.p. 389, note Mallet-Pujol ; Communication Commerce Electronique 1999, commentaire., n°134, obs., R. Desgorces.

⁷⁵⁸ TGI Paris Réf., 22 mai 2000 : Comm. com. électr. septembre 2000, commentaire. n°92, obs. J.-C. Galloux, mettant une obligation à la charge du fournisseur d'accès, tenu d'informer les internautes des risques juridiques découlant de la consultation d'un site vendant des objets nazis.

⁷⁵⁹ TGI Paris, réf., 30 octobre 2001 : Comm. com. électr. janvier 2002, commentaire. n°8, obs. Ch. Le Stanc.

⁷⁶⁰ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.290.

Internet nationaux qui donnaient accès à ce site illicite⁷⁶¹. Le juge fut forcé de constater qu'aucune disposition légale ne permettait d'imposer d'obligation aux fournisseurs d'accès. Il n'a pu en l'espèce que faire appel à leur sens éthique⁷⁶².

Les hébergeurs ont souvent tenté de s'exonérer de leur responsabilité quant au contenu des sites qu'ils hébergent par des contrats qu'ils ont eux-mêmes établis, en utilisant diverses clauses.

- **Des clauses de bon comportement.** Ce sont des clauses qui sont imposées au client à titre préventif. Elles font écho à l'exigence de la justice exprimée dès l'affaire Estelle Halliday. Exigence selon laquelle *« il apparaît nécessaire de préciser que le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le web et au respect par eux des lois et des règlements et des droits des tiers... »*.
- **Des clauses de non-responsabilité à l'égard des tiers :** *« En aucun cas X ne saurait voir sa responsabilité engagée à la suite de toute action ou recours de tiers, notamment du fait : d'informations, d'images, de sons, de textes, de vidéos contraires aux législations et réglementations en vigueur, contenus et/ou diffusés sur le ou les sites du client ; de la violation des droits de propriété intellectuelle relatifs aux œuvres diffusées, en intégralité ou partiellement, sur le ou les sites du client sans accord exprès de leur auteur... »*. Cette précaution ne vaut qu'entre les parties contractantes⁷⁶³. Par le contrat, l'hébergeur entend limiter les hypothèses d'engagement de sa responsabilité. Ce type de contrat confère parfois un pouvoir de contrôle du contenu du site à l'hébergeur, ce faisant il lui octroie un véritable pouvoir de police qui pourrait être de nature à créer à la défaveur des tiers une solidarité avec le titulaire du site⁷⁶⁴.

⁷⁶¹ Jacques Larrieu, Droit et Internet, préc., p.115.

⁷⁶² *« Attendu qu'en l'état de notre droit positif, les fournisseurs d'accès n'ont, en effet aucune obligation que celle de fournir à leurs clients des outils de filtrage, ils n'ont pas pour autant une obligation de fournir un accès à Internet ... qu'il leur sera donc laissé le soin de déterminer « librement » les mesures leur apparaissant nécessaires et possibles dans le prolongement du constat que nous venons de faire quant au caractère illicite du site Front 14. »*

⁷⁶³ J. Larrieu, Droit et Internet, préc., p.116.

⁷⁶⁴ Ibid.

1-b. La responsabilité pour faute.

Après l'abandon du système de responsabilité de l'hébergeur notamment à l'aune du droit de la communication, la jurisprudence s'est basée sur le principe de la faute personnelle de l'hébergeur pour ramener l'établissement de la responsabilité civile au droit commun⁷⁶⁵. Au civil dans une logique de responsabilité pour faute, ne doit pas pouvoir voir sa responsabilité engagée, celui qui ne pouvait agir ou qui était dans une situation où s'abstenir était légitime⁷⁶⁶.

L'hébergeur ne verra sa responsabilité engagée qu'à une triple condition :

- qu'il ait eu la faculté technique d'intervenir ;
- qu'il ait eu connaissance du site critiquable ;
- qu'il ait choisi de ne rien faire.

Cette triple condition pour l'engagement de la responsabilité de l'hébergeur se décline également sous forme d'obligations qui leur incombent et dont le non respect peut également engager leur responsabilité.

1.b'. L'obligation d'information.

Son objet est d'informer les créateurs de sites sur le respect dont ils doivent faire preuve à l'égard des droits des tiers (droits de la personnalité, droits d'auteur, droits sur les marques, droits de l'enfance, etc.)⁷⁶⁷. Il s'agit d'une obligation d'information sur le droit, dont l'exécution a lieu au moment de la conclusion du contrat. Le client se voit soumettre des documents contractuels dont une « charte de comportement »⁷⁶⁸, dans laquelle le fournisseur d'accès doit rappeler que « la liberté d'expression sur Internet a pour limite l'obligation de respecter les droits des tiers »⁷⁶⁹.

⁷⁶⁵ Versailles, 16 mai 2002, UEJF/Multimania, www.legalis.net; TGI Nanterre référé, 31 janvier 2000, Les 3 Suisses, D. 2001, 292 et TGI Paris, 23 mai 2001, PBME (qui écarte la responsabilité du fait des choses), www.juriscom.net.

⁷⁶⁶ Responsabilité des hébergeurs : http://www.murielle-cahen.com/p_hebergeurs3.asp

⁷⁶⁷ TGI Paris, réf. 9 juin 1998 : Dalloz affaires, p.1702, note F.-D. Golstein ; JCP E 1999, p.953, obs. M. Vivant et Ch. Le Stanc.

⁷⁶⁸ TGI Nanterre, 1^{ère} ch., 8 décembre 1999 : D. 2000, sommaire. p.274, obs. C. Caron ; Comm. com. électr. Mars 2000, commentaire. n°40, obs. A. Lepage ; JCP G 2000, I, 10279, note F. Olivier et E. Barbry. – CA Versailles 12^e ch., 8 juin 2000.

⁷⁶⁹ TGI Nanterre, réf., 31 janvier 2000, en annexe de l'article de G. Haas et O. de Tissot, L'activité du fournisseur d'hébergement à l'épreuve des droits des tiers : Comm. com. électr. Juillet – août 2000, chronique. P.16.

1.b". L'obligation de vigilance.

Cette obligation est à l'origine de nombreux débats sur la responsabilité des hébergeurs. La jurisprudence a établi que les hébergeurs devaient contrôler le contenu des sites qu'ils accueillent, cependant la sévérité varie au gré des décisions. Dans un arrêt du TGI de Nanterre du 8 décembre 1999, le comportement de l'hébergeur avait été jugé avec une extrême rigueur, qui fut tempéré par un arrêt de la Cour d'appel de Versailles du 8 juin 2000. Cet arrêt considérait que l'hébergeur est tenu « à une obligation de vigilance et de prudence quant au contenu des sites qu'il accueille (...) qui s'analyse en une obligation de moyens portant sur les précautions à prendre et les contrôles à mettre en œuvre pour prévenir ou faire cesser le stockage et la fourniture » des contenus illicites. L'hébergeur n'est pas tenu de surveiller en temps réel l'ensemble des sites qu'il accueille.

1.b'''. L'obligation de réaction.

Cette obligation prend naissance par l'injonction de l'autorité judiciaire, ou bien lorsque l'hébergeur a eu connaissance du caractère illicite soit par l'information d'un tiers, soit grâce à ses investigations propres. Le fournisseur d'hébergement n'est tenu de fermer le site incriminé qu'en cas de persistance de la situation illicite⁷⁷⁰. Le spectre de la censure a été brandi en raison du fait que la fermeture d'un site par un hébergeur puisse se faire sans intervention préalable du juge. Quel que soit le choix de l'hébergeur, interdire ou laisser libre l'accès au site, sa responsabilité pourra être recherchée si l'appréciation qu'il a faite de la licéité du contenu apparaît erronée.

Quand bien même sa responsabilité pourrait être engagée sur la base de ce trinôme, encore faudrait-il apprécier si son comportement a été ou non répréhensible.

Dans l'affaire Estelle Halliday⁷⁷¹ la Cour d'appel de Paris a tranché dans le sens de la responsabilisation des fournisseurs d'hébergement⁷⁷². L'arrêt a souligné que l'hébergement est une activité qui dépasse la simple transmission de données, puisque finalement il participe à la diffusion du contenu. Les juges ont considéré que l'hébergeur devait « assumer à l'égard des tiers aux droits desquels il serait porté atteinte (...), les conséquences d'une activité qu'il a

⁷⁷⁰ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.285.

⁷⁷¹ Cour d'appel de Paris du 10 février 1999 Estelle Halliday contre Valentin Lacambre.

⁷⁷² L'ordonnance de référé avait précisé que « le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité de celui qu'il héberge, au respect par eux des lois et règlements et des droits des tiers... Il a comme tout utilisateur de réseau, la possibilité d'aller vérifier le contenu du site qu'il héberge et en conséquence de prendre le cas échéant les mesures de nature à faire cesser le trouble qui aurait été causé à un tiers »

de propos délibéré, entrepris d'exercer ». Il s'agissait à l'évidence d'une responsabilité s'inspirant de la théorie du risque ; en raison de son émancipation à l'égard de la faute, cette théorie ne laissait nulle échappatoire à la responsabilité d'un hébergeur⁷⁷³. Si l'hébergement se fait comme en l'espèce, de manière anonyme, l'auteur de site n'étant pas identifiable, il paraît logique de se retourner contre celui qui le relaie. On n'est pas tout à fait dans l'hypothèse d'une responsabilité pour faute mais plutôt selon la théorie du risque.

Pour s'exonérer de sa responsabilité, le fournisseur d'hébergement devra justifier du respect des obligations mises à sa charge, quant à l'information de l'hébergé sur l'obligation de respecter les droits de la personnalité, le droit d'auteur. Il devra justifier de la réalité des vérifications qu'il aura opérées au besoin par des sondages ; des diligences qu'il aura accomplies ; des révélations d'une atteinte aux droits des tiers et des mesures pour faire cesser cette atteinte. C'est le trinôme : devoir – savoir - inertie. L'hébergeur commet une faute par omission s'il ne vérifie pas les contenus des sites.

Dans une affaire du 8 décembre 1999 trois fournisseurs d'hébergement ont été condamnés pour avoir abrité des photographies d'un ancien mannequin Lynda Lacoste. A cette occasion, le tribunal a rappelé que contrairement aux fournisseurs d'accès *« dont le rôle se limite à assurer le transfert des données dans l'instantanéité et sans possibilité de contrôler le contenu de ce qui transite par son service, le fournisseur d'hébergement effectue une prestation durable de stockage d'informations que la domiciliation sur son serveur rend disponibles et accessibles aux personnes désireuses de les consulter [et a] la capacité d'y accéder et d'en vérifier la teneur »* Il a une obligation générale de prudence et de diligence, et il lui appartient de prendre les précautions nécessaires pour éviter de léser le droit des tiers.

Le tribunal de grande instance de Nanterre a débouté le 24 mai 2000 l'Union des Etudiants Juifs de France (UEFJ) qui demandait la condamnation du portail Internet Multimania pour avoir hébergé un site nazi contenant des textes racistes. Il a estimé que Multimania avait satisfait aux obligations définies par la jurisprudence Lacoste. En outre dans un arrêt du 12 juin 2000 la Cour de Versailles a infirmé le jugement du tribunal de Nanterre dans l'affaire Lacoste. La cour a jugé que la société Multimania avait fait les diligences nécessaires :

⁷⁷³ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.283.

- en présentant dans sa page d'accueil-abonnement comme dans la charte qu'elle soumet à l'acceptation de son client lors de la conclusion du contrat, l'obligation de respecter les droits d'autrui, notamment les droits de la personnalité, tel le droit à l'image ;
- en effectuant la mise en place d'outils d'analyse statistiques des sites les plus consultés ou des transferts de fichiers volumineux ;
- en ayant, dès la prise de connaissance de l'illicéité de la diffusion des photographies de Madame Lynda Lacoste, fermé le compte Frenchcelebs et empêché la réouverture d'un site avec lesdites photographies.

Le 28 juin 2000, l'Assemblée nationale a adopté la loi sur la réforme de l'audiovisuel. Les hébergeurs de sites devraient être exonérés de responsabilité sur le contenu des sites hébergés sauf les cas où, saisis par les tribunaux, ils n'auraient pas agi rapidement pour empêcher l'accès aux contenus litigieux, ou encore lorsque saisis par un tiers estimant que le contenu hébergé est illicite ou lui est préjudiciable, ils n'auraient pas procédé aux diligences appropriées. Le préjudice reste à l'appréciation du juge et ce conformément à l'article 43-6 alinéa 2 de la loi.

Saisi de la constitutionnalité de cette loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, le Conseil constitutionnel a censuré le 27 juillet 2000⁷⁷⁴, la disposition relative à la responsabilité pénale des hébergeurs n'ayant pas procédé aux « diligences appropriées », lorsqu'ils ont été saisis par un tiers estimant un contenu illicite.

Une loi promulguée le 1^{er} août 2000, a rectifié la précédente en supprimant la disposition qui obligeait un fournisseur d'hébergement à fermer, sur requête d'un tiers un site estimé illicite. Le fournisseur d'accès est tenu par cette loi « d'agir promptement pour empêcher l'accès au contenu du site », uniquement si le juge lui en donne l'ordre⁷⁷⁵.

⁷⁷⁴ Décision n° 2000-433 DC du 27 juillet 2000

⁷⁷⁵ Art. 43-8. - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :« - si, ayant été saisis par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu ; - [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel no 2000-433 DC du 27 juillet 2000], <http://www.juriscom.net/txt/jurisfr/div/cc20000727.htm>

La loi du 1^{er} août 2000 avait laissé un vide en ne se prononçant pas expressément sur la responsabilité des fournisseurs d'accès. Il était fait le reproche aux fournisseurs d'accès de promouvoir indirectement les échanges de fichiers vidéo ou musicaux par la pratique contestée du peer to peer (P2P) et d'en tirer bénéfice.

Les juges n'ont pas attendu l'entrée en vigueur de la loi du 21 juin 2004 pour distinguer la situation du fournisseur d'accès de celle du fournisseur d'hébergement. Ils n'étaient pas très favorables à la mise en cause des fournisseurs d'accès Internet (FAI) et cela s'est ressenti dans leurs décisions⁷⁷⁶. La pression exercée par les producteurs de musique pour que les FAI collaborent davantage à la prévention et à la lutte contre le piratage des musiques sur Internet a été telle qu'une évolution du droit était inéluctable⁷⁷⁷.

2. La responsabilité pénale des intermédiaires techniques : le principe de la responsabilité en cascade.

La loi du 29 juillet 1881 a posé comme corollaire de la liberté de communication, le principe d'une présomption de responsabilité pénale du directeur de la publication, liée à l'exercice de la responsabilité éditoriale. La loi a ainsi souhaité protéger la victime en lui offrant un interlocuteur unique et identifiable, étant entendu que le nom du directeur de la publication doit être mentionné sur chaque revue et dans le cas d'Internet pour chaque site⁷⁷⁸.

La responsabilité pénale sur Internet est moins souvent invoquée que la responsabilité civile à tel point que « les hypothèses de responsabilité pénale des intermédiaires apparaissent finalement marginales par rapport aux hypothèses de responsabilité civile »⁷⁷⁹. Cela met en lumière les incertitudes régnant au sujet de l'application à Internet du système de la responsabilité en cascade à défaut de laquelle s'applique la responsabilité pénale de droit commun⁷⁸⁰. Le Conseil d'Etat a dans un rapport de 1998⁷⁸¹ conclu à l'inadéquation de la responsabilité en cascade au monde des réseaux⁷⁸² et proposé un certain nombre de solutions permettant de garantir le respect du droit sans faire porter aux intermédiaires des obligations

⁷⁷⁶ TGI Nanterre, 8 décembre 1999, L. Lacoste/Multimania, www.legalis.net ; TGI Paris réf, 1^{er} février 2002, préc.

⁷⁷⁷ Charte d'engagements pour le développement de l'offre légale de musique en ligne, 28 juillet 2004, www.culture.gouv.fr

⁷⁷⁸ La loi du 29 juillet 1881 sur la liberté de la presse. Responsabilité et procédure : http://www.ddm.gouv.fr/article.php3?id_article=597

⁷⁷⁹ A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et d'Internet, op.cit., n°703.

⁷⁸⁰ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc.

⁷⁸¹ « Internet et les réseaux numériques ». <http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm>

⁷⁸² « Clarifier les responsabilités des acteurs », <http://www.internet.gouv.fr/francais/textesref/rapce98/rap4.htm#2>

qui reviennent aux auteurs du contenu⁷⁸³. De toute évidence, les juges n'ont pas toujours suivi cette position. De fait, jusqu'à l'avènement de la loi pour la confiance dans l'économie numérique, le droit pénal commun s'est appliqué dans la recherche de la responsabilité des intermédiaires techniques dans le cyberspace.

2-a. Le régime de la responsabilité en cascade.

La responsabilité en cascade a été calquée sur la responsabilité éditoriale. Les sites web ont été assimilés à des services de communication audiovisuelle. La loi du 29 juillet 1982 qui régit la responsabilité en cascade pose en son article 93-3 que, « *Au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication audiovisuelle, le directeur de la publication sera poursuivi comme auteur principal lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public. A défaut l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal* ». Cette condition pour poursuivre le directeur de la publication comme auteur principal permet de caractériser la faute de ce dernier. L'auteur est poursuivi comme complice en cas de mise en cause du directeur de la publication (article 93-3 alinéa 3).

On peut ajouter au nombre des infractions visées par l'article 93-3, les infractions commises par voie de presse mais prévues hors de la loi de 1881 et que le législateur a soumises à ce système de détermination de responsabilités⁷⁸⁴. Il s'agit notamment des infractions qui sont visées aux articles 227-18 à 227-23 du code pénal. C'est l'article 227-28 du même code qui a étendu le champ de la responsabilité en cascade à ces articles. Il s'agit entre autre de :

- la provocation de mineurs à l'usage de stupéfiants ;
- la provocation de mineurs à la consommation habituelle et excessive de boissons alcooliques ;
- la provocation de mineurs à la mendicité ;
- la fixation, l'enregistrement ou la transmission de l'image d'un mineur présentant un caractère pornographique.

⁷⁸³ Richard Swetenham, « Le plan d'action pour une utilisation plus sûre d'Internet » article préc., p.162.

⁷⁸⁴ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet : il s'agit des infractions de droit commun prévues par le code pénal et les infractions spéciales précisées par des textes épars (Voir à ce propos D. de Bellescize, La loi du 29 juillet 1881 à l'aube de l'an 2000 in Clés pour le siècle, Université Panthéon-Assas-Paris II, Dalloz 2000, p.1413 et s., spéc., p.1424).

Dans toutes les autres hypothèses, le régime de responsabilité pénale de droit commun prévaut.

La responsabilité en cascade fait peser la responsabilité sur les différents intervenants sur le réseau : l'auteur de l'information litigieuse, le fournisseur d'hébergement, le fournisseur d'accès, l'opérateur, etc. Ce système repose sur une « présomption de surveillance » qui met à la charge du directeur de publication la responsabilité du contrôle de la ligne éditoriale du média concerné.

L'exercice de l'action publique et la procédure devant la juridiction de jugement sont régis par des règles très spécifiques et contraignantes limitant les poursuites. Lorsqu'il n'est plus envisageable de faire peser sur une personne cette obligation de surveillance, le système de responsabilité en cascade cesse⁷⁸⁵.

2-b. Les limites de la responsabilité en cascade.

Les techniques mises en œuvre sur Internet, tels les liens hypertexte, ne permettent pas une approche de la responsabilité purement éditoriale. Le directeur de la publication ne peut pas exercer de contrôle ni de surveillance sur des propos échangés sur le web⁷⁸⁶ et dans les forums pour lesquels le contenu est largement dépendant des individus qui y participent⁷⁸⁷.

L'article 43-10 de la loi du 30 septembre 1986 fait référence à l'article 93-2 relatif aux conditions de désignation d'un directeur de publication audiovisuelle. Il a été énoncé que, « la logique législative induit (...) que la désignation d'un directeur de publication ne s'explique que par la volonté de voir appliquer à la communication en ligne la responsabilité en cascade de l'article 93-3 »⁷⁸⁸. Le but est d'assurer aux victimes de l'infraction de trouver un responsable. Dans la pratique cependant, l'identification des différents acteurs de la chaîne de responsabilité est difficile. Ça l'est notamment pour un éditeur non professionnel. Comment l'intégrer dans la chaîne de responsabilité ? La diversité des applications d'Internet se concilie

⁷⁸⁵ Christiane Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve d'Internet*, préc., p.129.

⁷⁸⁶ Ibid.

⁷⁸⁷ En pratique, des modérateurs sont désignés dans les forums avec pour mission de contrôler le contenu des messages, ils ont le pouvoir de prendre la décision de ne pas diffuser les messages qu'ils estimeraient contraires à la loi ou de nature à porter atteinte aux tiers.

⁷⁸⁸ P. Auvret, *La détermination des personnes responsables (Réflexion sur l'application de la responsabilité en cascade à Internet)* : Gazette du Palais 12-14 mai 2002, p.17 et s., spéc., n°23.

mal avec un régime uniforme de responsabilité⁷⁸⁹. Ces difficultés pourraient conduire à juger le système de responsabilité en cascade inadapté à Internet⁷⁹⁰.

La jurisprudence elle-même semble être réservée sur la question. Souvent, les décisions condamnant l'auteur d'une infraction de presse sur Internet ne mentionne aucunement la responsabilité en cascade⁷⁹¹ ; d'autres décisions refusent expressément d'en faire application. Un arrêt de la chambre d'accusation de la cour d'appel de Paris en date du 12 octobre 1999 a refusé de faire application du système de responsabilité en cascade à Internet. Elle a considéré que ce système ne pouvait se voir appliquer la loi de 1881 ou de 1982. La même solution a été consacrée par le tribunal de grande instance de Paris, le 10 janvier 2000⁷⁹².

La responsabilité des prestataires de services sur Internet, fournisseurs d'accès et fournisseurs d'hébergement, repose sur une faute caractérisée en matière de responsabilité délictuelle et sur une obligation minimum de surveillance par les prestataires, de la commission de certaines infractions. La loi dite Loi pour la confiance dans l'économie numérique est venue refonder le régime de la responsabilité des intermédiaires techniques dans le cyberspace.

§2. Le régime spécifique de la responsabilité des Intermédiaires techniques dans le cyberspace : *la Loi pour la Confiance dans l'Economie Numérique (LCEN)*

La Loi pour la confiance dans l'économie numérique marque un tournant dans l'engagement de la responsabilité des intermédiaires techniques d'Internet. Il n'existait pas à l'origine de régime spécifique de responsabilité des prestataires techniques. Les décisions des juges du fond étaient rendues sur le fondement du droit commun de la responsabilité. C'est ainsi que traditionnellement on retrouvait une responsabilité avec ou sans faute du prestataire. La Loi pour la confiance dans l'économie numérique n'a pas révolutionné la matière de la responsabilité des prestataires techniques dans le fond, elle a simplement établi un régime

⁷⁸⁹ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc.

⁷⁹⁰ P. Auvret, article préc., n°25 et s. – A. Lucas, J. Devèze et J. Frayssinet, op. cit., n°702 et n°1008.- Internet et les réseaux, Rapport du Conseil d'Etat, La Documentation Française 1998, p.175 et s.

⁷⁹¹ TGI Paris, 17^e ch. 26 mars 2002 : Comm. com. électr. mai 2002, commentaire. n°78, obs. A. Lepage.

⁷⁹² CA Paris chambre d'accusation 12 octobre 1999, inédit et TGI Paris, ch. presse, 10 janvier 2000, cités par E. Pierrat, Les infractions de presse sur Internet : Légicom, 2000/1 et 2, n°21-22, p.74 et s., spéc., p.75. – Voir aussi TI Puteaux, 28 septembre 1999 : Légipresse, janvier-févr. 1999, III-19, note C. Bigot ; Comm. com. électr. Février 2000, commentaire. n°26, obs. A. Lepage.

spécifique de la responsabilité des prestataires techniques d'Internet. Les prestataires peuvent voir leur responsabilité civile ou pénale engagée si ayant eu connaissance du caractère « manifestement illicite »⁷⁹³ (selon l'interprétation donnée par le Conseil Constitutionnel) d'un contenu, ils n'ont pas procédé à sa suppression ou à sa suspension⁷⁹⁴.

La Loi pour la confiance dans l'économie numérique donne obligation à l'éditeur de contenus de mettre à la disposition du public plusieurs informations :

- le nom du directeur de la publication ;
- la dénomination ou la raison sociale, adresse et numéro de téléphone ;
- le nom du responsable de la rédaction s'il y a lieu ;
- le nom la dénomination ou raison sociale de l'hébergeur, avec son adresse et son numéro de téléphone.

L'absence de ces mentions est sanctionnée pénalement d'une peine pouvant aller jusqu'à un an d'emprisonnement et 75 000 € d'amende⁷⁹⁵.

La Loi pour la confiance dans l'économie numérique devient désormais le siège d'une responsabilité autonome. Ce choix repose sur la volonté de marquer symboliquement l'affranchissement de la réglementation d'Internet du droit commun et du droit de la communication audiovisuelle. La responsabilité des prestataires de services sur Internet (fournisseurs d'accès et fournisseurs d'hébergement), repose sur une faute caractérisée en matière de responsabilité délictuelle et sur une obligation minimum de surveillance s'agissant de la commission de certaines infractions.

Les responsables d'un site Internet peuvent voir leur responsabilité engagée sous deux formes : en leur qualité d'éditeur du site ou en leur qualité d'hébergeur au titre duquel leur responsabilité pourrait être engagée pour diffusion de contenus préjudiciables.

⁷⁹³ Cette notion recouvre des interprétations différentes. La première affaire qui a été engagée dans ce sens dès l'entrée en vigueur de la LCEN l'a été par le comité de défense de la cause arménienne. Il demandait à Wanadoo se suspendre l'accès au site du Consulat de Turquie au motif qu'y étaient publiés des propos négationnistes. Dans un jugement du 15 novembre 2004, le Tribunal de grande instance de Paris refusait de faire droit à cette demande. A ses yeux, en l'absence de criminalisation du négationnisme du génocide arménien, le contenu diffusé n'était pas illicite. En conséquence Wanadoo n'était pas tenu, en application de la LCEN de procéder à la suspension ou suppression dudit contenu. Cette décision est en appel.

⁷⁹⁴ Le Journal du Net, Benoît Tabaka, 19 juillet 2006, « LCEN : quel bilan deux ans après ? », <http://journaldunet.com/juridique/juridique06719.shtml>

⁷⁹⁵ La nouvelle LCEN et l'école. Ce que la loi sur la confiance dans l'économie numérique change pour les utilisations de l'informatique à l'école, 22 juin 2004, http://www3.ac-nancy-metz.fr/tice/imprimer.php3?id_article=427

A. La responsabilité délictuelle pour faute caractérisée.

La loi pour la confiance dans l'économie numérique de 2004 a restreint le nombre de prestataires techniques susceptibles d'engager leur responsabilité au titre des contenus qui sont édités et diffusés dans le cyberspace. Cette loi s'est focalisée sur la situation des hébergeurs et celle des fournisseurs d'accès.

1. La responsabilité des hébergeurs.

Selon la Loi pour la confiance dans l'économie numérique, les hébergeurs ne pourront être tenus pour civilement ou pénalement responsables du contenu stocké dans le cas où ils n'avaient pas connaissance de son caractère illicite. La mise en œuvre de la responsabilité de l'hébergeur repose sur un mécanisme à double niveau :

- il faut au préalable signaler au prestataire le caractère illicite du contenu et le mettre en demeure de cesser la diffusion ;
- dans l'hypothèse où ce dernier persiste dans la diffusion du contenu illicite, il sera alors possible d'établir sa faute.

L'hébergeur n'est pas astreint par la loi du 21 juin 2004 à un devoir de surveillance. Il pèse cependant sur lui une présomption simple de connaissance. Cela suppose qu'il ait reçu une notification dans les formes posées par l'article 6,I,5 qui institue une procédure de notification. Celle-ci doit être datée et contenir un certain nombre d'informations : l'identité du notifiant, l'identité du destinataire, la description et la localisation précises des faits, les motifs du retrait et la mention des dispositions légales justifiant ce retrait, la copie d'une correspondance adressée à l'auteur ou à l'éditeur des informations litigieuses demandant leur suspension ou leur modification⁷⁹⁶.

La question de l'engagement de la responsabilité des hébergeurs à l'égard des tiers en raison des contenus des sites qu'ils hébergent peut être encadrée différemment : par des clauses contractuelles, les textes, la jurisprudence, etc.

⁷⁹⁶ «Les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ». L'information de l'hébergeur doit pouvoir être assurée par tout autre moyen qui, contrairement à la notification de l'article 6,I,5 n'emportera pas présomption.

A contrario, les fournisseurs d'hébergement ne seront pas responsables si, dès le moment où ils ont eu connaissance du caractère illicite du contenu ou de faits et circonstances mettant en évidence ce caractère illicite, ils ont agi avec promptitude pour retirer ces données ou rendre l'accès à celles-ci impossible.

Le concept d'illicéité est interprété différemment selon les autorités administratives concernées. Classiquement ce contenu regroupait les contenus racistes, antisémites, négationnistes, révisionnistes ou pédopornographiques ; d'autres contenus ont été rajoutés⁷⁹⁷. La profusion d'interprétations de la notion « manifestation illicite » pose des difficultés dans l'application de la loi par les prestataires eux-mêmes. Certains hébergeurs (de blogs notamment) n'hésitent pas à recourir à la suspension d'un contenu pour des propos pouvant être jugés diffamatoires mais prescrits au moment de la demande adressée au prestataire⁷⁹⁸.

L'article 6-I-8 de la Loi pour la confiance dans l'économie numérique permettant au juge d'ordonner à un hébergeur, et le cas échéant à un fournisseur d'accès à Internet de cesser de permettre l'accès à un contenu qui serait jugé illicite a été mis en œuvre deux fois : le 13 juin 2005, le Tribunal de grande instance de Paris a ordonné à plusieurs fournisseurs d'accès de bloquer l'accès à un site révisionniste hébergé sur le territoire américain (AAARGH)⁷⁹⁹. Cette décision était justifiée par le fait que les démarches effectuées auprès des auteurs, des hébergeurs américains étaient restées lettre morte. Dans un autre secteur, la Cour d'appel de Paris a confirmé le 14 juin 2006⁸⁰⁰ deux ordonnances respectivement du 8 juillet et du 2 novembre 2005 qui ordonnaient à la demande du Pari mutuel urbain (PMU), à un site de paris sportifs hébergé au Royaume-Uni puis à Malte de faire cesser cette activité manifestation illicite sur le fondement de l'article 6-I-8 de la Loi pour la confiance dans l'économie numérique.

⁷⁹⁷ La Haute autorité de lutte contre les discriminations et pour l'égalité (HALDE) notifie aux hébergeurs que les « offres d'emploi diffusées sur Internet mentionnant un critère d'âge, en des termes dénués d'ambiguïté dont l'usage suffit à caractériser l'intention de discriminer, (...) sont constitutives du délit de discrimination prévu aux articles 225-1 et 225-2 du code pénal ».

⁷⁹⁸ Le Journal du Net, Benoît Tabaka, « LCEN : quel bilan deux ans après ? op. cit., <http://journaldunet.com/juridique/juridique06719.shtml>

⁷⁹⁹ TGI Paris, référé, 13 juin 2005, UEJF, SOS Racisme, AIPJ J'Accuse, MRAP et a. c/ OLM, Global, Planet.com, France Télécom, Free, AOL France, Tiscali, Neuf Télécom et a. <http://www.juriscom.net/jpt/visu.php?ID=717>

⁸⁰⁰ Cour d'Appel de Paris, 14^e chambre – Section A, 14 juin 2006, <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1082>

La personne qui solliciterait de manière abusive un tel retrait pourrait être sanctionnée pénalement d'un an de prison et 15 000 euros d'amende maximum. Pour constituer la faute de l'hébergeur, la personne qui sollicite le retrait des informations doit décliner précisément son identité, décrire les faits litigieux, exposer les motifs de la demande de retrait et envoyer une copie de la correspondance adressée à l'auteur ou à l'éditeur des informations litigieuses. Cette notification doit être datée. Le Conseil constitutionnel a validé ces dispositions en précisant qu'elles étaient conformes à la directive sous réserve « qu'elles 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».

2. La responsabilité des fournisseurs d'accès.

La responsabilité des fournisseurs d'accès n'est, quant à elle, pas directement régie par un texte. Elle se déduit d'une disposition applicable à tous les prestataires. Ainsi, la Loi pour la confiance dans l'économie numérique prévoit que l'autorité judiciaire peut prescrire à l'encontre d'un fournisseur d'accès ou d'un hébergeur, en référé ou sur requête, des mesures propres à prévenir un dommage ou à le faire cesser.

On en déduit que la responsabilité du fournisseur d'accès ne peut être engagée que si ce dernier ne se conforme pas à l'ordonnance rendue par le juge. Le nouveau texte indique que le fournisseur d'accès n'est pas en principe responsable du contenu sauf s'il est à l'origine de la transmission litigieuse ou lorsqu'il a sélectionné ou modifié les contenus faisant l'objet de la transmission. Par ailleurs, afin de faciliter l'identification de la source illicite ou de l'agissement répréhensible, la loi prévoit une obligation de conservation des données par les prestataires de services de communications en ligne afin de les communiquer aux autorités judiciaires à leur demande. Le défaut de conservation des données est puni d'un an d'emprisonnement et de 75 000 euros d'amende.

3. La requalification de la responsabilité de l'organisateur de forum de discussion.

Pendant quelques années on a admis que l'auteur direct ou quiconque ayant eu une incidence directe sur l'illicéité d'un message dans un forum de discussion devait engager sa responsabilité. Il y a eu des cas de figure où les juges du fond ont retenu la responsabilité des exploitants de forums en les assimilant assez sévèrement à des fournisseurs d'hébergement, étant donné qu'ils assuraient le stockage direct et permanent de messages pour mise à disposition du public⁸⁰¹.

Il est arrivé que la Cour de cassation retienne la responsabilité en tant que producteur, du président d'une association ayant pris l'initiative de créer un service télématique, en vue d'échanger des opinions sur des thèmes définis à l'avance, alors même que le message n'avait pas été fixé préalablement à sa communication au public⁸⁰². Dans un autre cas de figure, les juges ont décidé que « *le responsable d'un forum non modéré ou modéré a posteriori doit être considéré comme un hébergeur au sens de la loi puisqu'il assure le stockage direct des messages diffusés sans porter de regard préalable sur ces derniers* »⁸⁰³. Les juges ont également estimé que « *le message considéré comme diffamatoire ayant été supprimé du site par M. D., dans le 24 heures de la demande formulée par la société Groupe Mace, le prévenu [avait] ainsi agi promptement dès qu'il [avait] eu connaissance du caractère illicite du message* »⁸⁰⁴.

⁸⁰¹ TGI Paris, réf., 18 février 2002 : Comm. com. électr. Juillet.-août 2002, commentaire. n°102, obs. L. Grynbaum. – Tribunal correctionnel Rennes, 27 mai 2002. – TGI Lyon, 28 mai 2002 : Comm. com. électr. Décembre 2002, obs. A. Lepage. – TGI Toulouse, réf., 5 juin 2002 : Comm. com. électr. Septembre 2002, obs. L. Grynbaum.

⁸⁰² André Lucas (professeur à l'Université de Nantes) « La responsabilité des différents intermédiaires d'Internet », Université Paris-I Panthéon-Sorbonne Ecole doctorale de droit public et de droit fiscal, Colloque International : Internet et le Droit sous le patronage du Sénat, du Ministère des Affaires Etrangères, du Ministère de l'Education nationale, du Ministère de la Recherche et de l'Académie des Sciences Morales et Politiques, http://droit-internet-2000.univ-paris1.fr/di2000_19.htm

⁸⁰³ Tribunal de grande instance de Lyon, 14^e chambre, 21 juillet 2005 Groupe Mace c/ Monsieur Gilbert D., <http://www.foruminternet.org/texte/documents/jurisprudence/lire.phtml?id=1027>

⁸⁰⁴ Cette décision se justifie par le fait que, la loi du 21 juin 2004 a remplacé dans les articles 93-2 et 93-3 de la loi du 29 juillet 1982, les mots « communication audiovisuelle » par les mots « communication au public par voie électronique » tout en gardant l'exigence de la fixation préalable à condition de l'engagement de la responsabilité du directeur de publication. Il s'en réfère l'inapplicabilité de la loi du 29 juillet 1982 aux organisateurs de forum de discussion *a posteriori*. Ainsi la jurisprudence résultant de l'arrêt du 8 décembre 1998 selon laquelle « le producteur du service peut être poursuivi comme auteur principal, même si ce message n'a pas été fixé préalablement à sa communication au public et ce en application de l'article 93-3 de la loi du 29 juillet 1982 » est désormais obsolète.

La jurisprudence de la Cour de cassation fixée par un arrêt du 8 décembre 1998⁸⁰⁵ laissait entendre que l'exploitant d'un forum pouvait être poursuivi comme auteur principal alors même qu'aucune modification inopportune avant la communication du message au public ne lui était imputable. La règle semble être que la responsabilité d'un exploitant de forum de discussion ne peut être engagée que dans le cas où il procède à une modération *a priori* : à savoir qu'il se réserve le droit de modifier ou supprimer préalablement à leur communication au public les messages jugés délictueux. Son défaut de vigilance (dans le cas où un message délictueux parviendrait au public) et/ou sa modification préjudiciable sont ici sanctionnés. La différence entre cette jurisprudence et celles préalablement mentionnées⁸⁰⁶ réside dans le fait que c'est le type de modération (*a priori* ou *a posteriori*) qui détermine le régime de responsabilité de l'exploitant du forum. Pour une modération *a priori*, la responsabilité de l'exploitant de forum sera une responsabilité de droit commun au sens de la loi du 29 juillet 1881 sur la liberté de la presse. *A contrario* l'exploitant d'un forum modéré *a posteriori* doit être considéré comme un hébergeur au sens de la Loi pour la confiance dans l'économie numérique, puisqu'il assure le stockage direct des messages diffusés sans porter de regard préalable sur ces derniers et bénéficie de ce fait d'une responsabilité « allégée », ce qui n'a pas manqué de susciter des critiques⁸⁰⁷.

B. Une obligation minimum de surveillance pour certaines infractions.

La directive européenne énonce l'irresponsabilité pénale et civile des fournisseurs d'accès quant aux contenus accessibles par leurs services, sauf si ils sont à l'origine de la transmission, qu'ils ont sélectionné le destinataire ou dans l'hypothèse où ils ont choisi ou modifié les informations incriminées⁸⁰⁸. Cette disposition avait été laissée de côté par la loi du 1^{er} août 2000 ; la Loi pour la confiance dans l'économie numérique l'a reprise à son

⁸⁰⁵ Cass. Crim., 8 décembre 1998, Légipresse n° 161-III, p.57, « il résulte de l'article 93-3 de la loi du 29 juillet 1982 que lorsqu'une infraction prévue par le chapitre IV de la loi du 29 juillet 1881 est commise par un moyen de communication audiovisuelle, à défaut de poursuites contre l'auteur du message illicite, le producteur du service peut être poursuivi comme auteur principal, même si ce message n'a pas été fixé préalablement à sa communication au public ». Cette responsabilité de producteur appliquée à Internet rendait responsable des messages échangés en direct celui qui en a pris l'initiative et en a défini le thème du forum de discussion. La Cour d'appel de Montpellier dont l'arrêt a été cassé avait retenu que, « le producteur ne peut être que celui qui peut exercer son contrôle en cours de production ».

⁸⁰⁶ TGI Paris, réf., 18 février 2002 : Comm. com. électr. Juillet.-août 2002, commentaire. n°102, obs. L. Grynbaum. – Tribunal correctionnel Rennes, 27 mai 2002. – TGI Lyon, 28 mai 2002 : Comm. com. électr. Décembre 2002, obs. A. Lepage. – TGI Toulouse, réf., 5 juin 2002 : Comm. com. électr. Septembre 2002, obs. L. Grynbaum.

⁸⁰⁷ Dreyer, « Interrogations sur la responsabilité pénale des fournisseurs d'hébergement », Légipresse juin 2004.

⁸⁰⁸ Directive européenne du 8 juin 2000, article 12.1.

compte. Son article 9, I⁸⁰⁹ pose le principe d'une absence de responsabilité des intermédiaires (opérateurs de télécommunications, exploitants de réseaux, fournisseurs d'accès d'Internet) du fait des contenus circulant dans les réseaux, du moment qu'ils ont respecté une attitude de neutralité à l'égard de ces contenus⁸¹⁰.

Il ne s'agit pas non plus d'une irresponsabilité absolue dans la mesure où, la loi leur impose une exigence (simple) : qu'ils « informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner » et de leur proposer au moins un de ces moyens (article 6, I, 1 LCEN). Les fournisseurs d'accès ont par ailleurs l'obligation de détenir et de conserver les moyens d'identifier les usagers de leurs services en vue d'un engagement de la responsabilité de ces derniers⁸¹¹.

Cependant cette irresponsabilité ne les dispense pas d'obtempérer à une demande judiciaire de « surveillance ciblée et temporaire » (article 6, I, 7)⁸¹². Ils sont soumis aux injonctions judiciaires, notamment pour fermer l'accès à Internet à un internaute qui déploierait une activité illicite (article 12.3 de la Directive européenne ; article 6, I, 8 et II, LCEN) ou pour identifier leurs abonnés (article 6, II, alinéa 3 loi 2004)⁸¹³.

Les juges ne se sont pas montrés favorables à la mise en cause des fournisseurs d'accès Internet ce, bien avant l'entrée en vigueur de la loi du 21 juin 2004⁸¹⁴. D'aucuns pensent que la question du piratage de la musique sur Internet pourrait pousser les juges, sous le coup de la pression à inverser cette tendance au vu de la demande croissante de collaboration requise de

⁸⁰⁹ Nouvel article L. 32-3-3 du Code des postes et communications électroniques.

⁸¹⁰ Selon ce texte, la personne qui assure ce type de service « 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 ou modifie les contenus faisant l'objet de la transmission. »

⁸¹¹ Jacques Larrieu, Droit et Internet, préc., p.111.

⁸¹² Ibid. p.114.

⁸¹³ TGI Paris, réf. 1^{er} février 2002, SA SPPI/T, www.legalis.net

⁸¹⁴ TGI Nanterre, 8 décembre 1999, L. Lacoste/Multimania, www.legalis.net; TGI Paris référé, 1^{er} février 2002, préc. En l'occurrence, certaines décisions rappelaient que, aucune obligation particulière concernant la protection des tiers n'étaient imposées aux FAI par la loi du 1^{er} août 2000. C'est ainsi que dans l'affaire Front 14 les juges ont retenu que : « attendu qu'en l'état actuel de notre droit positif, les fournisseurs d'accès n'ont, en effet aucune autre obligation que celle de fournir de fournir à leurs clients des outils de filtrage...mais attendu que si ils n'ont aucune obligation personnelle de filtrage, ils n'ont pas pour autant une obligation de fournir un accès à Internet...qu'il leur sera donc laissé le soin de déterminer « librement » les mesures leur apparaissant nécessaires et possibles dans le prolongement du constat que nous venons de faire quant au caractère illicite du site Front 14 ».

la part des fournisseurs d'accès pour la prévention et la lutte contre le piratage de musique sur Internet⁸¹⁵.

1. Le devoir de vigilance pour les contenus illicites

Les fournisseurs d'accès Internet sont sollicités dans la lutte contre les contenus illicites (par nature ou du fait de leur accessibilité aux mineurs) d'un point de vue préventif et d'un point de vue répressif. Ils doivent agir en amont de la commission de ces délits en informant leur clientèle des peines qu'elle encoure en posant certains actes répréhensibles d'une part, et d'autre part en mettant à la disposition des internautes des moyens techniques de protection de leurs enfants mineurs lors de leur navigation dans le cyberspace. Si toutefois et malgré ces mesures préventives, une infraction venait à être commise, ils doivent prendre toutes les mesures nécessaires pour la faire cesser et solliciter le concours des autorités compétentes.

Dans le souci de conjurer ce sentiment d'impuissance, le législateur de la loi du 21 juin 2004 a rappelé que les fournisseurs d'accès Internet devaient concourir à la lutte contre l'apologie des crimes contre l'humanité, l'incitation à la haine raciale et la pornographie infantile. Pour ce faire, ils doivent faire connaître les moyens qu'ils consacrent à cette lutte. La loi leur fait obligation d'installer un dispositif d'alerte, « facilement accessible et visible », pour permettre aux internautes de leur signaler les comportements illicites de leurs abonnés et de rapporter promptement ces informations aux autorités publiques sous peine de sanctions pénales (article 6, I, 7)⁸¹⁶.

La loi du 21 juin 2004 en son article 6, I, 7 pose sensiblement le même principe que la directive 2000 en son article 15.1 à savoir que : les personnes assurant un service de fourniture d'accès « *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* ». Les fournisseurs d'accès ne sont tenus à aucune action positive de contrôle ou d'enquête, ni à l'obligation de filtrer préventivement les informations⁸¹⁷. La loi exige d'eux qu'ils « informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de

⁸¹⁵ J. Larrieu, Droit et Internet, préc. ; Charte d'engagement pour le développement de l'offre légale de musique en ligne, 28 juillet 2004, www.culture.gouv.fr

⁸¹⁶ Ibid., p.115.

⁸¹⁷ Ibid., p.113.

les sélectionner » et de leur proposer au moins un de ces moyens (article 6, I, 1). Dans ce but, les prestataires de services doivent mettre en place des dispositifs permettant à toute personne de porter à leur connaissance ce type de contenus, à charge pour ces prestataires de transmettre l'information aux autorités publiques. Le manquement à l'une de ces deux obligations est puni d'un an d'emprisonnement et de 75000 euros d'amende.

A la suite de la loi du 21 juin 2004, le label « Net + sûr » a été lancé le 8 février 2005 au niveau national. Ce label est apposé sur les portails de certains hébergeurs de contenu en ligne et de fournisseur d'accès. Avec ce label, les Fournisseurs d'Accès Internet (FAI), les hébergeurs, les membres de l'Association des Fournisseurs d'Accès, affichent leur volonté de lutter contre les contenus pédopornographiques ou incitants à la haine raciale. Les mesures présentées s'appuient surtout sur la bonne volonté des internautes. Il n'est pas question pour les fournisseurs d'accès Internet de faire la police.

Une charte relative à la lutte contre les contenus racistes ou pédopornographiques a été signée le 14 juin 2004 entre ces acteurs et le Ministre délégué de l'industrie. La charte prévoit plusieurs engagements dont des outils de contrôle parental, le fournisseur d'accès Internet doit proposer des informations d'accès facile destinées à mieux protéger les enfants et des formulaires pour signaler les abus⁸¹⁸.

2. Le devoir de vigilance contre le délit de téléchargement illicite.

La Loi pour la confiance dans l'économie numérique a également fait de la lutte contre la contrefaçon un axe essentiel dans ses dispositions sur la responsabilité ou la responsabilisation des intermédiaires techniques face aux activités qu'ils abritent. Cette volonté intervient en réaction au déferlement des connexions Internet haut débit et aux logiciels de téléchargement Peer to Peer (le taux d'équipement ADSL, graveurs et lecteurs MP3 est en nette augmentation), et à l'ampleur prise par le piratage. Les producteurs de musique, films, jeux, se sont engagés avec tous les moyens dont-ils disposent dans la lutte contre le téléchargement illégal. La loi est constante en la matière : on a le droit de graver un CD ou de le transformer en MP3 à la seule condition qu'il ait été acheté ou légalement téléchargé. La copie doit être à usage personnel et privé.

⁸¹⁸ Carole Gay, Faustine De Lumbée et Johanna Carvais, « Les atteintes à la dignité humaine sur Internet » (Dans le cadre des cours de M. Ferry et M. Neveu), 17 février 2005, http://www.e-juristes.org/article.php3?id_article=669

La loi Perben II du 9 mars 2004 a aggravé la répression du téléchargement illégal. L'article L335-2 du Code de la Propriété intellectuelle prévoit une peine de 3 ans d'emprisonnement et de 300.000 € d'amende. Si le piratage a été organisé en bande avec revente de compact disc (CD), la peine passe à 5 ans d'emprisonnement et 500.000 € d'amende.

Le volet de la répression du téléchargement illégal a fait l'objet de nombreux débats. L'idée a été avancée de mettre en place une « licence globale ». L'abonné Internet aurait payé une redevance à son fournisseur d'accès et aurait ainsi obtenu le feu vert pour télécharger gratuitement les œuvres de son choix. Cette solution bien que plébiscitée par les internautes n'a pas été retenue. Le Parlement avait adopté un projet de loi instaurant des amendes de 38 et 150 € pour téléchargement illégal via les réseaux peer to peer (P2P). Les pirates devaient être identifiés par leur adresse IP, et la contravention leur être signifiée. Le Conseil constitutionnel a invalidé cette disposition et on en est revenu aux anciennes sanctions.

Le législateur a préféré axer son action sur une certaine forme de prévention au téléchargement illégal. Il a pris l'initiative de réglementer la publicité commerciale des fournisseurs d'accès portant sur le téléchargement ce, quel que soit le support utilisé⁸¹⁹. Il a été fait le reproche aux fournisseurs d'accès de faire une promotion indirecte des échanges de fichiers vidéo ou musicaux par la pratique contestée du Peer to peer et d'en tirer bénéfice. La Loi pour la confiance dans l'économie numérique conformément à son article 7 énonce que, « *lorsque les personnes visées au chapitre I de l'article 6⁸²⁰ 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* ». Les intermédiaires techniques ont également l'obligation de détenir et conserver les moyens d'identification des usagers de leurs services. La loi insère un cinquième alinéa à l'article L. 332-1 du code de propriété intellectuelle prévoyant que le président du tribunal de grande instance peut par ordonnance sur requête, ordonner « *la suspension par tout moyen du contenu d'un service de*

⁸¹⁹ « Loi pour la confiance dans l'économie numérique : un nouveau cadre juridique pour Internet », Extraits du dossier du Forum des droits sur Internet coordonné par Yann Tésar et Benoît Tabaka, Légipresse n°213, juillet/août 2004, commentaire, p.68.

⁸²⁰ « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne... »

communication au public en ligne portant atteinte à l'un des droits d'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès »⁸²¹.

Le meilleur mode de responsabilisation des intermédiaires techniques quant aux contenus et comportements illicite serait une responsabilité sous le mode de l'autorégulation, surtout au niveau des offreurs ou hébergeurs de sites. Dans cet esprit, l'hébergeur s'engagerait à « moraliser » l'accueil des demandeurs si les sites et les contenus à abriter présentaient des risques d'atteinte à la dignité humaine entre autres. Mais cela ne reviendrait-il pas sur l'obligation de surveillance écartée par la Loi pour la confiance dans l'économie numérique⁸²² ?

L'alternative pourrait être la création d'une autorité de régulation supranationale qui assurerait un rôle de surveillance des sites, et d'alerte des autorités investies des pouvoirs légaux de répression (police, justice, etc.). Il existe déjà ce type d'organismes qui ont pour vocation de surveiller, de scanner le Web à la recherche de contenus illicites. Ce sont des organismes privés et qui n'ont pas vocation internationale même si par essence leur travail dépasse les frontières du fait de la nature transfrontalière d'Internet.

En définitive, toutes les mesures de préventions (techniques, pédagogiques, etc.), la responsabilisation des tuteurs légaux, les clauses contractuelles de non responsabilité des intermédiaires techniques semblent toutes viser à limiter la responsabilité des intermédiaires techniques pour les infractions dont ils ne sont pas directement les auteurs dans le cyberspace. On a donc opté pour un partage nécessaire des responsabilités entre acteurs : les pouvoirs publics, les acteurs du cyberspace, les parents, les associations et même les mineurs.

L'intensification de la lutte contre les utilisateurs de réseaux peer to peer en France se manifeste par des plaintes au pénal comme au civil contre les internautes. Le 2 février 2005, le Tribunal de Grande Instance de Pontoise a déclaré un téléchargeur coupable de contrefaçon par reproduction et diffusion d'œuvres de l'esprit en violation des droits de leurs auteurs⁸²³.

⁸²¹Forum des droits sur Internet, 15 juin 2004, « *Loi pour la confiance dans l'économie numérique : un nouveau cadre juridique pour Internet* », par Yann Tésar et Benoît Tabaka, op.cit.

⁸²² Carole Gay, Faustine De Lumbée et Johanna Carvais, « Les atteintes à la dignité humaine sur Internet », op.cit.

⁸²³ TGI de Pontoise 6ème chambre, le 2 février 2005 SACEM, SDRM, SPPF, SCPP c/ Alexis B. RLDI 2005/2, n°51 observation COSTES ; JCP édition E 2006 n°1195 paragraphe 8, observations VIVANT, Voir également le commentaire de C. Caron, Et si le droit d'auteur n'existait pas sur internet et ailleurs ?, D. 2005, Tribune p. 513. Cette

La Cour d'Appel de Versailles, par un arrêt du 16 mars 2007⁸²⁴ a confirmé le jugement rendu par le Tribunal de Grande Instance de Pontoise du 2 février 2005.

La décision du Tribunal de grande instance de Pontoise a suscité la polémique au sein d'une partie de la doctrine qui a estimé que l'exception de copie privée pourrait être vidée de tout son sens par une jurisprudence telle que celle de Pontoise qui semble appréhender de la même manière la mise à disposition et le téléchargement d'œuvres en ligne⁸²⁵.

A l'inverse, la Cour d'appel de Montpellier a confirmé un jugement controversé écartant le délit de contrefaçon par une application étendue de l'exception de copie privée, le 10 mars 2005⁸²⁶. Il s'était posé la question devant le Tribunal correctionnel de Rodez de savoir si une copie réalisée à partir d'un exemplaire contrefaisant était elle-même contrefaisante ; ou si elle pouvait dans le cas d'une utilisation strictement réservée à l'usage privé du copiste être considérée comme couverte par l'exception de copie privée. Le Tribunal a retenu l'exception de copie privée et ce faisant, étendu cette exception. A l'inverse de cette position, le Tribunal correctionnel de Blois avait sévèrement condamné le 7 décembre 2004, deux informaticiens à 2 mois de prison avec sursis et 20.000 euros de dommages et intérêts.

Dans le même temps, de nombreuses procédures civiles ont été initiées par la Société Civile des Producteurs Phonographiques (SCCP) sur requête pour obtenir soit la suspension, soit la résiliation des contrats d'accès Internet des pirates aux visas des articles 6.I.⁸²⁷ et 8 de la Loi pour la confiance dans l'économie numérique. Cependant, dans une ordonnance du 8 octobre 2004⁸²⁸, le Président du Tribunal de Grande Instance de Paris a considéré que la requête fondée sur l'article 6.I §8 ne peut être invoquée pour obtenir la résiliation d'un contrat d'accès

décision fait partie intégrante de la stratégie de « jugement pour l'exemple » qui est menée actuellement. Condamnation du « téléchargeur » particulièrement sévère : une « application modérée de la loi pénale » (3 000 euros d'amende avec sursis), mais tout de même plus de 10 000 euros de dommages et intérêts alloués aux plaignants, sans que l'on puisse déterminer l'ampleur réelle du préjudice, et alors même qu'une redevance sur les supports vierges est perçue par ailleurs (V. les obs. sous ce jugement de F. Macrez, A l'abordage des pirates, RLDI, mars 2005). Cette sanction, qui s'apparente presque à des *punitive damages*, est la manifestation d'un mouvement plus ample de constitution d'un nouvel ordre normatif plus favorable aux industries qu'aux auteurs eux-mêmes.

⁸²⁴ CA Versailles, 9^{ème} Chambre, 16 mars 2007, n°05/00658

⁸²⁵ Cyril Rojinsky et Sébastien Canevet, « Et si le droit d'auteur allait trop loin, sur internet et ailleurs ? » (toujours à propos de TGI Pontoise 2 février 2005), Recueil Dalloz n° 13, p. 849.

⁸²⁶ CA Montpellier, 10 mars 2005, Ministère Public, FNDF, SEV, Twentieth Century Fox et a. c/ Aurélien D. <http://www.juriscom.net/jpt/visu.php?ID=650>

⁸²⁷ Selon cet article, « L'autorité judiciaire peut prescrire en référé ou sur requête (à tout hébergeur ou à défaut à tout fournisseur d'accès), 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 ».

⁸²⁸ TGI de Paris, ordonnance sur requête, 3^{ème} chambre, SCCP c/ Wanadoo, 8 octobre 2004, publié par le Forum des droits sur Internet le 10 janvier 2005.

Internet. Pour ce faire il s'est attelé à définir les champs d'application respectifs des articles 6.I 8 et 8 de la LCEN dans le cadre d'une telle procédure. L'article 8 prévoit uniquement « *la suspension, par tout moyen, du contenu d'un service de communication au public en ligne portant atteinte à l'un des droits de l'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut de cesser d'en permettre l'accès (...)* ». Le Président du Tribunal a estimé que la résiliation du contrat d'accès à Internet « *ne ressort pas de la compétence du juge des requêtes ni d'ailleurs de celle du juge des référés* ». Il a toutefois rappelé que, conformément à l'article 493 du Nouveau Code de Procédure Civile, « *l'ordonnance sur requête est une décision provisoire rendue non contradictoirement dans les cas où le requérant est fondé à ne pas appeler de partie adverse* ». La Loi pour la confiance dans l'économie numérique n'a pas pour objectif de permettre la résiliation unilatérale de contrats de droit privé mais d'assurer la suspension d'un contenu illicite ou à défaut de cesser d'en permettre l'accès.

Dans la charte anti-piratage signée le 28 juillet 2004 sous l'égide de Monsieur Sarkozy alors Ministre de l'économie, est prôné le développement de l'offre légale de musique en ligne. La charte prévoit que les fournisseurs d'accès s'engagent à mener une campagne de communication auprès de leurs abonnés afin de les sensibiliser et vanter les mérites du téléchargement légal. Un message automatisé pourra être envoyé à l'internaute qui télécharge illégalement des fichiers protégés. Il est également question d'un filtrage des réseaux Peer to Peer. Ce filtrage pourrait se présenter sous forme de contrôle parental.

La loi informatique et libertés prévoit en son article 9 la possibilité pour certaines personnes morales de constituer un fichier d'infraction permettant de recenser via leur adresse IP notamment, les personnes qui se livreraient au téléchargement de fichiers illégaux. Le Conseil constitutionnel dans sa décision du 29 juillet 2004 a déclaré conforme à la Constitution cette mesure⁸²⁹.

Pour conclure, les prestataires techniques ont une obligation de célérité. Bien que n'ayant pas une obligation générale de surveillance, lorsqu'ils ont été informés que des fichiers illégaux étaient disponibles via un réseau peer to peer, ils devront agir rapidement pour éviter de voir

⁸²⁹ Il s'agit de la possibilité donnée « *aux sociétés de perception et de gestion des droits d'auteur et de droits voisins, mentionnés à l'article L. 321-1 du code de propriété intellectuelle, ainsi qu'aux organismes de défense professionnelle, mentionnée à l'article L. 331-1 du même code, de mettre en œuvre des traitements portant sur des données relatives à des infractions, condamnations ou mesures de sûreté* »

leur responsabilité engagée et d'être déclarés complices desdits téléchargements et partages illicites. Il était important de différencier leur régime de responsabilité de celui des cybercriminels, afin qu'ils n'en subissent pas la répression.

Chapitre 2. LA RÉPRESSION DE LA CRIMINALITÉ CONTRE LES MINEURS DANS LE CYBERESPACE.

La criminalité qui sévit dans le cyberespace, est communément appelée cybercriminalité. La cybercriminalité ne constitue pas dans son intégralité une criminalité propre et/ou exclusive à Internet. Il peut s'agir d'une criminalité qui, prenant naissance dans le "monde réel" (par opposition au monde virtuel) se prolonge ou se trouve aggravée, amplifiée par l'utilisation d'Internet. Il peut également s'agir d'une criminalité propre au cyberespace, qui n'est possible que par et dans le cyberespace, c'est ce qu'on l'appelle la criminalité informatique.

Pour la majorité, la cybercriminalité, est quasi automatiquement liée à la pédocriminalité qui sévit sur la Toile. Il faut admettre que le développement technologique d'Internet s'est accompagné d'une explosion de la cybercriminalité d'un point de vue global. Les mineurs sont parmi les internautes ceux qui présentent une plus grande vulnérabilité au regard de tous les contenus et comportements déviants et délictueux qu'ils sont susceptibles de rencontrer lors de leur navigation sur Internet. Les agressions dont ils sont les victimes dans le cyberespace suscitent de vives réactions. Il est donc compréhensible que ce soit l'une des matières d'Internet qui suscite le plus de réglementations.

Tous les Etats déplorent et condamnent la cybercriminalité envers les enfants d'un même élan. La difficulté réside dans le fait que, leurs traditions culturelle et juridique ne leur font pas toujours adopter des réglementations similaires ou du moins concordantes.

Le volet répressif de la cybercriminalité contre les mineurs suppose : dans un premier temps de déterminer dans ses différentes déclinaisons la criminalité dont les mineurs sont victimes dans le cyberespace, avant d'énoncer et d'analyser les moyens de répression de cette criminalité. Dans cette étude, la dimension transnationale du cyberespace sera confrontée aux choix de répressions choisies le plus souvent au cas par cas (répression nationale ou répression internationale).

§1. La cybercriminalité à l'encontre des mineurs.

Les mineurs sont sans conteste parmi les plus grands utilisateurs d'Internet⁸³⁰. Leur utilisation importante d'Internet (en termes de durée et de nombre d'utilisateurs⁸³¹) les expose aux contenus et comportements choquants et illégaux qui sévissent dans le cyberspace⁸³². La vulnérabilité qui est unanimement reconnue aux mineurs dans « la vraie vie » se prolonge dans la "vie virtuelle". Ils sont victimes sur Internet de cybercriminalité. La criminalité "réelle" ne leur est pour autant pas épargnée ; certaines formes de criminalités se prolongent dans le cyberspace ; ce faisant leurs conséquences et leur répression s'en trouvent aggravées du fait de l'utilisation d'Internet. Les mineurs peuvent être confrontés à la cybercriminalité en tant que spectateur ou en être victime.

A. L'enfant spectateur de la cybercriminalité.

La baisse du coût des communications locales rapidement supplantée par le haut débit a accéléré l'appropriation d'Internet par le mineur. La question de la protection du mineur en a logiquement découlée, mettant à contribution tous les acteurs susceptibles d'apporter une contribution positive en la matière. Pour la majorité, protéger l'enfant sur Internet c'est lutter en priorité contre les contenus pédophiles. Ce ne sont malheureusement pas les seuls périls courus par l'enfant sur Internet. Il est presque autant vulnérable en tant que spectateur de contenus même légaux mais choquants pour lui, que par le fait qu'il soit la victime d'actes innommables prenant naissance sur Internet ou prolongés par ce média. Le problème majeur est celui de l'accès aisé et souvent inopportun aux contenus sensibles et/ou préjudiciables : contenus érotiques ou pornographiques, images violentes ou racistes, etc⁸³³.

⁸³⁰ Une enquête du CREDOC (Centre de recherche pour l'étude et l'observation de conditions de vie) publiée en décembre 2004 indique que 2,4 millions de jeunes de moins de 17 ans surfent sur le net.

⁸³¹ Selon une enquête quantitative Opinion Way/Aol de mars 2002 « *Que font nos enfants sur Internet ? Ce que disent les enfants, ce que pensent les parents* », 61% des internautes de 8 à 18 ans surfent tous les jours, 76% accèdent au réseau au moins trois fois par semaine, Voir dans : « Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur Internet » publié le 11 février 2004.

⁸³² Selon une enquête menée l'IFOP pour la Délégation Interministérielle à la Famille en Mars 2005, selon les parents, 29% de leurs enfants ont été confrontés à des images à caractère sexuel dans leur utilisation d'Internet, 24% à des contenus violents et 16% à des contenus traumatisants, Source Innocence en danger.

⁸³³ Etienne Wery, Sexe en ligne : aspects juridiques et protection des mineurs, op.cit., p.49.

1. L'incitation à la haine et à la violence.

L'incitation à la haine et à la violence peut prendre plusieurs formes ; les crimes d'opinion ou l'incitation à la violence se manifestent par différents comportements des infracteurs.

1-a. Les crimes d'opinion.

Les crimes d'opinion sont ceux qui font l'apologie d'une idéologie socialement et juridiquement répréhensible.

1.a'. Le révisionnisme et l'incitation à la haine raciale.

L'incitation à la haine raciale, peut être assimilée à de l'incitation à la violence. « Tout appel à la haine nationale, raciale ou religieuse est interdit par la loi » conformément à l'article 20 § 2 du Pacte des droits civils et politiques de 1966 entré en vigueur en France en 1980. Tout message à caractère discriminatoire, diffusé en vue d'engager vivement, de pousser d'autres individus à y adhérer, ou à agir dans ce sens est caractéristique d'une incitation d'un appel à la haine.

L'auteur d'un message, sous réserve qu'il soit identifié est le premier responsable au regard du droit commun. Un internaute s'est vu condamner à dix-huit mois d'emprisonnement par le Tribunal de Grande Instance de Paris⁸³⁴ pour avoir diffusé de manière continue, des messages discriminatoires dans des forums de discussions.

Les outils de prédilection pour véhiculer cette haine sont souvent les pages personnelles, les blogs et bien sûr les forums de discussion. S'agissant des sites, ils sont plus facilement repérables, parce portant parfois dans leur intitulé une indication de ce que le contenu sera. S'agissant des blogs, ils n'ont pas toujours pour vocation première la haine raciale. Ils fonctionnent sur le même principe que des journaux intimes la différence étant dans leur accessibilité au public. Un internaute coutumier d'un discours de haine le véhiculera dans son blog.

Il existe des sites prônant la haine contre d'autres races, religions, etc., qui font la promotion, la propagande de leurs idées. Les mineurs sont susceptibles d'y être confrontés. Outre le fait qu'en droit français la haine raciale, l'incitation à la discrimination nationale, raciale ou

⁸³⁴ TGI Paris, 17^e chambre, 26 mars 2002.

religieuse soient prohibées⁸³⁵, les auteurs de ces supports haineux engagent leur responsabilité par le seul fait que leurs contenus puissent être accessibles aux mineurs.

1.a". Les dogmes nocifs à l'intégrité physiques des mineurs.

On est dans le domaine d'application de l'article 24 de la loi de 1881 pour ce qui est des apologies prohibées telle l'incitation au suicide, les atteintes volontaires à l'intégrité physique de la personne et des agressions sexuelles, toutes de nature criminelle (apologie de l'anorexie, de toute forme d'auto mutilation...), etc.

i. Incitation au suicide.

Certains messages, visent à influencer les mineurs à commettre un suicide. Internet constitue un support idéal et presque sans entrave pour ce type de pratiques. On attribue souvent cette pratique à certaines sectes⁸³⁶. Il s'agit des atteintes volontaires à sa propre vie par une incitation ou provocation au suicide (art. 223-13 à 223-15). Cette matière est régie par l'article 223-13 du code pénal lorsque l'incitation « a été suivie d'un suicide ou d'une tentative de suicide » ; les peines sont de trois ans d'emprisonnement et de 45.000 euros et sont portées à cinq ans et 75.000 euros lorsque le mineur est âgé de quinze ans. De même l'article 223-14 condamne « la propagande ou la publicité, quel qu'en soit le mode, en faveur de produits, objets ou méthodes préconisés comme moyens de se donner la mort ». La peine prévue est de trois ans d'emprisonnement et 45.000 euros d'amendes.

Un rapport récent de l'association Innocence en Danger a mis en évidence les dangers que courraient les mineurs confrontés à des sites gothiques. Certains sites gothiques ne se contentent pas de vanter un mode de vie par la promotion d'un certain type de musique et d'une mode vestimentaire ; ils font également l'apologie des scarifications, voire du suicide. Il existe une frange plus dangereuse et radicale du gothisme : les satanistes. Ils favorisent les contacts individuels et utilisent avec profit les facilités que leur offre l'anonymat des contacts sur le Web. Les mineurs peuvent y avoir accès :

⁸³⁵ Tribunal de Grande instance de Strasbourg a déclaré coupable un prévenu qui avait diffusé par la voie de forums Internet des propos de haines et de discrimination à l'égard des arabes et des immigrés, TGI de Strasbourg, 7^e ch. corr., 27 août 1999, Procureur de la République et Sté Infonie c/M. X, voir sur <http://www.juriscom.net>

⁸³⁶ C. Féral-Schuhl, Cyberdroit, préc., p.109.

- via les sigles officiels satanistes,
- via les forums de discussion ouverts sur les portails créés par les fournisseurs d'accès, au détour de certaines contributions d'internautes invitant des participants à des apartés,
- via des pseudos sites personnels d'adolescents passionnés par le vampirisme, les films d'épouvante, la science-fiction, la magie, l'occultisme, la voyance, etc.,
- via des infiltrations des satanistes sur certains webzines d'information jeunesse aux thèmes éclectiques par le biais de rubriques telles : paranormal, jeux vidéos ou jeux de rôle.

Ces sites sont d'autant plus dangereux qu'ils sont souvent en accointance avec d'autres types de cybercriminalités telles que :

- les entreprises de voyance et marchés de la magie sources potentielles d'escroquerie ;
- groupes ésotériques et sociétés secrètes, suspects de dérives sectaires ;
- industries pornographiques et marché de snuff movies, avec un accès à des sites parfois pédophiles via des sites satanistes ;
- organisations extrémistes les plus radicales⁸³⁷.

ii. L'apologie de l'anorexie.

Il a beaucoup été question de manière croissante de l'anorexie ces dernières années, par une représentation dangereuse pour les mineurs d'un idéal de minceur véhiculé notamment par les mannequins et autres personnalités célèbres. La question a rebondi lorsque, en l'espace de quelques mois des mannequins sont décédés des suites de leurs troubles alimentaires. Certains Etats dont l'Espagne ont pris l'initiative de légiférer sur la matière dans un souci de protection de la santé et de prévention de l'adhésion à de telles pratiques des mineurs⁸³⁸. Le danger est plus insidieux du fait des sites et des blogs qui pullulent et font l'apologie de la minceur extrême, n'hésitant pas à trafiquer des photos pour faire paraître les mannequins plus maigres. Internet constitue le moyen pour certains adolescents de partager leur mal-être et leurs

⁸³⁷ Mission Interministérielle de vigilance et de lutte contre les dérives sectaires, 8 septembre 2004, « Satanismes et dérives sectaires. Quels sont les risques, comment les prévenir ?

http://www.miviludes.gouv.fr/IMG/pdf/Satanisme_et_derive_sectaire-2.pdf

⁸³⁸ Espagne : lutte contre l'apologie de l'anorexie sur Internet, Source El Pais, 9 juin 2004. L'existence sur Internet d'un grand nombre de sites propageant l'idée séduisante et dangereuse que les personnes souffrant des ces graves troubles alimentaires forment une communauté partageant un véritable style de vie. L'ONG « Protégez-les » dédiée à la poursuite des crimes contre les enfants sur Internet et le Juge de la Protection des Mineurs de Madrid sont parvenus à faire fermer une trentaine de sites faisant l'apologie de l'anorexie.

troubles alimentaires en l'occurrence. Ces sites représentent un réel danger pour l'intégrité physique des mineurs. Ils se développent sous le terme générique de « pro-ana »⁸³⁹. Dans certains blogs et sites personnels, on trouve des recettes pour maigrir ou des astuces pour se faire vomir. Certaines (95% des anorexiques sont des filles) ont même créé des forums de discussion, protégés par mot de passe, où elles peuvent librement se retrouver pour exhiber leurs photos, suivre leurs progrès d'amaigrissement (avec des objectifs dangereux tels que 40 kg...), etc.⁸⁴⁰. Suite au battage médiatique sur les dangers de ces sites, la plupart ont été fermés par les hébergeurs. Il est difficile aujourd'hui de trouver un site en Français faisant l'apologie de la minceur (alors que les sites anglo-saxons restent nombreux). Une proposition de loi a même été émise par le député UMP François Vannson⁸⁴¹, afin d'interdire purement et simplement les sites qui présenteraient l'anorexie sous un jour favorable. Outre les dangers pour la santé que de tels sites présentent, ils véhiculent une certaine violence infligée à sa propre personne.

1-b. Les contenus violents ou incitants à la violence.

Il y a les contenus qui sont par nature violents par leurs représentations nocives pour le mineur et par les contenus qui incitent le mineur à commettre des actes de violence.

1.b'. Les contenus violents par nature.

Il faut entendre par contenus violents tout ce qui constitue une représentation de la violence. Ces contenus n'ont pas été strictement définis. La violence sur Internet peut se décliner sous plusieurs formes : une violence réelle relayée par des images et/ou du son et des écrits ; une violence virtuelle dans le sens de l'utilisation d'images de synthèse ou par de la fiction quelle qu'en soit le support.

Le cyberspace est l'espace informatif le plus interactif à ce jour, quiconque peut s'y informer ou y véhiculer de l'information en l'absence de contrôle ou avec une effectivité de contrôle assez limitée. Les informations sont de natures diverses de la plus anodine à la plus

⁸³⁹ Ana est le surnom pour anorexie et Mia pour boulimie.

⁸⁴⁰ Sites pro-ana : les dangers de l'anorexie sur Internet, Alain Sousa

<http://www.doctissimo.fr/html/nutrition/dossiers/anorexie/10349-pro-ana.htm>

⁸⁴¹ Interdiction des sites Internet valorisant et faisant l'apologie de l'anorexie, Travaux préparatoires Assemblée nationale 1^{ère} lecture. Proposition de loi de M. François Vannson et plusieurs de ses collègues tendant à interdire les sites valorisant et faisant l'apologie de l'anorexie, n° 3481, déposée le 30 novembre et renvoyée à la commission des affaires culturelles, familiales et sociales.

http://www.assemblee-nationale.fr/12/dossiers/interdiction_sites_anorexie.asp

innommable. Le mineur peut se retrouver confronté à des illustrations très choquantes⁸⁴² de la réalité. La prolifération des appareils numériques, a fait de toute personne en disposant un « journaliste » en puissance ; il filme et diffuse ses vidéos en ligne sans contrôle. Les contenus violents existent dans tous les médias où ils sont soumis à un encadrement visant la protection de l'enfance. Ils utilisent une signalétique indiquant à quel public leurs programmations ou leurs publications sont destinées. Internet est le seul média qui n'a pas encore adopté de signalétique qui serait affectée selon un degré de nocivité aux contenus qu'ils véhiculent. Le caractère transfrontalier et intemporel d'Internet, de même que les disparités des législations mondiales n'en permet pas en l'état actuel la possibilité.

La pratique du "happy slapping" chez les adolescents a récemment été médiatisée; cette pratique consiste dans sa forme la plus "légère" à gifler quelqu'un pendant qu'un complice filme la scène qui sera diffusée d'abord entre mobiles compatibles et dont la finalité est une diffusion à grande échelle dans le cyberspace. Dans sa forme la plus dure il peut s'agir d'agressions physiques caractérisées : passages à tabac en règle, viols, tortures, meurtres, etc. Ces images sont diffusées librement sur la Toile. Ces contenus sont facilement accessibles à tous, dont aux mineurs. Les relais sont souvent très nombreux, ce qui rend peu aisée l'identification du premier diffuseur souvent auteur ou complice de cette violence.

On a aussi beaucoup entendu parler des vidéos dites « Snuff movies»⁸⁴³ qui véhiculent pornographie et extrême violence. Ces contenus n'ont pour autre ambition que d'être diffusés au plus grand nombre. Aucune mesure n'est prévue par le premier diffuseur pour prémunir les mineurs de la confrontation à une telle violence, or dès qu'un contenu est "lâché" dans le cyberspace il est difficile de le rattraper. Les images violentes ne sont pas uniquement des images tirées de la réalité, il peut s'agir d'images fabriquées par graphisme ou par une technologie créant des images de synthèse. Les contenus violents peuvent consister en des textes, des discours haineux et/ou violents : des contenus véhiculant des idéologies très

⁸⁴² Au plus fort de la dernière guerre en Irak, les enlèvements et les assassinats d'occidentaux ont fait la Une des journaux télévisés ; ce qui a pu être censuré à l'antenne pour des raisons évidentes circulait librement sur la Toile. C'est ainsi que des millions d'internautes ont pu voir sans autres restrictions des décapitations et autres exactions contre des otages par leurs bourreaux.

⁸⁴³ Il s'agit souvent de films amateurs pornographique très violents dans la mesure où ils mettent en scènes de vraies tortures pouvant aller jusqu'au meurtre. Ne pouvant être inclus dans un réseau légal de distribution, ces productions prolifèrent « sous le manteau » et Internet est souvent un des moyens de prédilection pour en faire la promotion et/ou diffusion. Les diffusions de pornographie enfantine contiennent un certain nombre de ces contenus.

virulentes, haineuses. Il s'agit en vrac de toutes les idéologies faisant l'apologie de la haine raciale, religieuse, etc.

1.b''. Les contenus incitatifs à la violence.

Ce sont tous les contenus susceptibles d'encourager ou d'inciter le mineur à commettre des actes violents. Sans en être l'origine directe, Internet favorise et encourage la propagation de l'intolérance, de la haine, et de la violence. Des groupements prêchant la haine et la violence peuvent adresser facilement des messages de propagande et répandre anonymement l'intolérance par l'intermédiaire du spamming par exemple. Des sites, des blogs peuvent être ouverts à ces fins, des chats et forums de discussion détournés dans ce but.

i. Incitation au crime

Il s'agit de provocations de mineurs à commettre diverses actions (art. 227-18 à 227-21). On l'a vu Internet est une véritable tribune planétaire pour tous. Quiconque le souhaite a aujourd'hui la possibilité de créer son site personnel, son blog, etc. Dans ces espaces l'expression se veut libre de toute contrainte. Les internautes abordent tous les sujets qui les intéressent. Dans l'optique d'incitation à commettre des actes illicites il y a des sites qui font l'apologie de la consommation de tous types de drogues⁸⁴⁴. L'incitation à la violence contre autrui. Cette incitation peut être faite par des propos haineux contre des catégories de personnes, ou contre des personnes identifiées. Internet peut selon les personnes qui l'utilisent se révéler incitatrice au meurtre⁸⁴⁵. Il y a eu une affaire⁸⁴⁶ portée devant un tribunal américain à la suite de l'assassinat de trois lycéens abattus le 1^{er} décembre 1997 par l'un de leurs camarades de classe. Selon les plaignants, les « *sites pornographiques sadomasochistes violents du Net [...] auraient influencé [le] jugement moral de l'assassin* »⁸⁴⁷.

⁸⁴⁴ Article 227-18 (Loi n° 98-468 du 17 juin 1998) art. 16 Journal Officiel du 18 juin 1998)(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait de provoquer directement un mineur à faire un usage illicite de stupéfiants est puni de cinq ans d'emprisonnement et de 100000 euros d'amende. Lorsqu'il s'agit d'un mineur de quinze ans ou que les faits sont commis à l'intérieur d'un établissement scolaire ou éducatif ou, à l'occasion des entrées ou des sorties des élèves, aux abords d'un tel établissement, l'infraction définie par le présent article est punie de sept ans d'emprisonnement et de 150000 euros d'amende ».

⁸⁴⁵ Article 227-21alinéa 1 du code pénal « Le fait de provoquer directement un mineur à commettre un crime ou un délit est puni de cinq ans d'emprisonnement et de 150000 euros d'amende ».

⁸⁴⁶ Voir l'article de Patrick Sabatier, « Le Net accusé d'incitation au meurtre », Libération, supplément Multimédia du 16 avril 1999.

⁸⁴⁷ C. Féral-Schuhl, Cyberdroit, préc.,p.110.

ii. Incitation à la violence contre les autorités publiques et de police.

Suites aux évènements et différentes manifestations sauvages en Seine Saint-Denis de 2005, les weblogs et autres sites Internet ont fleuris sur la toile, relatant les faits. Certains auteurs de weblogs ont dû comparaître devant la justice pour incitation à la violence. Ils ont été condamnés pour provocation à la violence⁸⁴⁸.

iii. Incitation aux actes de terrorisme

Ces infractions sont prévues par le titre 2 du livre IV du Code pénal. En son article 322-6-1, le code pénal sanctionne d'une peine d'un an de prison et de 15.000 euros d'amende, « *le fait de diffuser par tout moyen, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substance explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole* ». L'utilisation d'Internet pour une diffusion vers un public non déterminé est un facteur aggravant qui fait passer la peine à trois ans d'emprisonnement et 45.000 euros d'amende.

Internet sert la cause des organisations terroristes qui veulent faire propagande à une échelle mondiale. On a beaucoup parlé dans la période post "11 septembre", des manifestes de fabrication de bombes qui circulaient librement sur le net. Le 21 septembre 2001, le responsable présumé du site stcom.net, site de fondamentalistes musulmans qui encourageait les attentats suicides, a été mis en examen pour « apologie de crime d'atteinte volontaire à la vie ». Ce site donnait accès à plusieurs autres sites prônant le « djihad » et les attentats suicides. Ces sites diffusent des images et des textes particulièrement violents, racistes et antisémites⁸⁴⁹.

Parfois, en dehors de toute activité terroriste clairement affichée, des individus ou des groupes éditent des recettes d'explosifs et d'engins incendiaires, à l'image du Manuel du terrorisme en libre accès sur le web. C'est ainsi qu'une telle initiative avait fait scandale en France en 1995,

⁸⁴⁸ Article de Nicolas Aquila paru le 9 novembre 2005 « Des weblogs appelant à la violence envoient leurs auteurs devant la justice » ; Les prévenus avaient de source policière écrit sur un weblog de Skyrock : « *L'Ile-de-France, unissez-vous, faites cramer tous les keufs. Allez au commissariat de votre ville et cramez-le* ». L'un des auteurs de ce journal n'avait que 14 ans, et officiait avec deux autres compères, âgés de 16 et 18 ans. Tous les trois ont été déférés au Parquet de Paris, où deux d'entre eux ont été mis en examen pour "*provocation à une dégradation volontaire dangereuse pour les personnes par le biais d'internet*". Le plus jeune d'entre eux a été remis en liberté pour un problème de procédure. Les deux autres sont donc aujourd'hui en liberté sous contrôle judiciaire.

Source <http://www.infos-du-net.com/actualite/5714-weblogs.html>

⁸⁴⁹ Ibid.

alors que cette dernière connaissait une vague d'attentats. Tout internaute pouvait accéder à la description exacte du procédé de fabrication d'une bombe artisanale. On pourrait être tenté de relativiser la portée de cette information tout au moins pour les mineurs à l'époque. Internet n'avait pas encore connu son explosion dans les foyers, et finalement une proportion limitée de personnes et donc de mineurs avait accès à cet outil.

Par ailleurs si l'on admet qu'Internet est rentré dans les mœurs, on prend la mesure de l'importance qu'il peut revêtir pour tout type de groupuscules extrémistes. Ils vivent dans la marginalité et la clandestinité, pour continuer à exister ils ont besoin de communiquer sur leur mouvement et de recruter. Internet leur facilite ces deux conditions de survie. Malgré l'existence de contrôles à leur égard, ils parviennent aisément à se fondre dans les interstices de la Toile. Les mineurs qui sont assez sensibles à l'appartenance à un groupe, sont susceptibles au détour de leur navigation de rencontrer ce type de propagande, d'y adhérer et de s'enrôler dans le mouvement.

Dans les modes incitatifs à la violence, les jeux en ligne et en réseaux on souvent été pointés du doigt. De tous temps, les jeux vidéo ont été soupçonnés de provoquer la violence. L'avènement de jeux en réseau qui en est le prolongement bénéficie de la même mauvaise presse. 35% des internautes français de 12 à 17 ans déclarent s'adonner aux jeux en réseau sur Internet⁸⁵⁰. Il s'agit là de la première catégorie de joueurs en nombre. Au delà de la mauvaise presse dont les jeux vidéo souffrent, il faut admettre certains jeux prêtent le flanc à de telles accusations. Il existe dans le cyberspace une catégorie de jeux qui ont fait de la violence un mode de fonctionnement. Le rapport remis au Ministre des solidarités, de la santé et de la famille Philippe Douste-Blazy en 2005⁸⁵¹ en a fait état. Le jeu *Grand Theft Auto : San Andreas*⁸⁵² en est une illustration ; le joueur peut voler des voitures, tuer des civils et des policiers (présentés comme corrompus), devenir proxénète. Le jeu peut être sans fin à moins que le héros ne meure (mort violente nécessairement). Ce n'est pas le seul jeu de cette nature. Ces jeux sont pour la plupart interdits aux mineurs ; revient alors l'éternelle question : comment vérifier l'âge des joueurs et comment empêcher les mineurs d'y accéder ? On en revient à la part de responsabilité des parents et des intermédiaires techniques dans la protection des mineurs dans le cyberspace.

⁸⁵⁰ Voir à ce propos « *La diffusion des technologies de l'information dans la société française* », CREDOC novembre 2003.

⁸⁵¹ Conférence de la famille 2005, « Protection de l'enfant et usages d'Internet », op.cit., p. 46.

⁸⁵² Distribué en France par Take Two et déconseillé au moins de 18 ans

Dans l'intervalle et en dépit des méthodes de contrôle mises en place, des mineurs accèdent et s'adonnent à ces jeux au fort potentiel de violence et qui peuvent être incitatifs à une violence réelle.

Un projet de loi relatif à la prévention de la délinquance pose dans un chapitre V article 17, des dispositions relatives à la prévention d'actes violents pour soi-même ou pour autrui⁸⁵³. Cet article vise à renforcer les moyens d'éviter que les mineurs ne soient confrontés à des images inconvenantes (pornographiques ou violentes). Pour ce faire, il met en place un dispositif répressif spécifique pour lutter contre l'utilisation des moyens de communication électroniques par les pédophiles et les trafiquants de stupéfiants : il modernise en son paragraphe I, la rédaction des articles 32 à 39 de la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs⁸⁵⁴. Cet article apporte des innovations :

- Il donne une base légale à la signalétique devant être apposée sur les documents à caractère violent, risquant d'inciter à la discrimination ou à la haine raciale et autres infractions.
- Il interdit l'exposition de documents à caractère pornographique ou violent dans les lieux publics, sauf si ces lieux sont explicitement interdits d'accès aux mineurs.

Ces innovations notables laissent cependant en suspens la question de la mise en application et donc du contrôle de ces règles. Qui va se charger d'apposer la signalétique aux millions de pages parfois volatiles qui circulent dans le cyberspace et selon quel procédé ? Le système des listes blanche et noire repose déjà sur une technique similaire à celle de la signalétique avec le succès mitigé que l'on connaît. L'apposition de la signalétique suffirait-elle à faire cautionner des documents par définitions illégaux juste parce qu'ils ne devraient pas être accessibles aux mineurs ?

La même question se pose pour le deuxième « innovation ». Il existe déjà des dispositions qui prévoient que certains sites inconvenants pour les mineurs ne leur soient pas accessibles. Ce n'est pas pour autant qu'ils ne peuvent y accéder. La nouvelle disposition pourrait marquer un

⁸⁵³ Chapitre V, article 17 (articles 32 à 39 de la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, article 227-22-1 du code pénal, article 60-3, 77-1-3 et 99-4 du code de procédure pénale) Protection des mineurs contre la pornographie et lutte contre la pédophilie sur Internet. Source le site du Sénat : Bienvenue au Sénat, « Projet de loi relatif à la prévention de la délinquance. <http://www.senat.fr/rap/a05-477/a05-47713.html>

⁸⁵⁴ C'est cette même loi qui réglemente la diffusion des films à caractère pornographique ou violent.

recul. Jusque là, était sanctionné l'accessibilité par les mineurs à des images ou contenus inconvenants. Désormais suffira-t-il qu'une interdiction explicite ait été formulée pour que la responsabilité des auteurs ne soit pas engagée ? Le problème s'était déjà posé pour des sites pornographiques qui notifiaient une interdiction d'accès pour les mineurs sur leur page d'accueil alors qu'y figuraient déjà des représentations pornographiques inconvenantes pour les mineurs. Quelle attitude adopter à l'aune des dispositions ci-dessus mentionnées ?

2. Les contenus choquants et illicites pour les mineurs.

On estime que 10% des contenus disponibles sur Internet seraient entachés d'illicéité⁸⁵⁵. La Communication de la Commission européenne sur le contenu illégal et préjudiciable sur Internet en date du 16 octobre 1996 établit une distinction. Il y aurait contenu illégal lorsque ledit contenu est délictueux en toute circonstance telles la pédopornographie, l'incitation à la haine raciale ou à la violence. Le contenu serait simplement préjudiciable en ce sens que non délictueux en soi tels les contenus pornographiques⁸⁵⁶, ils ne le deviennent que lorsqu'ils sont rendus accessibles aux mineurs (article 227-24 du code pénal).

Pour la majorité des personnes, protéger l'enfant sur Internet c'est d'abord et avant tout lutter contre les contenus pédophiles. Mais au-delà de la pornographie infantine, les contenus réprouvés pour une consultation par le mineur sont de manière générale tous les contenus érotiques ou pornographiques⁸⁵⁷.

La vente de contenus et services pour adultes aurait représenté en 2001-2002, 70% des revenus de la vente de contenus numériques auprès du grand public en Europe et dans le monde selon l'institut Jupile MMXI⁸⁵⁸. En 2005-2006, la pornographie pourrait se maintenir en tête des ventes de contenus en ligne, soit environ 17% de la valeur totale des transactions⁸⁵⁹.

⁸⁵⁵ P. Sirinelli, Conclusion in La Galaxie Internet. L'impératif de la conquête, Ed. Unicomm 1999, p. 220.

⁸⁵⁶ Livre Vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information. Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions sur le contenu illégal et préjudiciable sur Internet : Rev. DIT 1997/1, p. 44 et s., obs. S. Picard, spéc., p.45.

⁸⁵⁷ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, op.cit., p.49.

⁸⁵⁸ Source, Jupile MMXI mars 2002 : www.jmm.com/xp/jmm/press/2002/pr_031802.xml

⁸⁵⁹ Source Jupile MMXI mars 2002 et Forrester Research décembre 2002. www.forrester.com/ER/Press/Release/0,1769,658,00.html

Le déferlement de la pornographie sur Internet avec un risque accru que les mineurs puissent y être confrontés, a suscité de véritables inquiétudes qui ont générées des réactions visant la préservation des enfants. La pornographie n'est pas en elle-même illégale. Il relève de la liberté individuelle des adultes de consulter des sites pornographiques ou de diffuser à destination d'autres adultes de la pornographie. Ce qui est illégal, c'est le fait d'émettre en direction d'un mineur des messages à teneur pornographique, mais également de ne pas prévenir l'accession (inopinée ou non) d'un mineur à un contenu pornographique⁸⁶⁰.

Selon une étude consacrée en 2002 par le National Research Council (NRC) américain à la jeunesse, la pornographie et Internet, il y aurait quatre cent mille sites pornographiques payants dans le monde dont plus de cent mille seraient hébergés aux Etats-Unis. 74% de ces sites affichent des images pornographiques dès leur page d'accueil⁸⁶¹. 17% des internautes de moins de dix-huit ans (soit 24% de garçons et 10% de filles dans la tranche 12-17 ans) ont vu au cours du mois de juin 2003 au moins un page de sélection de cinquante sites pornographiques parmi les plus fréquentés sur la période⁸⁶².

La pornographie n'est pas précisément définie. Cependant la doctrine et la jurisprudence ont dégagé quelques repères. La pornographie ne peut être définie par rapport à une morale religieuse ou philosophique ; la distinction entre ce qui est permis et qui est défendu doit être faite uniquement en fonction de l'état d'évolution des mœurs à une époque définie et dans un lieu déterminé, etc.

Le code pénal n'a pas manqué de régir la matière. En son article 227-24⁸⁶³ il réprime l'atteinte indirecte qui peut être faite au mineur par la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par ce dernier. La circulaire du 13 mai 1993 précise que, « la formulation de cet article traduit la volonté de voir cet article appliqué aux services de communication audiovisuelle ainsi qu'aux service de la télématique ».

Le souci est de protéger la moralité des mineurs sans pour autant contrevenir de manière insupportable à la liberté d'expression des adultes. Dans les chiffres cités, il faut prendre en

⁸⁶⁰ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc. P. 187.

⁸⁶¹ Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur Internet, Publication 11 février 2004.

⁸⁶² Les enfants du net (I), préc.

⁸⁶³ Article 227-24 du code pénal, puni d'une peine de 75 000 euros d'amende et de trois ans de prison « le fait soit de fabriquer, transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message » lorsque ce message est susceptible d'être vu ou perçu par un mineur.

considération la part d'accès volontaires des jeunes internautes à des contenus pornographiques. Cette accession volontaire des mineurs à des contenus qui leurs sont interdits n'exonère en rien les auteurs et les éditeurs de contenus de leur responsabilité. L'élément constitutif d'infraction tient au fait que ces contenus aient été accessibles au mineur⁸⁶⁴.

Il n'a pas encore été trouvé de solution infaillible pour permettre un barrage du mineur à des contenus pornographiques. Toutefois, les mesures prises par l'éditeur du contenu pour empêcher l'accessibilité d'un mineur à des contenus violents ou pornographiques seront appréciées dans l'analyse des magistrats⁸⁶⁵. Dans l'arrêt précédemment cité du 2 avril 2002, les juges n'ont pas voulu tenir compte dans le cas qui leur était soumis, de la mise en garde placée sur la page d'accueil du site et de l'information relative à l'existence de logiciels de restriction d'accès. Dans un arrêt du 22 février 2005⁸⁶⁶, la cour d'appel de Paris a également considéré que le « caractère pornographique des publicités diffusées sur le site Internet en cause [n'était] pas contesté et le descriptif d'accès à ce site [...] [démontrait] sans équivoque que des mineurs pouvaient visionner ces messages et images simplement en se présentant comme étant majeurs et donc sans contrôle efficace ». Les juges ont également relevé que « les prévenus ont [...] admis que le contrôle mis en place ne garantissait pas une sécurité parfaite alors que des mesures techniques simples pouvaient être adoptées afin, sinon d'interdire le site aux mineurs, du moins d'ôter tout caractère choquant aux images, techniques d'ailleurs en place sur le site en cause dès le début de l'année 2000 ».

Il existe des dispositifs techniques qui demeurent néanmoins imparfaits. Le premier dispositif a pour objectif de pouvoir contrôler l'âge des internautes accédant à certains sites⁸⁶⁷. Cette disposition répond à la Recommandation du Conseil de l'Europe du 24 septembre 1998 qui suggère notamment que « *l'offre et la diffusion de contenus susceptibles de nuire aux mineurs*

⁸⁶⁴ Cour d'appel de Paris, 14 décembre 1994, voir « Courriels pornos : quand les juges trébuchent sur les liens », <http://www.juricom.net/actu/visu.php?ID=344>; et « La protection des mineurs face aux sites pornographiques », <http://www.journaldunet.com/printer;juridique040203.shtml> – Cour d'appel Paris, 13^e chambre, 2 avril 2002, D. 2002, p.1900, obs. C. Manara ; Comm. com. électr. 2002, commentaire 111 et obs., l'éditeur du site web concerné était selon la cour d'appel tenu à une « obligation de précaution ».

⁸⁶⁵ Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, Dalloz 2006, p.643.

⁸⁶⁶ CA Paris, 11^e ch. A, 22 février 2005, B. G..., J. M..., Sté New Video Production c/ le Ministère public, Juris-Data n° 2005-275291 ; voir Comm. com. électr., oct. 2005, p. 41 s., obs. A. Lepage.

⁸⁶⁷ En 1997, le Communication Decency Act (CDA) a créé un moyen de défenses pour les opérateurs qui utilisaient le systèmes de carte de crédit afin d'empêcher l'accès des mineurs aux contenus obscènes. En 1998, un Sénateur américain a déposé un autre projet de loi qui imposait (sous peine d'amende et/ou de prison) aux fournisseurs de services, la mise en place d'un système de contrôle de l'âge de l'utilisateur par le biais d'un numéro de carte bancaire. Ces deux textes ont été abandonné après que le tribunal ait jugé que ce système était impraticable, Etienne Wery, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p. 106.

[soient] subordonnées chaque fois que cela serait réalisable, à l'utilisation de moyens de protection tels que [...] des systèmes de vérification de l'âge des utilisateurs ». Ce contrôle pourrait s'effectuer par vérification d'un numéro de carte bancaire. Pendant de nombreuses années de nombreux systèmes se sont fiés à la possession de carte de crédit avec plus ou moins de succès⁸⁶⁸. Il y aurait également le système de certification par un tiers mais la difficulté réside dans le fait que les personnes qui vont consulter des sites pornographiques veulent une satisfaction immédiate et n'entendent pas entamer un processus administratif long qui les privera de l'anonymat dans lequel ils se complaisent derrière leur écran d'ordinateur.

Le Forum des droits sur Internet préconise « des solutions réalistes en ce domaine, et invite les magistrats à privilégier une interprétation des dispositions de l'article 227-24 du code pénal prenant en compte l'état de l'art des moyens permettant de satisfaire à ses dispositions »⁸⁶⁹. Ainsi, « les solutions consistant à limiter l'accès aux contenus pornographiques aux personnes en mesure d'opérer un paiement par carte bancaire, de transmettre une reproduction d'un document d'identité ou de fournir un certificat électronique attestant de leur âge paraissent par exemple constituer, en l'état de l'art, des diligences suffisantes au regard des obligations faites par l'article 227-24 du code pénal ».

Le mineur peut donc, au gré de sa navigation dans le cyberspace, rencontrer des contenus qui tout en étant légaux lui sont interdits du fait de l'effet néfaste qu'ils pourraient avoir sur lui. Il n'est pas la cible choisie, ni la victime désignée de tels contenus, et pourtant les éditeurs desdits contenus s'exposent à des poursuites pour ne pas l'avoir prémuni de cette violence ou de cette pornographie. Ce sont des infractions considérées comme faisant partie de la cybercriminalité à l'encontre des mineurs. Sans vouloir minimiser la portée de cette criminalité, il en existe une plus abjecte qui s'est construite sur l'abus et l'exploitation sexuels des mineurs de même que la diffusion des images qui en découlent. Cette cybercriminalité directe contre les mineurs et la plus fédérative pour tous les acteurs impliqués dans le combat pour la protection des mineurs. Cette criminalité à ceci de choquant qu'elle se nourrit de la vulnérabilité du mineur dont elle fait un objet de ses désirs.

⁸⁶⁸ La difficulté réside dans le fait que tous les adultes n'ont pas nécessairement une carte bancaire et que parallèlement certains mineurs peuvent en disposer, cela est surtout vrai aux Etats-Unis. Depuis le 17 septembre 2002, Visa a interdit que sa carte serve de méthode de détermination de l'âge, Etienne Wery, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p. 107.

⁸⁶⁹ Forum des droits d'Internet, « Les Enfants du Net. Les mineurs et les contenus préjudiciables sur Internet », 2004, p. 50 s. ; http://www.foruminternet.org/telechargement/documents/reco-enfance1-20040211_2.pdf

B. L'enfant objet de la cybercriminalité.

La cybercriminalité contre les mineurs est à de nombreux égards la matière la plus génératrice de textes nationaux et internationaux. C'est également la matière dans laquelle les coopérations interétatiques ont eu le plus souvent une conclusion positive. Un aspect de cette cybercriminalité cristallise à lui seul la quasi-totalité des efforts normatifs, judiciaires et policiers : il s'agit de la pédophilie. C'est l'une des criminalités la plus extrême à l'encontre des mineurs ; elle est malheureusement loin d'être la seule forme de cybercriminalité contre les mineurs. Le mineur est considéré par certains cybercriminels comme une marchandise : c'est ainsi que des enfants se négocient en ligne pour divers usages : l'adoption, l'exploitation sexuelle, etc.

1. Le « commerce » des enfants en ligne.

Internet a la réputation d'être le plus grand marché du monde. Le meilleur comme le pire se vend dans le cyberspace. Tout peut se trouver et s'acheter sur Internet. Il suffit de savoir où chercher et d'avoir la patience de chercher. Selon le rapport 2005 effectué par l'International Labour Organization (ILO), le trafic de femmes et d'enfants est le plus rentable au monde puisqu'il rapporte par an 12 milliards de livres sterling⁸⁷⁰.

La traite des êtres humains telle que définie par le droit communautaire est une violation fondamentale des droits de l'homme. L'article 5, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne stipule que « la traite des êtres humains est interdite ». C'est un acte criminel visant l'exploitation sexuelle (le plus souvent), et l'esclavage domestique, et dans une acception plus large l'exploitation à des fins commerciales des êtres humains et plus précisément, des enfants⁸⁷¹. Europol (article 2, paragraphe 2 et annexe de la convention Europol) est compétent en matière de lutte et de prévention de la traite des êtres humains, y compris les diverses formes d'exploitation sexuelle des enfants, les agressions de mineurs et le commerce des enfants abandonnés. En outre, Eurojust⁸⁷² est compétent en matière de lutte contre la traite des êtres humains dans le contexte des enquêtes et des poursuites judiciaires concernant au moins deux Etats membres de l'Union européenne

⁸⁷⁰ Source site Internet d'Innocence en danger.

⁸⁷¹ L'action de l'UE contre la traite des êtres humains et l'exploitation sexuelle des enfants, voir le site de l'Union européenne Europa – Justice et affaires intérieures – Liberté, Sécurité et Justice, http://ec.europa.eu/justice_home/fsj/crime/trafficking/fsj_crime_human_trafficking_fr

⁸⁷² Réseau institué par une décision du Conseil du 28 février 2002

(article 2, paragraphe 4 de la décision). Les enfants servent d'objet commercial pour une destination criminelle ou non. L'adoption en ligne, bien qu'illégale et basée sur la commission d'un acte illégal qui vise à terme un objectif non criminel : trouver une famille ou une nouvelle famille à un enfant. Par contre dans leur majorité, les exploitations commerciales et criminelles d'enfants n'ont pour autre but que d'en faire les victimes de crimes encore plus graves.

1- a. "L'adoption en ligne".

"L'adoption en ligne" signifie en réalité l'achat d'enfant par le biais d'Internet. Internet est souvent l'instrument de mise en relation, suivies par des démarches plus ou moins légales d'adoption de l'enfant proposé en ligne. Or l'achat d'un enfant constitutive de traite d'être humain est prohibé⁸⁷³.

Des sites proposant d'adopter des enfants, quels que soient leur âge, leur état de santé et leurs origines pullulent sur Internet. Ils proposent un « catalogue » comprenant des photographies d'enfants. Ces pratiques existent dans certains pays en voie de développement dans lesquels les demandes d'adoption sont démultipliées du fait des démarches administratives plus aisées d'adoption liées à la pauvreté et/ou à la corruption ambiante. Le Cambodge a été cité en exemple⁸⁷⁴ au point que la France a suspendu un temps les procédures d'adoption venant de ce pays.

Il s'est développé à l'échelle mondiale des activités commerciales « extraordinairement lucratives » de ventes d'enfants⁸⁷⁵. De véritables officines sont apparues qui sont spécialisées

⁸⁷³ Article 35 de La Convention Internationale sur les droits de l'enfant dispose que « Les Etats parties prennent toutes les mesures appropriées sur les plans national, bilatéral et multilatéral pour empêcher l'enlèvement, la vente ou la traite d'enfants à quelque fin que ce soit et sous quelque forme que ce soit ».

⁸⁷⁴ Une soixantaine d'agences sont spécialisées dans l'adoption au Cambodge dont la plupart agissent illégalement. Des rabatteurs repères des jeunes familles vulnérables dont ils soustraient l'enfant sous de faux prétextes pour alimenter leur catalogue d'adoption pour les occidentaux. L'enfant est alors doté d'une nouvelle identité, d'un faux certificat d'abandon et trouve rapidement le chemin d'un orphelinat. Sa photo est publiée sur Internet, son nom anglicisé, son « prix » clairement annoncé : entre 15 000 et 20 000 dollars. L'ensemble des procédures est pris en charge par l'intermédiaire. Entre 1998 et juillet 2003, date de la décision du gouvernement français de suspendre les adoptions, plus de cinq cents enfants cambodgiens ont été adoptés en France et environ deux mille aux Etats-Unis. Il est vraisemblable, compte tenu des informations qui se font jour actuellement, que dans de nombreux cas les enfants adoptés n'aient pas réellement été abandonnés ; Voir l'article Stéphanie Le Saux paru le 16 décembre 2004 dans Réformes, « Les limites du désir d'enfant » Dossier Adoption internationale.

<http://www.reforme.net/archive/article.php?num=3107&ref=200>

⁸⁷⁵ Le Monde, 21 mars 2000, « Enfants vendus, enfants bafoués, enfants trahis », par Claire Brisset (alors Directrice de l'information au comité français pour l'Unicef).

dans les adoptions illégales pour lesquelles il arrive que des nouveaux nés soient enlevés à leurs parents⁸⁷⁶. Des personnes désespérées tentant de contourner les administrations réglementant les adoptions, s'adressent à ces "marchands" et paient le prix fort pour un enfant souvent issu des pays de l'est, d'Amérique latine, de certains pays d'Asie, d'Afrique, etc. De manière générale il s'agit de pays où la législation n'est pas suffisamment répressive et les réseaux de trafic trop bien organisés. Ces trafics sont préexistants à Internet. Ces réseaux se sont emparés de cet outil dont ils ont très vite saisi les enjeux planétaires. Désormais plus besoin de se déplacer pour aller à la rencontre des enfants à adopter sur place, derrière votre écran d'ordinateur vous pourrez prendre contacts avec des intermédiaires qui se chargent des recherches et prennent en prime en charge toutes les démarches administratives.

La traite des êtres humains telle que définie dans le droit communautaire ne constitue pas seulement un acte criminel visant à l'exploitation des personnes à des fins sexuelles c'est également une violation fondamentale des droits de l'homme. Le traité sur l'Union européenne fait mention explicite de la traite des êtres humains et des délits commis à l'encontre des enfants.

Le trafic des enfants de manière générale et sur Internet en particulier suppose que l'enfant soit dépossédé de sa qualité d'humain pour être assimilé à une chose commercialisable. La notion de réseaux de trafic s'articule sur plusieurs dimensions. Mais ces "adoptions" ne se font pas toujours dans le cadre de réseaux mafieux de pays en voie de développement et/ou gangrenés par la pauvreté et la corruption. Des individus peuvent prendre contact en ligne pour organiser en direct des transactions pour la cession de leurs enfants moyennant rémunération.

Il y a quelques années, une affaire a défrayé la chronique, lorsqu'une Britannique a assigné en justice un couple dont elle était la mère porteuse ; ce dernier exigeait qu'elle se fasse avorter du deuxième fœtus dont elle était la porteuse pour n'en garder qu'un. La particularité de cette affaire reposait sur le fait qu'elle avait accepté d'être la mère porteuse du couple américain rencontré sur Internet moyennant la somme de 19 000 dollars⁸⁷⁷.

⁸⁷⁶ Ibid.

⁸⁷⁷ 11-08-2001, Une mère porteuse en justice parce qu'elle refuse de se faire avorter ; <http://lcn.canoe.com/infos/lemonde/archives/2001/08/20010811-205641.html>

En 2004 sur le site eBay, une fillette a été mise aux enchères dans la catégorie « jouets »⁸⁷⁸. Le 17 avril 2004, un couple allemand a mis en vente la fille de la femme. La fillette était âgée de 8 ans. Cent personnes auraient cliqué sur l'annonce avant qu'elle ne soit stoppée par la police alertée par une utilisatrice d'Internet. L'homme interrogé par la police a affirmé qu'il voulait tester le site et montrer les abus qui peuvent avoir lieu quasi impunément sur Internet. Les webmasters du site des enchères d'eBay qui ne s'étaient rendus compte de rien, ont indiqués à leur décharge qu'il leur était impossible de filtrer un tel « produit » avant sa vente. Une enquête a été ouverte pour tentative de trafic d'enfant⁸⁷⁹; des documents, des objets et deux disques durs d'ordinateur ont été saisis au cours d'une perquisition au domicile du couple⁸⁸⁰.

La gravité de ces crimes prend une toute autre ampleur lorsqu'ils sont commis en réseaux. De toute évidence la traite de mineurs est un commerce lucratif qui attire de nombreux réseaux mafieux.

1-b. Les réseaux de trafics de mineurs en ligne.

Les trafics de mineurs en ligne se déclinent sur plusieurs formes, avec des finalités diverses : des adoptions, des exploitations sexuelles d'enfants ou des exploitations assimilables à de l'esclavage. La constante pour tous ces crimes, est que le mineur est un produit commercial auquel il est attribué une valeur marchande.

La vente et la traite des enfants, la prostitution et la pornographie impliquant des enfants sont des pratiques étroitement liées. La vente et la traite d'enfants à des fins sexuelles sont des ramifications de la prostitution, qui va elle-même généralement de paire avec la production

⁸⁷⁸ Source : e-Juristes, « Les atteintes à la dignité humaine sur Internet », dans le cadre des cours de M. Ferry et de M. Neveu, Faustine de Lumbée, Carole Gay et Johanna Carvais ; 7 février 2005, http://www.e-juristes.org/article.php3?id_article=669

⁸⁷⁹ Le couple allemand fait l'objet d'une enquête policière pour avoir proposé une enfant de huit ans sur le site eBay. Le couple avait publié une photo de la petite-fille sur la version allemande d'eBay, avec comme mention « On peut jouer avec elle, la déguster au grill ou bien la vendre à des gitans. L'enquête ouverte en Allemagne au sujet de la petite fillette de 8 ans mise aux enchères sur Internet durant le week-end a été étendue à trois enchérisseurs. En plus du couple vendeur, les trois individus sont susceptibles d'être poursuivis pour tentative de trafic d'être humain. Les trois enchérisseurs ont proposé entre 7 \$ et 41 \$ au couple qui a mis la jeune fille aux enchères sur eBay.

⁸⁸⁰ Source : e-Juristes, « Les atteintes à la dignité humaine sur Internet », dans le cadre des cours de M. Ferry et de M. Neveu, Faustine de Lumbée, Carole Gay et Johanna Carvais ; 7 février 2005, http://www.e-juristes.org/article.php3?id_article=669

d'images, de vidéos et autres formes de matériels sexuels explicites impliquant des enfants et dont Internet n'est que le vecteur⁸⁸¹.

i. Le tourisme sexuel impliquant des enfants.

Il s'agit d'une forme d'exploitation commerciale exercée par des adultes sur des enfants au cours de voyages, généralement dans des pays peu développés⁸⁸². Ce phénomène s'est accru avec le développement des moyens de transports et le choix délibéré d'une répression plus dure de la pédophilie dans les pays les plus développés. Les pédophiles fuyant des systèmes plus répressifs "s'échappent" quelques semaines par an leur quotidien, se rendent dans des pays où la législation et la mise en œuvre de la répression comportent des lacunes de nature à leur assurer une relative impunité quant aux crimes de pédophilie.

Internet a joué un rôle important dans la pérennisation de cette pratique. Il existait déjà des agences de voyages qui sous le couvert d'activités de voyagistes légales, organisaient des réseaux parallèles de circuits sexuels « spécialisés » pour les pédo-criminels. Ces agences courraient le risque d'être découvertes et condamnées à tout moment. Désormais, pour celles qui persévèrent dans ces pratiques criminelles, Internet joue le rôle d'une succursale virtuelle proposant des services réels. Pour ce faire ils usent autant que faire se peut des failles que leur offre le cyberspace, des méthodes de cryptographie et toutes les techniques leur permettant d'entretenir leur anonymat et d'échapper aux mailles répressives. Ces voyagistes d'un genre spécial, s'organisent en de véritables réseaux auxquels il n'est possible d'accéder que sur recommandation et après avoir rempli de nombreuses conditions, leur hantise étant de faire l'objet d'infiltrations pouvant aboutir à un démantèlement de leur réseau avec toutes les conséquences que cela suppose.

Toujours pour les initiés, des pédophiles mettent sur pied des sites qui leur fournissent des astuces pour assouvir leurs penchants en prenant le moins de risques possibles. Ils se

⁸⁸¹ La pédo-pornographie – La pornographie infantile,
<http://users.swing.be/criminologie/contenus/.../pornodown.ht>

⁸⁸² Selon l'Unicef, près de 3 millions d'enfant seraient chaque année victimes d'exploitation sexuelle dans un cadre commercial ; selon l'Organisation Internationale du Travail, 1800 enfants seraient victimes de prostitution ou participeraient à des activités pédopornographiques. Toujours selon l'OIT, 1 200 000 enfants feraient l'objet de trafics, dont une partie à des fins d'exploitation sexuelle. La réalité est qu'il est très difficile d'établir des chiffres fiables car il n'existe aucun marqueur pour évaluer l'exploitation sexuelle des enfants. Source : Rapport de propositions remis à Marie-Josée Roig Ministre de la famille et de l'enfance, et à Léon Bertrand Ministre délégué au Tourisme, « La lutte contre le tourisme sexuel impliquant des enfants », http://www.famille.gouv.fr/rapports/tourisme_sex/rapport.pdf

partagent les informations sur les pays les plus laxistes en la matière, des adresses et des contacts sur place, etc. Ils existent un marché en aval pour leurs « souvenirs de vacances » : photographies, vidéo de vacances qu'ils s'échangent sous le mode du troc ou moyennant paiement.

L'arsenal juridique qui vise la répression du tourisme sexuel impliquant des enfants est en nette progression depuis quelques années tant au niveau national qu'international. De nombreux textes internationaux traitent la question de l'exploitation sexuelle des enfants. Le texte de référence est la Convention onusienne relative aux droits des enfants de 1989. D'autres processus internationaux ont été engagés, notamment au congrès de Stockholm de 1996 relatif à l'exploitation sexuelle des enfants à des fins commerciales. Un congrès similaire a été réitéré cinq ans plus tard à Yokohama. En 2000, a été adopté un protocole additionnel à la Convention sur les droits de l'enfant relatif à la vente d'enfants, la prostitution et la pornographie. En 2001 est intervenu le protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer, punir la traite des personnes et en particulier des femmes et des enfants. Au sein de l'Union européenne, une décision-cadre a été adoptée le 22 décembre 2003⁸⁸³ ; elle est relative à l'exploitation sexuelle des enfants et à la pédopornographie.

L'article 225-12 du code pénal sanctionne le fait d'avoir des relations sexuelles avec un mineur se livrant même occasionnellement à la prostitution avec une aggravation des peines encourues lorsque le contact s'est fait par le biais d'Internet. La notion de tourisme sexuel existe en droit pénal français dans l'article 225-12-3 qui énonce que : « Dans les cas où les délits prévus par les articles 225-12-1 et 225-12-2 sont commis à l'étranger par un Français ou par une personne résidant habituellement sur le territoire français, la loi française est applicable ». Les peines sont portées à sept ans d'emprisonnement et 100.000 euros d'amende lorsqu'il s'agit d'un mineur de quinze ans.

L'expression tourisme sexuelle recouvre différentes incriminations telles que la corruption de mineur, les atteintes ou agressions sexuelles portée par un majeur à un mineur de quinze ans ou la prise d'image de mineurs à caractère pornographique en vue de la diffusion. Ces

⁸⁸³ Décision-cadre 2004/68/JAI du Conseil, du 22 décembre 2003, relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. JO L 13/44 du 20.01.2004
<http://europa.eu/scadplus/leg/fr/lvb/l33138.htm>

agissements sont réprimés même lorsqu'ils sont commis à l'étranger. Pour ce faire il convient de faire appliquer les articles 113-6 et suivants du code pénal à la lumière des lois du 17 juin 1998 et du 4 mars 2002 qui ont facilité les poursuites en la matière. La loi pénale française applicable à tout crime commis à l'étranger et notamment aux viols, l'est aussi aux délits d'atteintes et agressions sexuelles, aux recours à la prostitution de mineurs. La loi française s'applique même si ces délits ne sont pas punis dans le pays où ils ont été commis et même en l'absence de dénonciation par les autorités locales et/ou de plainte de la victime.

Il existe de nombreux textes, chartes, codes et labels développés par l'industrie du tourisme et les pouvoirs publics. Ces textes ont pour but d'associer tous les acteurs du tourisme contre le tourisme sexuel impliquant des enfants⁸⁸⁴. Ces engagements ont rarement débouché sur la mise en œuvre d'actions concrètes hormis la diffusion d'informations auprès des voyageurs. Peu de systèmes de suivi de réalisations ont été mis en place.

ii. Le trafic d'enfants en ligne à des fins sexuelles.

L'article 225-12-1 du code pénal érige en infraction le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution, y compris de façon occasionnelle. L'infraction est punie de trois ans et de 45.000 euros d'amende. Lorsque la personne a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication, la peine est portée à cinq ans d'emprisonnement et 75.000 euros d'amende.

Il a souvent été affirmé que les pédophiles s'organisaient en réseau sur la Toile afin de pouvoir échanger entre eux tout ce qui se rapporte à leurs crimes : échange de matériel pédopornographique (photographies, vidéos, etc.), échanges d'informations pratiques telles des adresses ou des destinations propices au tourisme sexuel portant sur des mineurs. On

⁸⁸⁴ La charte de l'Enfant et de l'Agent de voyages adoptée en 1993 et réalisée par la Fédération Universelle des Associations d'Agences de Voyages – La Résolution adoptée en 1995 par l'International Association of social Tourism – La Résolution adoptée par l'International Air Transport Association en 1996 – La Déclaration de l'ECTAA (European association of travel agents and tour operators) en 1996 – La Résolution adoptée en 1997 par la Federaton of International Youth Travel organisation – Le Code mondial d'Ethique du Tourisme adopté en 1999 au sein de l'OMT – La Charte d'Ethique du Tourisme adoptée en 2000 par le gouvernement français et signé par plusieurs professionnels du tourisme, elle prévoit un label « Tourisme Ethique » – Le Code de conduite mis en place par l'ECPAT en partenariat avec l'OMT et signé par de nombreux professionnels du tourisme. Ce code repose sur six critères : il a été développé dès 2000 en Autriche, Allemagne, Italie, Pays-Bas, Suède, Royaume-Uni, il implique des formations dans pays victimes de ce fléau.

envisage même qu'ils puissent organiser par le biais d'Internet de véritables réseaux de prostitutions enfantines.

Les trafics d'enfants en ligne renvoient à plusieurs types de criminalités visant à terme l'exploitation sexuelle et/ou commerciale des enfants. Des pédocriminels se servent de la Toile pour faire du proxénétisme⁸⁸⁵. A ce propos le tribunal de grande instance de Nanterre a eu l'occasion de juger que, se rendait coupable de proxénétisme, celui qui diffuse sur Internet des messages qui ont pour objet d'attirer des clients au profit d'une prostituée. Les animateurs de réseaux de prostitution de mineurs sur Internet, disposent d'enfants qui sont les leurs ou ceux de leur entourage immédiat, des enfants qu'ils ont enlevés ou qui sont sous leur responsabilité. Ils les proposent aux membres occasionnels ou non du réseau. Internet leur sert de vitrine sur le même modèle que des sites de vente normaux. Ils fournissent des représentations des enfants à vendre, organisent des enchères. Ces proxénètes de la pédocriminalité ne sont pas toujours eux-mêmes des pédocriminels. Il s'agit parfois de personnes simplement dénuées de scrupules qui ne voient là qu'un trafic très lucratif. Le doigt est souvent pointé sur des réseaux mafieux des pays de l'est.

Le trafic des enfants sur Internet peut s'organiser sur le mode d'un « troc ». Des pédocriminels créent des réseaux leur permettant de s'échanger entre eux des enfants qu'ils ont eux même déjà abusés. Il peut s'organiser sous le mode de cession.

Ce qu'il faut noter s'agissant des trafics de mineurs dans le cyberspace, c'est qu'ils existaient préalablement à Internet ; seulement Internet leur a donné une nouvelle dimension comme cela a été le cas pour de nombreux domaines légaux ou non. Ces pratiques criminelles perdurent dans le monde réel à cause des défaillances et/ou du laxisme de certains Etats à l'égard des touristes sexuels. Ceci engendre une recrudescence dans ces endroits du nombre de touristes sexuels pédocriminels. Pour pallier les carences de ces pays souvent en voie de développement, les pays développés n'hésitent plus à poursuivre leurs ressortissants qui se sont adonnés à la pédocriminalité même hors de leurs frontières. Par ailleurs, au regard de l'ampleur nocive prise par ces trafics et ces pratiques, les pays concernés commencent à prendre conscience de la nécessité d'agir. Ils commencent à prendre et à mettre en oeuvre des mesures concrètes contre ces pratiques par le biais de campagnes préventives auprès des

⁸⁸⁵ TGI Nanterre, 18 mai 2000 : Comm. com. électr., novembre 2000, commentaire. n°117, obs. J.-C. Galloux ; JCP E 2002, p.78, obs. A. Bertrand-Doulat.

familles vulnérables et des mesures répressives contre les pédocriminels. Les pédocriminels, sentant l'étau se resserrer, ont tendance à se replier dans les failles du cyberspace où à force de paranoïa il devient plus difficile de les tracer, leur potentiel de dangerosité peut s'en trouver accru.

L'organisation de réseaux de trafics d'enfants suppose un accomplissement successif de plusieurs actes criminels visant en définitive le trafic en lui-même des enfants ; l'agression sexuelle contre des mineurs, le trafic d'êtres humains, la diffusion de pornographie, etc. Les pédocriminels encourent donc de lourdes peines lorsqu'ils sont appréhendés pour ces faits. Ces crimes contre les mineurs alimentent la pédopornographie sur Internet qui est dans une logique de diffusion de supports mettant en scène des mineurs, des personnes ayant l'air de mineurs ou encore des représentations de mineurs engagés dans des postures sexuellement explicites .

2. La pédophilie sur Internet ou pédopornographie.

L'association Internet Watch Foundation (IWF)⁸⁸⁶ a publié en juillet 2006⁸⁸⁷ des statistiques sur le nombre de sites pédophiles pour le premier semestre de l'année 2006. Voici quelques chiffres clés : 14 000 signalisations à la hotline de l'association soit 24% de plus que pour le premier semestre de 2005 ; 5 000 de ces appels concernaient des problèmes liés à la pédophilie (49% de progression) ; 50% des cas de pédophilie remontent aux Etats-Unis ; 12% vers la Russie, 12% vers le Japon et 9% vers l'Espagne.

La notion de pédopornographie peut parfois poser des difficultés quant à son appréciation, difficultés de la multiplicité de définitions de la pornographie. En 2002, la Cour d'appel de Paris décrivait comme pornographique les contenus d'un site Internet figurant « des organes génitaux masculins en érection et des actes de pénétration génitale, buccale, anale »⁸⁸⁸. La décision cadre du Conseil de l'Union européenne du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants définit la pédopornographie comme la représentation visuelle « d'un enfant réel », « une personne réelle qui paraît être un enfant » ou « des images réalistes d'un enfant qui n'existe pas, participant à un comportement

⁸⁸⁶ Association de surveillance d'Internet située en Grande-Bretagne.

⁸⁸⁷ Source : Exhaustif.com, « Statistiques sur la pédophilie sur Internet », publié le 21 juillet 2006, http://www.exhaustif.com/statistiques_sur_la_pedophilie_sur_internet-00225.actu.ht...

⁸⁸⁸ CA Paris 2 avril 2002, E.L. c/Ministère public.

sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne »⁸⁸⁹. Cette décision liait les Etats membres quant aux résultats à atteindre tout en laissant les instances nationales libres de décider de la forme et des moyens d'action⁸⁹⁰.

Le cyberspace est une véritable plateforme à l'échelle internationale de diffusion de la pornographie infantine. L'évolution des technologies et des techniques d'anonymisation favorise l'explosion de pornographie infantine dans le cyberspace. Les pédophiles y ont installé des "niches" où ils communiquent entre eux, échangent des informations et des photographies⁸⁹¹, recrutent des victimes potentielles.

Derrière toute image de pornographie infantine, se cache un enfant maltraité. La photographie et la vidéo pornographique sont simplement la preuve de la maltraitance d'un enfant⁸⁹². Il existe deux types de pornographie infantine : la pornographie infantine réelle et celle dite virtuelle.

La décision-cadre de l'Union européenne a partiellement défini la pornographie infantine comme étant « l'exhibition lascive des parties génitales ou de la région pubienne d'un enfant ». Est-ce à dire qu'une photo d'un enfant dans une position équivoque mais dont la région pubienne serait couverte ou masquée ne constituerait pas de la pornographie ? Et qu'en est-il d'une scène de la vie ordinaire d'un enfant nu sous la douche ou dans son bain ? Le fait est que de nombreuses personnes se sont engouffrées dans cet interstice porteur de un flou juridique. Le résultat en est que des enfants se sont trouvés exploités jusqu'à l'extrême limite de la légalité et parfois au-delà⁸⁹³.

⁸⁸⁹ Décision cadre 2004-68-JAJ du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie, JO n° L13 du 20 janvier 2004, pp.44-48.

⁸⁹⁰ Le Forum des droits sur Internet, Recommandation, « Les enfants du Net (II) : Pédo-pornographie et pédophilie sur Internet, 25 janvier 2005.

⁸⁹¹ 500.000 photographies pornographiques mettant en scène des mineurs circulent sur Internet voire, D. Martin et F.-P. Martin, Cybercrimes : menaces, vulnérabilités et ripostes, PUF 2001, p. 35.

⁸⁹² Article du 4 mai 2006, « Le blocage des paiements via les canaux bancaires habituels soutient la lutte contre la pornographie infantine sur Internet Child Focus se réjouit de la réaction positive des banques européennes », <http://www.childfocus-net-alert.be/fr/BlocagePaiements.pdf>

⁸⁹³ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p.88-89.

2-a. La pédopornographie « réelle ».

La pornographie infantile est celle qui met en scène des enfants dans des postures ou des actes sexuels. La pédopornographie est tout matériel pornographique représentant de manière visuelle :

- Hypothèse A : un enfant réel participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne.
- Hypothèse B : une personne réelle qui paraît être un enfant participant ou se livrant au comportement visé sous le premier tiret.
- Hypothèse C : des images réalistes d'un enfant qui n'existe pas participant ou se livrant au comportement visé sous le premier tiret⁸⁹⁴.

L'article 34 de la Convention Internationale des droits de l'enfant du 20 novembre 1989, interdit explicitement l'exploitation sexuelle des enfants dans les termes suivants : « les Etats parties s'engagent à protéger l'enfant contre toutes les formes d'exploitation sexuelle et de violence sexuelle. A cette fin les Etats prennent en particulier toutes les mesures appropriées sur les plans national, bilatéral et multilatéral pour empêcher :

- que des enfants ne soient incités ou contraints à se livrer à une activité sexuelle illégale ;
- que des enfants ne soient exploités à des fins de prostitution ou autres pratiques sexuelles illégales ;
- que des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique ».

Le 26 juin 2000, l'assemblée générale de l'ONU a adopté le Protocole facultatif de la Convention relative aux droits de l'enfant. Il concerne la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants. Ce texte présente un intérêt particulier, il y est fait référence à Internet comme un phénomène nouveau et spécifique nécessitant des mesures complémentaires⁸⁹⁵. A ce propos, une Conférence internationale sur

⁸⁹⁴ Etienne Wery, 28 janvier 2004, L'Europe adopte une nouvelle décision pour mieux lutter contre la pédopornographie.

www.droit-technologie.org/1_2.asp?actu_id=882

⁸⁹⁵ Etienne Wery, Sexe en ligne : aspects juridiques et protection des mineurs, op.cit., p.52-53.

la lutte contre la pornographie impliquant des enfants sur Internet s'est tenue à Vienne en 1999. Il y a été demandé la criminalisation dans le monde entier de la production, de la distribution, l'exportation, l'importation, la transmission, la possession intentionnelle et la publicité de matériels pornographiques impliquant des enfants. Ce faisant, l'accent a été mis sur la nécessité d'une coopération et d'un partenariat entre les pouvoirs publics et les professionnels d'Internet.

La liste des formes de pornographies visées est restrictive. Dans certains pays comme les Etats-Unis, il n'y a pornographie infantile que lorsqu'il y a eu au préalable abus ou exploitation sexuelle d'enfants. Dans d'autres pays toute image sexuellement explicite d'enfants, réelle ou créée est considérée comme de la pornographie. La loi française cite de manière exhaustive comme supports incriminés : les emblèmes, objets, films, photos, diapositives ou autres supports visuels. Point n'est fait référence à la pornographie infantile véhiculée par des écrits ou des discours. Cette dernière peut pourtant se montrer aussi nocive que la pornographie visuelle. Interpol a établi une définition assez large de la pornographie infantile : « la pornographie infantile est la conséquence de l'exploitation ou de l'abus sexuel perpétré sur un enfant. Elle peut être définie comme tout moyen de dépeindre ou de promouvoir l'exploitation sexuelle d'un enfant, y compris sous forme écrite et/ou audio centrées sur les actes sexuels ou les organes génitaux de l'enfant »⁸⁹⁶.

Dans la réglementation française, l'article 227-23 du code pénal est l'article phare qui régit la pornographie infantile.

2.a'. La participation à l'échange de pornographie infantile.

La loi Guigou a réformé en profondeur le régime de la pornographie infantile ; cette refonte s'est poursuivie par l'article 14 de la loi du 4 mars 2002 relative à l'autorité parentale⁸⁹⁷. Dorénavant, 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 représentation présente un caractère pornographique est puni de trois ans d'emprisonnement et de 45.000 euros d'amende. Le fait 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 (article

⁸⁹⁶ Source UNESCO Web World - Innocence en Danger, La pédophilie et les abus sexuels sur enfants.
http://www.unesco.org/webworld/innocence_fr/faq_paedophilia.html

⁸⁹⁷ La loi n° 2002-305 du 4 mars 2002 relative à l'autorité parentale, J.O. Numéro 54 du 5 Mars 2002
<http://www.legifrance.gouv.fr/texteconsolide/ARECB.htm>

227-23 NCP). Le recours à Internet est un facteur aggravant faisant passer la peine à cinq ans d'emprisonnement et 75.000 euros d'amende.

2.a". La détention de pornographie infantine.

L'alinéa premier de l'article 227-23 vise expressément comme délit la diffusion de pornographie infantine, l'utilisation et la détention pour « consommation personnelle⁸⁹⁸. Pour combler cette lacune, la jurisprudence s'est servie de la théorie du recel telle que définie à l'article 321-1 du code pénal pour sanctionner la détention de pornographie infantine : le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit est punissable. Ce principe a été appliqué par le Tribunal de grande instance du Mans⁸⁹⁹.

Dans le but de réprimer spécifiquement la détention de pornographie infantine, le législateur français a ajouté un quatrième alinéa à l'article 227-23, énonçant que le fait de détenir une telle image ou représentation [de mineur] est puni de deux ans d'emprisonnement et 30.000 euros d'amende. La Cour de cassation a pris le soin de différencier comme deux infractions distinctes la diffusion et la détention de pornographie infantine. Ce faisant, elle a affirmé que rien ne s'opposait à ce que le recel d'une chose provenant d'un délit soit réprimé plus sévèrement que le délit lui-même⁹⁰⁰. Sur le fondement de cet alinéa 4, la Cour de cassation dans un arrêt du 9 novembre 2004⁹⁰¹, a considéré que la détention d'images et de représentations de mineurs dans des scènes à caractère pornographique caractérisait le délit dont elle a déclaré le prévenu coupable. La Cour de Pau dans un arrêt du 17 mars 2005 a retenu la même interprétation⁹⁰². La chambre criminelle de la Cour de cassation dans un arrêt du 28 septembre 2005⁹⁰³, a précisé que « le recel du délit de fixation, enregistrement ou transmission, en vue de leur diffusion, d'images pornographiques de mineurs est constitué

⁸⁹⁸ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, op.cit., p.65.

⁸⁹⁹ TGI Le Mans, chambre correctionnelle, 16 février 1998, Expertises, juin 1998, N°216, p.194 ; voire <http://www.droit-technologie.oeg>, rubrique « Jurisprudence ». Le directeur de cabinet du président du Conseil général de la Sarthe avait utilisé un ordinateur du secrétariat pour se connecter le soir et recevoir plusieurs milliers d'images de pornographie infantine.

⁹⁰⁰ Cass. Crim., 18 juin 2003, voire Lamy droit de l'informatique et des réseaux, Bull. actualité, n° 163, novembre 2003.

⁹⁰¹ Cass. Crim., 9 novembre 2004, n°04-82.199, F-D, RLDI 2005, n° 101, p.38, obs. L. Costes.

⁹⁰² CA Pau, chambre correctionnelle, 17 mars 2005, PP/Ministère public, n°04/00683, Juris-Data n°273677 ; Lamyline Reflex 2 décembre 2005, p.5, obs. L. Costes ; RLDI 2005/11, n°299, p.28 ;

⁹⁰³ Cass. Crim., 28 septembre 2005, n° 04-85.024, Lamyline Reflex 2 décembre 2005, p. 6 s., obs. L. Costes ; RLDI 2005/11, n° 300, p.38 s. ; Comm. com. électr. Mars 2006, p. 39, commentaire A. Lepage.

lorsque lesdites images ont été conservées dans un fichier enregistré sur le disque dur d'un ordinateur ».

La Cour de cassation italienne a catégorisé les types de diffusions incriminantes de pédopornographie sur le réseau Internet. L'article 600-ter du code pénal italien réprime la diffusion de matériel pornographique concernant les mineurs. En son premier alinéa, il prévoit que toute personne qui exploite un mineur pour la production de matériel pornographique est passible d'un emprisonnement de 6 à 12 ans et d'une amende allant jusqu'à 258.228 €, peine identique pour celui qui fait commerce de ce matériel. En son troisième alinéa, il est établi des peines pour la diffusion et la divulgation de ces matériels pornographiques.

La Cour de cassation italienne a introduit une différence entre la diffusion de pédopornographie via chat room et via le web⁹⁰⁴. Dans son arrêt n.4900 du 3 février 2003⁹⁰⁵, la cinquième section pénale de la Cour de cassation italienne se prononçant dans une affaire délicate de pédophilie en ligne a conclu que, l'article 600-ter ne s'appliquait pas au cas d'espèce. Pour la Cour, l'envoi de photos dans la chat-room est une communication one-to-one⁹⁰⁶ et ne peut être assimilé à une diffusion alors même que l'article 600-ter s'applique uniquement à la diffusion one-to-many⁹⁰⁷, à l'exclusion donc de la communication entre deux utilisateurs des réseaux. La Cour de cassation est arrivée à cette conclusion en renvoyant à sa propre jurisprudence⁹⁰⁸. Cette conclusion de la Cour a cassé la décision du Tribunal de Trieste, qui avait au contraire retenu l'application de l'article 600-ter du fait que, dans le cyberspace l'interlocuteur est inconnu⁹⁰⁹. La Cour de cassation crée donc une distinction entre la diffusion par le web et celle par chat room Il est toutefois à signaler que, la Cour de cassation s'était préalablement prononcée en sens contraire dans une autre affaire de 2000⁹¹⁰, elle avait conclu à l'application de l'article 600-ter et non de l'article 600-quater⁹¹¹. Si la

⁹⁰⁴ Giovanni Maria Riccio, La Cour de cassation crée une différence entre la diffusion de pédo-pornographie via chat room et via web, 23 mai 2003, <http://www.droit-technologie.org>

⁹⁰⁵ Dans le cas d'espèce, un homme avait agi dans un chat line sous le pseudonyme « tcbsx » et avait divulgué du matériel pornographique représentant des mineurs engagés dans des activités sexuelles entre eux, ainsi qu'avec des adultes. Ces photos étaient incidemment parvenues à des policiers présents dans la chat room sous de faux noms.

⁹⁰⁶ Communication privée

⁹⁰⁷ Communication publique

⁹⁰⁸ Voir dans le même sens les arrêts n°2842 de 2000, n°2421 de 2000 et n°5397 de 2002.

⁹⁰⁹ Suivant le raisonnement du juge, il est possible que, une, deux ou plusieurs personnes reçoivent l'information diffusée : l'émetteur ne peut pas savoir avec précision qui est son interlocuteur et s'il n'y a qu'une ou plusieurs personnes.

⁹¹⁰ Décision du 27 avril 2000, 2000, II, c., 685 obs. Russo, publiée également sur <http://www.foro.it>

⁹¹¹ Giovanni Maria Riccio, La Cour de cassation crée une différence entre la diffusion de pédo-pornographie via chat room et via web, op.cit.

pornographie mettant en scène les abus dont ont été victimes des enfants est unanimement sanctionnée, la représentation fallacieuse de pornographie infantine ou la création de pornographie infantine par le biais d'images de synthèse, ne génère pas la même unanimité.

2-b. La « pseudo pornographie » infantine ou pornographie infantine virtuelle.

Elle englobe deux phénomènes principaux :

- d'une part des images virtuelles telles que des réalisations de synthèses, des dessins représentant des mineurs ;
- d'autre part des représentations de personnes ayant l'aspect de mineurs⁹¹².

Au sujet de l'aspect de mineur, l'article 227-23 du code pénal précise que l'ensemble de la disposition est applicable aux images pornographiques sauf à prouver que ces personnes étaient bien majeures au sens de la loi au moment de la fixation ou de l'enregistrement de l'image.

La pornographie infantine virtuelle est celle qui met en scène des représentations de synthèses de mineurs ou de personnes en apparence mineures dans des actes sexuels ou des postures lascives. C'est l'une des matières sur laquelle se cristallisent les divergences entre les Etats qui ont eu à légiférer en la matière.

Aux Etats-Unis, la pornographie virtuelle infantine n'est pas considérée comme un crime. Le Child pornography Prevention Act (CPPA) de 1996 interdisait et punissait de prison la pornographie infantine à base d'image de synthèse, considérant qu'elle ne pouvait que banaliser et alimenter la pédophilie. Saisie sur le sujet, la Cour suprême a jugé cette loi inconstitutionnelle car contraire à la liberté d'expression⁹¹³ telle qu'établie par le premier amendement. Les juges de la Cour suprême ont estimé que, la production de scènes sexuelles qui n'ont pas existées dans la réalité ne fait aucune victime et peut parfois répondre à des motivations artistiques légitimes.

L'utilisation d'Internet a été retenue comme une cause aggravante de la sanction de certaines infractions sexuelles⁹¹⁴. Internet peut être incriminé de deux manières soit parce qu'il est à

⁹¹² Etienne Wery, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p. 67.

⁹¹³ Libération 18 avril 2002, Etats-Unis : la pédophilie virtuelle n'est plus un crime, Pascal Riché.

⁹¹⁴ 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.

l'origine de la mise en contact de la victime avec l'infacteur, tantôt parce que l'infraction a été commise par Internet⁹¹⁵.

3. L'utilisation d'Internet facteur aggravant de la pédophilie.

Un certain nombre d'infractions sexuelles voient leur sanction aggravée « *lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunication* » (par exemple grâce à un forum de discussion sur Internet). La 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 mineurs⁹¹⁶ a pris en compte, dans la répression de ces infractions, le développement des télécommunications dont Internet est la manifestation la plus évidente.

C'est ainsi que le code pénal qui traite en son article 227-22 de la corruption de mineur porte la sanction de cinq ans d'emprisonnement et 75 000 euros, à sept ans d'emprisonnement et 100 000 euros d'amende en cas d'utilisation d'Internet dans la commission de l'infraction. Cette sanction semble se justifier par la réprobation du législateur qui entend appliquer une grande sévérité à l'égard du « *racolage électronique* »⁹¹⁷.

Pour l'essentiel, les types de criminalités concernées par Internet sont tout à fait "traditionnels" et préexistants à Internet tel : le terrorisme, les traites de mineurs, la pornographie infantile, etc. Les criminels se sont contentés d'utiliser cette nouvelle technologie au profit de leurs activités dès lors qu'ils en ont évalué les débouchés planétaires exponentiels. Dans un souci de se maintenir à niveau, le législateur a intégré le caractère aggravant d'Internet lorsqu'il a servi à la commission de délits. C'est dans cette logique que, lorsque la diffusion d'images pédophiles a été faite sur Internet, les peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende. De même le législateur a prévu une aggravation de la sanction du proxénétisme lorsque celui-ci est commis « *grâce à l'utilisation pour la diffusion de message à destination d'un public non déterminé d'un réseau de télécommunication* ». La sanction encourue est alors portée à dix ans d'emprisonnement et 1 500 000 euros d'amende (code pénal article 225-7, 10°).

⁹¹⁵ A. Lepage, Droits et libertés fondamentaux à l'épreuve d'Internet, préc., p. 168.

⁹¹⁶ F. Le Gunehec, Aperçu rapide de la loi n° 98-468 du 17 juin 1998 renforçant la prévention et la répression des infractions sexuelles : JCP G 1998, act. n°28.

⁹¹⁷ F.-J. Pansier et E. Jez, La criminalité sur Internet, op.cit., p.80.

Les pédocriminels utilisent Internet comme un outil de « prédation ». C'est par ce biais qu'ils entrent en contact avec leurs futures victimes, souvent sous de fausses identités. Internet a l'avantage et l'inconvénient de faciliter l'anonymat de ses utilisateurs. Par le jeu des pseudonymes, tout internaute peut se créer une identité virtuelle qui ne correspond en rien à sa véritable identité. C'est ainsi que de nombreux prédateurs sexuels fréquentent des espaces d'échanges spécialisés ou non pour les mineurs en se faisant passer pour l'un d'entre eux. Ils se servent d'Internet comme outil de "racolage". L'objectif poursuivi par ces prédateurs est de réussir à obtenir du mineur une rencontre physique, le plus souvent basée sur un mensonge. C'est cette rencontre qui va être déterminante dans l'agression sexuelle sur le mineur. Parfois après une prise en contact sous une fausse identité, certains prédateurs réussissent à introduire leur véritable identité. Ils ont au préalable œuvré pour une mise en confiance du mineur. Ce sont souvent des personnes qui sont familières au monde des enfants, des adolescents. Ils connaissent leurs centres d'intérêts, leur langage, leurs codes et savent souvent détecter leurs détresses et trouver les mots que ne pourraient pas avoir des adultes (selon l'avis du mineur). Ils repèrent les plus vulnérables sur la Toile, et « tissent leur toile » autour d'eux.

Le Conseil d'Etat s'est montré réticent à l'égard de ces causes d'aggravation de sanction. A la suite de l'adoption de la loi du 17 juin 1998, il a rendu un rapport sur Internet et les réseaux numériques. Il émet la crainte que ces mesures soient de « nature à jeter le discrédit sur Internet en assimilant le réseau à l'utilisation d'une arme alors même qu'il constitue un espace neutre dans lequel toute forme d'activité humaine, positive ou négative, peut se développer »⁹¹⁸.

On pourrait rajouter que cette politique d'aggravation de la sanction a laissé de côté certaines infractions sexuelles dont la diffusion de messages pornographiques susceptibles d'être perçus par un mineur⁹¹⁹ par le biais des Spams ou des pop-ups.

Internet n'est pas à l'origine des crimes perpétrés à l'encontre des mineurs, mais, du fait de sa nature particulière, c'est un élément amplificateur des infractions de droit commun dont le mineur est victime. L'évolution technologique constante de la Toile engendre un type de criminalité spécifique au cyberspace. Les cybercriminels, lorsqu'ils sont appréhendés

⁹¹⁸ Internet et les réseaux numériques : Les études du Conseil d'Etat, La documentation française 1998, p.190.

⁹¹⁹ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc.,p.170.

doivent répondre de leurs crimes. Tout le dispositif juridique est mis à contribution (droit commun, droit spécifique, droit national et international), tous les acteurs également (acteurs nationaux, internationaux, institutions internationale, etc.).

§2. La sanction des cybercriminels.

Le cyberspace regorge de dangers mettant en péril la sécurité et l'intégrité des mineurs. Une lutte optimale contre les cybercriminels ne peut se satisfaire de limitations ou contingences géographiques, matérielles ou juridictionnelles. La mobilisation doit être globale : les polices, la justice, les organisations non gouvernementales, les chercheurs, les fournisseurs de services et tous les intervenants directs ou non d'Internet doivent unir leurs forces et leurs ressources⁹²⁰.

Une lutte efficace contre la cybercriminalité exige un arsenal juridique adéquat, des moyens d'investigation et de poursuite adaptés à l'ampleur et à la nature spécifique du cyberspace. Les législations étatiques s'emploient à ne pas se laisser distancer par les cybercriminels. Elles font l'effort de se mettre régulièrement en adéquation avec les évolutions technologiques d'Internet. Au niveau international, il est également à noter la multiplication de négociations, de concertations en vue de favoriser l'élaboration de textes transnationaux. La limite à cet élan international tient au fait que l'application de ces textes internationaux ne peut actuellement être que de portée nationale et dépend de la bonne volonté des Etats de les appliquer ou non. Les systèmes judiciaires et policiers bien que conscients de la nécessité de travailler en collaboration, peinent à mettre en place un système efficace et simplifié de collaboration qui ne soit pas freiné par des de morcellements géographiques et juridictionnelles. Les cybercriminels profitent des failles dans la mise en œuvre de la répression à leur encontre. Concrètement de quel arsenal normatif dispose-t-on à ce jour contre la cybercriminalité dans le cyberspace ? Et comment la rendre encore plus efficace ?

⁹²⁰ Réunion internationale organisée par l'UNESCO à Paris, les 18 et 19 janvier 1999, Henrikas Yushkavičius Sous-Directeur général pour la communication et l'information et l'informatique de l'UN, « Exploitation sexuelle des enfants, pornographie impliquant des enfants et pédophilie sur Internet : un défi international. – Vers un plan d'action à l'échelle globale » <http://www.unesco.org/general/fr/events/pedophilie/action.html>

A. Les moyens de répression contre les infractions sexuelles commises sur le mineur.

Un certain nombre de textes ont été élaborés spécialement contre la cybercriminalité tandis que dans sa majorité l'arsenal normatif relève du droit commun. Dans un souci d'adéquation il a souvent fait l'objet d'une extension ou d'une adaptation au cyberespace. La principale difficulté dans la régulation du cyberespace tient à la pléthore de textes existants. Les législations nationales et internationales se chevauchent du fait de la nature transnationale du cyberespace. Un litige survenu dans le cyberespace se cantonne rarement à l'échelle d'un seul Etat.

1. L'élaboration d'une réglementation répressive.

La répression des cybercriminels sur Internet suppose qu'il y ait un socle textuel permettant de la mettre en œuvre. Le travail d'élaboration d'une réglementation répressive contre la cybercriminalité est fait à plusieurs échelles : nationale, européenne et internationale.

1-a. Les textes internationaux.

Les textes internationaux ont la particularité d'être élaborés à la suite de négociations entre plusieurs Etats. Ces textes ne sont pas directement applicables en l'état dans les Etats. Les Etats doivent faire montre d'une volonté claire de les mettre en application, en les introduisant de manière formelle dans leur législation par le biais de transpositions notamment. Les textes internationaux, ont dès l'origine posé le principe de la protection des enfants par les Etats dont ils dépendent. Les textes internationaux dans leur majorité, ménagent des dispositions spécifiques aux enfants, il existe quelques textes internationaux uniquement élaborés autour de l'enfant.

1.a'. La Déclaration de Genève de 1924 sur les droits de l'enfant.

Cette déclaration est la première tentative de codifier les droits fondamentaux des enfants par l'Union Internationale de secours aux enfants (UISE). C'est au sein de la Société des Nations (SDN) qu'a été rédigée puis adoptée, le 26 septembre 1924, la première Déclaration des Droits de l'Enfant, connue sous le nom de la Déclaration de Genève. Le texte est très court : un petit

préambule et cinq articles⁹²¹, mais il constitue le socle de ce qui deviendra la Convention des droits de l'enfant de 1989.

1.a". La Déclaration des droits de l'enfant du 20 novembre 1959⁹²².

En 1959 les Nations unies adoptent, à l'unanimité des 78 Etats alors membres de l'organisation, une Déclaration des droits de l'enfant⁹²³. Il s'agit d'une déclaration de principe en dix points, d'ordre éthique, non contraignante pour les Etats, mais qui constitue une véritable reconnaissance des droits de l'enfant. Dans son préambule, la Déclaration énonce que « ...l'enfant, en raison de son manque de maturité physique et intellectuelle, a besoin d'une protection spéciale et de soins spéciaux, notamment d'une protection juridique appropriée, avant comme après la naissance, [et] que l'humanité se doit de donner à l'enfant le meilleur d'elle-même ».

1.a'''. Le Pacte international relatif aux droits civils et politiques de 1966⁹²⁴

En 1966, les Nations Unies adoptent deux pactes (le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels) qui concrétisent la Déclaration universelle et incluent des dispositions qui concernent la protection de l'enfance.

Le Pacte international relatif aux droits civils et politiques énonce en son article 24 alinéa 1 que : « *Tout enfant, sans discrimination aucune fondée sur la race, la couleur, le sexe, la langue, la religion, l'origine nationale ou sociale, la fortune ou la naissance, a droit, de la part de sa famille, de la société et de l'Etat, aux mesures de protection qu'exige sa condition de mineur* ». Mention est faite expressément dans l'article 10 alinéas 2 et 3 du droit du mineur à un traitement spécifique dans le régime pénitentiaire.

Les droits de l'enfant connaîtront leur consécration en 1989 avec l'adoption de la Convention internationale des droits de l'enfant.

⁹²¹ <http://www.droitsenfant.com/geneve.htm>

⁹²² Voir le texte dans son intégralité sur : <http://www.droitsenfant.com/1959.htm> ou http://www.unhchr.ch/french/html/menu3/b/25_fr.htm

⁹²³ http://www.aidh.org/DE/DE_decla_04.htm

⁹²⁴ Pacte international relatif aux droits civils et politiques, a été adopté à New-York le 16 décembre 1966 par l'Assemblée générale des Nations unies dans sa résolution 2200 A (XXI). Il est entré en vigueur après la ratification par 35 États le 23 mars 1976. Il est en principe applicable directement par les juridictions des États signataires. http://www.unhchr.ch/french/html/menu3/b/a_ccpr_fr.htm

1.a'''. La Convention internationale des droits de l'enfant du 20 novembre 1989.

Le droit international a consacré le droit de l'enfant par le biais d'un texte qui lui a été spécialement consacré. La Convention Internationale des droits de l'enfant du 20 novembre 1989 a été adoptée dans le cadre de l'Assemblée générale des Nations Unies. Cette convention fonde les droits fondamentaux internationaux du mineur. L'article 34 pose l'interdiction de l'exploitation sexuelle des enfants en ces termes : « ...les Etats prennent [...] toutes les mesures appropriées sur les plan national, bilatéral et multilatéral pour empêcher :

- que des enfants ne soient incités ou contraints à se livrer à une activité sexuelle illégale ;
- que des enfants ne soient exploités à des fins de prostitution ou autres pratiques sexuelles illégales ;
- que des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique. »

Ce texte fondateur n'a qu'une incidence limitée et indirecte dans les Etats signataires. La sanction des manquements aux droits du mineur est théorique dans la mesure où, les Etats ayant toute latitude pour prendre les mesures appropriées ne risquent aucune sanction en cas de carence. La convention dans son ensemble n'est pas coercitive à l'égard des Etats. Bien que dans certains Etats tel que la France il est possible pour les enfants et/ou leurs représentants légaux de se prévaloir des dispositions de la convention relative aux droits de l'enfant devant les juges pour faire respecter leurs droits.

Le 26 juin 2000, l'assemblée générale de l'ONU a adopté un protocole facultatif à la Convention relative aux droits de l'enfant⁹²⁵. Ce protocole porte sur la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants. L'intérêt particulier de ce texte réside dans le fait que, pour la première fois, il dénonce expressément Internet comme un phénomène nouveau et spécifique nécessitant l'adoption de mesures complémentaires.

⁹²⁵ Assemblée générale ONU, Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants ONU - 26 juin 2000 ; ce protocole est entré en vigueur depuis le 18 janvier 2002 et a été ratifié par la France le 15 avril 2003. <http://www.droitsenfant.com/protocole.htm>

D'autres textes internationaux sans aucune force contraignante se veulent également protecteurs de l'enfant.

1.a'''''. Convention sur la cybercriminalité.

Le Conseil de l'Europe a adopté à Budapest le 23 novembre 2001 une Convention sur la cybercriminalité complétée le 28 janvier 2003 par un protocole additionnel relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. La convention distingue les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes, les infractions informatiques, les infractions liées à la propriété intellectuelle et aux droits connexes, les infractions se rapportant au contenu, avec un chapitre spécial visant la répression de la pornographie infantile. Ce texte n'est pas d'application directe dans les Etats. Pour se conformer à ce texte, chaque partie doit adopter les mesures normatives nécessaires pour une répression pénale conforme à son droit interne. Cette Convention limite elle-même ses effets en laissant la possibilité aux Etats qui le souhaitent de ne pas appliquer en tout ou partie deux de ses dispositions :

- celle incriminant le fait de se procurer ou de procurer à autrui de la pornographie infantile par le biais de système informatique ;
- celle incriminant la possession de pornographie infantile dans un système informatique ou un moyen de stockage de données informatiques.

Cette concession vise à « ménager » les Etats ayant par tradition une notion plus large de la liberté d'expression. Cette volonté de faire des concessions se retrouve dans la définition de la pornographie infantile, et notamment de la pornographie dite virtuelle. Ce texte laisse une grande marge d'interprétation individuelle aux Etats. La bonne volonté des Etats est indispensable au respect des textes internationaux à l'échelle nationale. Il en découle une réelle disparité dans l'application de ces textes qui n'ont aucune force autonome pour imposer leur application⁹²⁶ contrairement aux textes communautaires.

1-b. Les textes communautaires

L'Union européenne est assez prolixe en matière de textes sur le cyberspace.

⁹²⁶ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p.55.

*L'Action commune du Conseil de l'Union européenne du 24 février 1997 relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants*⁹²⁷. A cette occasion les Etats membres ont accepté de revoir leur législation respective afin d'ériger en infractions pénales certains comportements comme « *l'exploitation sexuelle des enfants aux fins de la production (...) de matériel à caractère pornographique, y compris la production, la vente et la distribution ou d'autres formes de trafic de matériel de ce type, et la détention de ce type de matériel* ».

*La Décision du Conseil de l'Union européenne du 29 mai 2000 relative à la pédopornographie sur Internet*⁹²⁸. Cette décision a été prise afin de renforcer les mesures de prévention et de lutte contre la production, le traitement, la diffusion et la détention de documents pornographiques mettant en scène des enfants. Les Etats membres devaient prendre les mesures nécessaires pour que les internautes puissent signaler aux autorités répressives les cas de diffusion présumée de documents pornographiques mettant en scène des enfants. Ils devaient dans le même temps veiller à ce que les autorités réagissent promptement dans le sens d'une répression effective. Par ailleurs ce texte visait également à mettre sur pied une coopération entre les Etats membres⁹²⁹.

L'action commune de février 1997 n'ayant permis d'atteindre ni les objectifs fixés, ni de mettre en œuvre une coopération policière efficace la Commission a élaboré un texte en 2001.

Une proposition de décision-cadre relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie a été élaborée en 2001 par la Commission européenne. Selon cette proposition, les Etats devaient prendre les mesures nécessaires pour que certains actes (ou leur tentative) soient incriminés, y compris si ils impliquent l'utilisation d'un système informatique.

Les 14 et 15 octobre 2002, le Conseil des ministres de l'Union européenne a dégagé une position commune concernant la décision-cadre relative à la lutte contre l'exploitation sexuelle des enfants et de la pédopornographie. Ce texte adopté le 22 décembre 2003, est

⁹²⁷ 97/154/JAI: Action commune du 24 février 1997 adoptée par le Conseil sur la base de l'article K.3 du Traité sur l'Union européenne, relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants *Journal officiel n° L 063 du 04/03/1997 p. 0002 - 0006*

⁹²⁸ Décision du Conseil du 29 mai 2000 relative à la pédopornographie sur Internet (2000/375/JHA). *Journal officiel des Communautés européennes L 138/1 du 9 juin 2000.*

⁹²⁹ Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, JO C 197 du 12.7.2000, p. 1-2.

entré en vigueur le 20 janvier 2004. Il était prévu qu'il soit transposé dans les Etats avant le 20 janvier 2006⁹³⁰. Ce texte comme tous les textes communautaires à vocation à constituer le droit des Etats membres.

L'article premier de la décision-cadre règle la question de la définition de la "pédopornographie". Est considérée comme de la pédopornographie, « tout matériel pornographique représentant de manière visuelle: i) un enfant réel participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne d'un enfant; ou ii) une personne réelle qui paraît être un enfant participant ou se livrant au comportement visé sous i); ou iii) des images réalistes d'un enfant qui n'existe pas participant ou se livrant au comportement visé sous i) ».

Le deuxième article énonce une série de comportements qui doivent être considérés comme illicites en tant qu'infractions liées à l'exploitation sexuelle des enfants. Ces comportements illicites consistent à :

- Contraindre un enfant à se livrer à la prostitution, exploiter ou faciliter par tout autre moyen ce phénomène ou en tirer profit ;
- Se livrer à des activités sexuelles avec un enfant, en recourant à un des moyen suivant : 1/ utilisation de la force, de la contrainte ou des menaces, 2/ offre d'argent, ou toute autre forme de rémunération en échange de services d'ordre sexuel, 3/ abus d'une position reconnue de confiance, d'autorité ou d'influence sur un enfant.

Les comportements punissables constituant une "infraction liée à la pédopornographie" impliquant ou non l'usage d'un système informatique sont : la production de pédopornographie ; la distribution, la diffusion ou la transmission de pédopornographie; le fait d'offrir ou de rendre disponible du matériel pédopornographique ; l'acquisition et la détention de matériel pédopornographique.

⁹³⁰ Décision-cadre 2004/68/JAI du Conseil, du 22 décembre 2003, relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. Cette décision-cadre vise à rapprocher les dispositions législatives et réglementaires des États Membres en ce qui concerne la coopération policière et judiciaire en matière pénale, en vue de lutter contre la traite des êtres humains, l'exploitation sexuelle des enfants et la pédopornographie. Elle consiste à introduire au niveau européen un cadre de dispositions communes afin d'aborder certaines questions, telles que l'incrimination, les sanctions, les circonstances aggravantes, la compétence et l'extradition
JO L 13/44 du 20.01.2004

Les pays membres devront adopter les dispositions nécessaires afin de rendre punissable l'incitation à commettre une des infractions énoncées ainsi que la tentative d'adopter un des comportements interdits. Les sanctions prévues par chaque État devront être "effectives, proportionnées et dissuasives". La peine privative de liberté pour les infractions visées aux articles 2, 3 et 4 est d'une durée d'un à trois ans. La peine privative de liberté pour certaines infractions qui ont des circonstances aggravantes prévoit une durée de cinq à dix ans. L'article cinq fournit une liste de circonstances aggravantes, sans préjudice d'autres circonstances introduites par la législation nationale :

- le fait de commettre une infraction sur un enfant n'ayant pas atteint la majorité sexuelle conformément à la législation nationale ;
- l'auteur a délibérément ou par imprudence mis la vie de l'enfant en danger ;
- les infractions ont été commises par recours à des violences graves ou ont causé un préjudice grave à l'enfant ;
- l'infraction est commise dans le cadre d'une organisation criminelle.

La décision-cadre introduit la responsabilité pénale et civile des personnes morales. Cette responsabilité est complémentaire de celle de la personne physique. La personne morale sera responsable si l'infraction est commise pour son compte par une autre personne qui agit individuellement ou comme membre d'un organe de la personne morale, ou qui exerce un pouvoir de décision. Les sanctions pour les personnes morales comprendront des amendes pénales et non pénales, et des sanctions spécifiques telles que l'interdiction temporaire ou définitive d'exercer une activité commerciale, une mesure judiciaire de dissolution ou l'exclusion des bénéfices et avantages publics.

Afin d'éviter que des crimes restent impunis pour cause de conflit de compétence, la décision a introduit deux critères.

- L'un lié à l'attribution de compétences. Un État aura un pouvoir de juridiction lorsque :
 - l'infraction est commise sur son territoire (principe de territorialité) ;
 - l'auteur de l'infraction est ressortissant dudit État membre (principe de la personnalité active) ;
 - l'infraction est commise pour le compte d'une personne morale établie sur le territoire dudit État membre.

- Le deuxième critère est particulièrement important pour les États qui refusent l'extradition de leurs ressortissants. Ils devront établir les mesures nécessaires afin de poursuivre leurs ressortissants pour les infractions commises en dehors de leur territoire⁹³¹.

Le procédé de la décision-cadre se veut plus contraignant en permettant de rapprocher les dispositions législatives et réglementaires des Etats membres. Les Etats membres sont liés quant au résultat à atteindre tout en laissant les instances nationales libres de décider des moyens d'action⁹³².

1-c. Les législations nationales.

La majorité des Etats se sont dotés de dispositions pénales plus ou moins répressives dont le but est d'interdire la pornographie infantine, les abus sexuels et l'exploitation sexuelle des enfants. Quelles que soient leurs différences, il existe des points communs dans les législations nationales.

1.c'. Les constantes dans les législations nationales.

Il existe des constantes dans les neuf pays pris comme référence en la matière, ces pays sont : l'Allemagne, l'Angleterre/Pays de Galles, l'Autriche, la Belgique, le Danemark, l'Espagne, l'Italie, la Suisse, et les Etats-Unis. Dans tous ces pays, il existe des dispositions spécifiques de lutte contre la pornographie infantine⁹³³.

La production et la diffusion de représentations pornographiques d'enfants constituent des infractions spécifiques dans tous ces pays. L'élaboration de mesures répressives est assez récente en Autriche⁹³⁴, en Belgique⁹³⁵, en Espagne⁹³⁶ et en Italie⁹³⁷. Ces législations ont respectivement fait l'objet de modifications afin d'en élargir le champ des infractions et

⁹³¹ Synthèse de la décision-cadre du 22 décembre 2003, <http://europa.eu/scadplus/leg/fr/lvb/133138.htm>

⁹³² La décision-cadre est un instrument juridique issu du titre VI du Traité sur l'Union européenne (« Coopération policière et judiciaire en matière pénale ») depuis l'entrée en vigueur du Traité d'Amsterdam. Cet instrument se veut plus contraignant et directif, voir plus efficace dans le cadre du troisième pilier remanié. La décision-cadre est proposée sur l'initiative de la Commission ou d'un Etat membre, elle doit être adoptée à l'unanimité.

⁹³³ Site du Sénat français : Bienvenue au Sénat, La lutte contre la pornographie infantine, Service des affaires européennes Mai 2001.

http://www.senat.fr/lc/lc90/lc90_mono.html

⁹³⁴ Elles ont été instaurées par un amendement de 1994 du code pénal autrichien.

⁹³⁵ Loi belge du 25 avril 1995.

⁹³⁶ Le nouveau code pénal espagnol entré en vigueur depuis mai 1996.

⁹³⁷ La loi italienne dite anti-pédophiles du 3 août 1998.

alourdir les sanctions. La nature des sanctions diffère selon les pays : en Allemagne, Autriche, Belgique, Espagne et Italie les peines sont privatives de liberté tandis que dans les autres pays elles peuvent n'être que pécuniaires. L'Allemagne, la Belgique, l'Espagne et la Suisse ont prévu des sanctions renforcées lorsque le coupable agit dans un but lucratif ou appartient à un groupe organisé se livrant de manière régulières à ces délits.

Tous les pays étudiés à l'exception de la Suisse sanctionnent la détention de pornographie infantine. Cette position est récente ; elle a été adoptée en Angleterre en 1988, en 1993 en Allemagne, en 1994 au Danemark et plus récemment encore dans d'autres pays.

Toutes ces législations s'accordent en ce fait que la détention est moins lourdement sanctionnée que la production ou la diffusion de pornographie infantine.

Les interdictions concernent le plus souvent les seuls supports visuels. La plupart des formulations permettent de prendre en compte les représentations virtuelles de la pornographie infantine.

Les législations allemande, espagnole, italienne et suisse ont étendu les interdictions aux documents sonores, et de manière générale à tout type de représentations. En revanche dans les autres pays, la formulation retenue ne permet de prendre en compte que les supports visuels ; ce faisant les textes énumèrent les principaux supports visuels (photographie, film, diapositive, image...) et y ajoutent « tout autre support visuel », ce qui permet de ménager une possible adaptation à l'évolution technologique.

En matière de représentations virtuelles, les législations belge, espagnole et italienne ne permettent pas leur prise en compte. Les législations anglaise et américaine sont très exigeantes : la législation anglaise mentionne les "pseudo photographies" c'est-à-dire les représentations ayant l'apparence de photographies. La code fédéral américain s'est enrichi quant à lui de l'article 2252 A en 1996. Cet article vise la pornographie infantine fabriquée à partir de montage ou de transformations, ainsi que les images purement virtuelles. Pour autant, les Etats-Unis n'ont pas encore consacré la pédopornographie virtuelle comme une infraction. La faute en est au Premier amendement de leur Constitution.

S'agissant de l'âge en dessous duquel la protection du mineur doit être assurée, il varie de quatorze à dix-huit ans selon les Etats.

D'autres Etats ont élaboré des législations plus répressives de lutte contre la pornographie infantine sur Internet à la suite d'évènements nationaux. A l'instar de la Belgique qui dispose d'un arsenal juridique qui fait référence en la matière.

1.c". Belgique

La loi du 13 avril 1995 contenant des dispositions en vue de la répression de la traite des êtres humains et de la pornographie infantine a mis en place un dispositif inédit de lutte contre la pornographie infantine.

Une règle d'extraterritorialité permettant la poursuite en Belgique des ressortissants belges (ou des étrangers se trouvant en Belgique) qui ont commis des infractions sexuelles à l'étranger. Cette loi ne concernait que les enfants de moins de seize ans. Elle sera modifiée par la loi du 28 novembre 2000 relative à la protection pénale des mineurs. Entrée en vigueur le 1^{er} avril 2001, cette loi précise que le mot mineur « désigne la personne n'ayant pas encore atteint l'âge de dix-huit ans ».

La diffusion de pornographie infantine est réprimée à l'article 383 bis du code pénal⁹³⁸. Ainsi, « [...] *quiconque aura exposé, vendu, loué, distribué, diffusé* [terme ajouté par la loi du 1^{er} avril 2001] *ou remis des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou faits importer, remis à un agent de transport ou de distribution, sera puni de la réclusion de cinq ans à dix ans et d'une amende de cinq cent francs à dix milles francs* ». Il y a une disposition spéciale qui aggrave l'incrimination si elle constitue un acte de participation à l'activité principale ou accessoire d'une association, et ce que le coupable ait ou non la qualité de dirigeant.

La possession de pornographie infantine est réprimée à l'article 383 bis § 2. Il faut préciser que c'est la possession en connaissance de cause qui est punie. Subsiste toutefois une incertitude quant à la consultation, peut-on l'assimiler à une possession ? La réponse se fera au cas par cas, selon l'appréciation des juges. Ceci révèle une grande importance ce d'autant

⁹³⁸ Cet article a été ajouté au code pénal belge par la loi de 1995.

plus que le droit pénal étant d'interprétation restrictive, certains fichiers et comportements à connotation pédophiles auraient pu échapper à la répression⁹³⁹.

La publicité directe ou indirecte pour les offres de service à caractère sexuel destinée spécifiquement aux mineurs, ou faisant état de services proposés par des mineurs ou des personnes prétendues telles, est réprimé par l'article 380 ter du code pénal. La peine prévue est moindre lorsque le service est fourni (uniquement) par Internet ou tout autre moyen de communication⁹⁴⁰, ce contrairement à d'autres législations nationales où il s'agit d'un facteur aggravant de la peine.

1.c'''. Les Etats-Unis

La pornographie infantine est punissable aussi bien au niveau des Etats fédérés qu'au niveau fédéral. L'article 2251 du code fédéral condamne la production d'images d'un enfant de moins de dix-huit ans « se livrant à un comportement sexuellement explicite », ainsi que la publicité relative à ces images. Sont également sanctionnées toutes les opérations préalables à cette production, qu'ils soient directs (tel que le fait d'employer, d'utiliser, de persuader, d'inciter ou de contraindre un mineur, à se livrer à un tel comportement) ou indirects (tel le fait de transporter un mineur en sachant qu'il sera utilisé pour produire des images pornographiques). Cette infraction est qualifiée d' « exploitation sexuelle d'enfants » même si la scène n'est pas réelle mais simulée.

Il faut entendre par comportement sexuellement explicite et ce conformément à l'article 2256 :

- les relations sexuelles quelle que soit leur nature ;
- la zoophilie ;
- la masturbation ;
- les violences sadomasochistes ;
- l'exhibition « lascive » des parties génitales ou de la région pubienne d'un mineur.

L'infraction relative à la possession d'images pornographiques représentant des mineurs est constituée dès lors que l'accusé détient l'une de ces représentations. Toutefois il peut

⁹³⁹ La loi établit une liste restrictive de ce qui tombe sous le coup de la loi : les emblèmes, objets, films, photos, diapositives, ou autres supports visuels. Excluant par exemple des fichiers sonores à caractère pornographique.

⁹⁴⁰ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, op.cit, p.59.

valablement se défendre, s'il détient moins de trois documents et s'il établit qu'il a pris, rapidement et de bonne foi, des mesures pour les détruire ou en référer à l'autorité responsable, tout en empêchant l'accès ou la copie de ces instruments.

La lutte américaine contre la pornographie infantile ne se conçoit que dans le respect du premier amendement de la constitution protégeant la liberté d'expression, farouchement défendue (avec un succès certain) par les associations de protection des droits civiques⁹⁴¹. La liberté d'expression et le premier amendement de la constitution américaine qui en est le creuset, ont constitué jusque là un frein à la régulation américaine sur certains aspects du cyberspace.

→ Le 8 février 1996 le Congrès a adopté le Communication Decency Act (CDA) dont la première disposition, condamne la diffusion en toute connaissance de cause de messages obscènes ou indécents à des mineurs. La deuxième disposition condamne la diffusion de messages « manifestement choquants » dont les mineurs sont des destinataires potentiels. Le *Communication Decency Act* prévoyait de punir d'amende et de peines d'emprisonnement la diffusion de messages "obscènes" ou "indécents" susceptibles d'être captés par des personnes de moins de 18 ans.

Ces dispositions ont été invalidées par le contrôle de constitutionnalité opéré par la Cour suprême après que, des associations de libertés civiques en aient contesté la constitutionnalité⁹⁴². La Cour a jugé la qualification des contenus incriminés trop vague et le champ d'application de la loi trop large pour ne pas être de nature à porter atteinte aux principes du 1^{er} amendement de la constitution américaine. Les termes employés par la Communication decency act tels : « indécent » ou « manifestement choquant » ont été considérés comme étant insuffisamment précis par rapport à la portée potentiellement pénale du texte. Il aurait été trop difficile de définir ce qui constitue une information à caractère « obscène ». Par ailleurs, toute restriction d'accès fondée sur l'âge de la majorité sexuelle serait à la fois difficile à mettre en place d'un point de vue technologique et serait onéreuse. La Cour suprême a ainsi indiqué que « toute réglementation d'Internet visant les contenus, l'intention fût-elle louable, risquait de mettre le feu au village global simplement pour faire rôtir un cochon », et ce « en raison de la nature d'Internet » et de la Constitution américaine. Elle a reconnu qu'Internet différerait de toutes les infrastructures de communication mises en

⁹⁴¹ Etienne Wéry, Sexe en ligne : aspects juridiques et protection des mineurs, préc., p.73.

⁹⁴² Arrêt de la Cour suprême, Reno vs American Civil Liberties Union (ACLU) rendu le 26 juin 1997.

place jusqu'alors et qu'il pouvait aider les individus à renforcer leurs capacités, en ajoutant que tout processus de réglementation devait faire preuve de la plus grande prudence. Ce qui n'était pas le cas selon elle de la Communication decency act⁹⁴³. Il faudrait y voir l'équivalent du principe de légalité de la peine⁹⁴⁴.

→ Dans la foulée, le législateur américain a adopté un texte s'attaquant spécifiquement à la pédopornographie qu'elle soit en ligne ou non par la Child Pornography Prevention Act (CPPA 1996). Cette loi crée trois types d'incrimination :

- la pédophilie en chair et en os c'est-à-dire l'utilisation d'enfants dans la production pornographique (18 U.S.C. 2256(8)A) ;
- la pédophilie « virtuelle », c'est-à-dire le fait de créer l'impression que les acteurs sont des enfants alors que ce n'est pas le cas soit qu'il s'agisse d'adultes maquillés ou d'images créées par ordinateur (18 U.S.C. 2256(8)B) ;
- la diffusion ou la promotion de cette pédophilie virtuelle (18 U.S.C. 2256 (8)D).

Alors que le premier juge avait validé la loi⁹⁴⁵, la Cour d'appel l'a censurée par une décision du 17 décembre 1999⁹⁴⁶. Elle a notamment rappelé que la pornographie aux Etats-Unis ne peut être interdite que si elle revêt un caractère obscène selon l'arrêt *Miller v. California* de 1973⁹⁴⁷. Craignant que la Child Pornography Prevention Act (CPPA) ne menace les activités de ses membres, la *Free Speech Coalition*⁹⁴⁸, avait décidé de contester la constitutionnalité de la loi en justice. Elle alléguait que certaines dispositions interdisant les images qui mettent en scène des personnes qui ont l'apparence de mineurs ou donnent l'impression que des mineurs sont engagées dans une relation sexuelle, étaient rédigées en termes trop vagues les empêchant ainsi de développer leurs activités artistiques, littéraires, politiques et scientifiques protégées par la liberté d'expression garantie au premier amendement de la constitution américaine⁹⁴⁹. La cour a néanmoins admis que la mise en scène de mineurs pouvait être

⁹⁴³Publication de l'UNESCO, « Politique et société de l'information : Limitation et restriction de la circulation globale de l'information », par Gus Hosein, Février 2004, p.16.

<http://unesdoc.unesco.org/images/0013/001375/137516f.pdf>

⁹⁴⁴ Etienne Wéry, Sexe en ligne : aspects juridiques et protection du mineur, préc., p. 75.

⁹⁴⁵No. 01-1058, William Kenneth Peebles, Petitioner v. United States of America,

<http://www.usdoj.gov/osg/briefs/2001/0responses/2001-1058.resp.pdf>

⁹⁴⁶ laws.findlaw.com

⁹⁴⁷ leatherquest.com

⁹⁴⁸ Une coalition composée d'associations professionnelles de l'industrie pornographique et d'autres requérants (éditeurs, peintres et photographes)

⁹⁴⁹ États-Unis – Une loi sur la pornographie infantile invalidée par la Cour suprême 27/04/2002, <http://www.foruminternet.org/actualites/lire.phtml?id=308>

proscrite indépendamment du caractère obscène des images lorsqu'une telle réglementation répond à un intérêt supérieur : la protection des enfants contre toutes les formes d'exploitation⁹⁵⁰ et la poursuite de ceux qui encouragent la pédophilie. Mais selon elle, les termes de la loi étaient trop larges et condamnaient ainsi les images qui ne sont ni obscènes, ni issues de l'exploitation d'enfants réels.

Le 16 avril 2002, la Cour suprême a abondé dans ce sens, annulant les deux dispositions relatives à la pornographie virtuelle. Pour 6 des 9 juges, la loi était trop imprécise et imposait des restrictions injustifiées.

→ Une autre tentative législative a eu lieu en 1998 avec la Child Online Protection Act. Son champ d'action est plus restreint que la Child Decency Act. Elle ne s'applique qu'au matériel diffusé sur le Web plutôt qu'à toute communication électronique. Seules sont concernées les communications commerciales et les messages préjudiciables aux mineurs. Le mineur est entendu comme toute personne de moins de 17 ans. Le « contenu préjudiciable aux mineurs » a été préalablement défini⁹⁵¹. La Cour suprême dans un arrêt du 13 mai 2002 *Ashcroft vs ACLU* a considéré que l'utilisation de ces critères par cette loi ne peut rendre par elle-même la Child Online Protection Act inconstitutionnelle. Cela reviendrait à dire que toutes les lois fédérales sur l'obscénité ne peuvent s'appliquer au Web. La loi n'a pas été déclarée inconstitutionnelle mais son application a été suspendue et la cour l'a renvoyée à l'étude devant une Cour inférieure estimant que certains points n'avaient pas été traités⁹⁵².

→ En 2002, le législateur a édicté la Child Obscenity and Pornography Act⁹⁵³, incriminant les photos retouchées pour simuler la pornographie enfantine.

→ En avril 2003 a été adoptée la Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act, plus connue sous l'appellation Protect Act 2003. La définition de la pornographie enfantine est inspirée de la Child Pornography Prevention Act

⁹⁵⁰ Selon l'arrêt *New York v. Ferber* de 1982 bc.edu

⁹⁵¹ Il s'agit de contenu qui, pour un citoyen moyen appliquant les standards contemporains de la communauté, apparaît destiné à en appeler aux intérêts lubriques ; représente un acte sexuel spécifiquement visé par la loi applicable : et qui, pris dans son ensemble, manque d'un intérêt littéraire, artistique, politique ou scientifique, J. Krause, *Can anyone stop Internet porn ?* ABA journal, sept. 2002.

⁹⁵² Le 6 mars 2003, la 3^e Cour d'appel de Philadelphie a statué pour la deuxième fois sur la constitutionnalité du COPA. Elle a décidé que les termes employés par cette loi étaient encore trop imprécis et par conséquent empiétaient sur la liberté d'expression des internautes, les raisons évoquées sont les mêmes que celles évoquées à l'encontre de la CDA.

⁹⁵³ <http://www.whitehouse.gov/omb/legislative/sap/107-2/HR4623-h.html>

1996. Elle a toutefois été modifiée pour tenir compte des objections de la Cour suprême⁹⁵⁴. La loi s'articule autour de la pornographie impliquant réellement un mineur, la pornographie virtuelle et la pornographie retouchée rendant un mineur identifiable. Pour éviter une nouvelle sanction pour inconstitutionnalité par la Cour suprême, la loi a eu recours à la définition de la pornographie qui implique un « comportement sexuellement explicite » lequel est défini différemment selon le cas :

- dans les hypothèses où un mineur est impliqué et/ou identifiable, le comportement sexuellement explicite vise les comportements réels ou simulés suivants : « *sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same opposite sex ; bestiality ; masturbation ; sadistic or masochistic abuse ; or lascivious exhibition of the genitals or pubic area of any person* » ;
- dans l'hypothèse de pornographie virtuelle, il s'agit de comportements réels ou simulés suivants : « *graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited ; graphic or lascivious simulated bestiality, masturbation or sadistic or masochistic abuse ; or graphic or simulated lascivious exhibition of the genitals or pubic area of any person* ».

1. c'''. France

La loi Guigou a réformé en profondeur le régime de la pornographie enfantine. L'article 14 de la loi n°2002-305 du 4 mars 2002 a poursuivi l'aménagement de la matière en remodelant les articles 227-23 et 227-24 du code pénal français qui sont parmi les dispositions phares de la lutte contre la pornographie enfantine en France. L'article 227-23 dispose que, « *Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation*

⁹⁵⁴ « Any visual depiction, including any photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic mechanical, or other means, of sexually explicit conduct, where :

- (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- (B) such visual depiction is a digital image, computer image or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct ». M. Minow, *Legal Definitions of Child Pornography, Obscenity and Harmful to Minors*.

d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

» Le fait 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 cinq ans d'emprisonnement et à 75 000 € 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 télécommunications ».

La détention de pornographie infantile est réprimée à l'alinéa 4 de l'article 227-23 ; la peine étant de deux ans d'emprisonnement et 30.000 € d'amende.

L'article 227-24 du code pénal lui prévoit que *« le fait de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 € d'amendes lorsque ce message est susceptible d'être vu ou perçu par un mineur »*. C'est également au nom de la protection de l'enfance que l'article R.624-2 du code pénal sanctionne la diffusion de messages contraires à la décence⁹⁵⁵.

La loi du 17 juin 1998 dite loi Guigou et relative aux infractions sexuelles et à la protection des mineurs a étendu le champ des infractions liées à la pornographie infantile en remplaçant notamment le terme image par l'expression « image ou représentation », et alourdi les sanctions. Certains auteurs s'accordent à dire que la rédaction de l'article 227-23 est imprécise et générale pour une disposition du code pénal⁹⁵⁶, ce qui pourrait nuire à son efficacité. Cette imprécision lui conférerait le caractère d'une « infraction ouverte » ; les termes utilisés permettant de sanctionner des comportements à caractère violent ou pornographique alors même que la loi ne définit pas ce qu'est la violence ou la pornographie, dont les notions varient dans le temps et selon l'espace.

⁹⁵⁵ Mémoire de Daphnée Labourdique, sous la direction de Madame N. Mallet-Poujol, La protection des mineurs sur Internet : comparaison entre le droit français et le droit américain, Université Panthéon Assas – Paris II, DESS Droit du Multimédia et de l'Informatique 2002-2003, p.6.

⁹⁵⁶ E. Derieux, Droit de la communication, Ed. LGDJ, 1999, p.476 ; M-L. Rassat, Droit pénal spécial, Ed. Dalloz 1997, p.550 « La violence à la télévision » : Rapport de Blandine Kriegel à M. Jean-Jacques Aillagon Ministre de la culture et de la communication.

« Les dispositions du présent article sont également applicable 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 ». Cette disposition vise la "pseudo" pédopornographie qui elle, « englobe deux phénomènes principaux : d'une part les images virtuelles telles que les réalisations de synthèse et les dessins représentant des mineurs ; d'autre part les images impliquant des personnes réelles ayant l'apparence de mineurs, mais qui sont en réalité majeures au sens de la loi, au moment où les images ou les représentations incriminées ont été fixées.

Conformément à l'article 227-22 introduit par la loi de juin 1998 et l'ordonnance n°2000-916 du 19 septembre 2000, le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75 000 € ; l'utilisation d'Internet est un facteur aggravant qui porte la peine à sept ans d'emprisonnement et 100 000 € d'amende notamment si le mineur est âgé de moins de quinze ans.

Par une loi du 4 avril 2006, la France a transposé la décision-cadre du Conseil de l'Union européenne du 23 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. Par son article 16, cette loi modifie l'article 227-23 du code pénal. La modification porte sur plusieurs points :

- S'agissant du fait, en vue de sa diffusion de fixer, enregistrer ou de transmettre l'image à caractère pornographique d'un mineur, la peine est portée de trois à cinq ans d'emprisonnement et de 45 000 à 75 000 euros d'amendes.
- La mise à disposition de contenus à caractère pédopornographique est désormais sanctionnée par le code pénal de cinq ans d'emprisonnement et 75 000 euros d'amende.
- Les peines sont renforcées en cas de diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé par le biais d'un réseau de télécommunication. Les peines passent de cinq à sept ans d'emprisonnement et de 75 000 à 100 000 euros d'amende.
- La tentative est étendue à l'infraction de diffusion des contenus comme pour leur création.
- La circonstance aggravante de bande organisée s'applique désormais à toutes les infractions prévues par l'article 227-23 du code pénal.

Le projet de loi relatif à la prévention de la délinquance a été adopté en première lecture par l'Assemblée Nationale le 5 décembre 2006 et doit désormais être examiné par le Sénat. Ce projet renforce le dispositif pénal contre la délinquance des mineurs, les infractions sexuelles, etc. En matière d'Internet, il contient diverses mesures : création d'une procédure d'infiltration électronique pour rechercher les auteurs de traite de mineurs, de proxénétisme et de prostitution des mineurs, il adapte le délit de corruption de mineur aux communications électroniques et fait obligation aux fournisseurs d'accès et d'hébergement de prévenir leurs abonnés quant à l'interdiction de jeux en ligne. Les deux mesures essentielles de ce projet de loi visent à lutter contre la pédophilie sur Internet : le projet crée d'une part une infraction de « proposition sexuelle », et d'autre part, institue une procédure d'infiltration électronique⁹⁵⁷.

L'infraction de « *proposition sexuelle* » sur Internet est constituée par « *Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique* ». Ce délit est puni de deux ans d'emprisonnement et de 30 000 euros d'amendes. Les peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amendes lorsque les propositions ont été suivies d'une rencontre. Cette infraction vient compléter d'autres délits définis par le code pénal. Ce projet n'est pas très précis s'agissant de la consultation, du téléchargement et de la copie d'images pédophiles⁹⁵⁸.

La procédure « *d'infiltration électronique* ». Il s'agit d'une procédure permettant aux agents et officiers de police judiciaire de s'infiltrer électroniquement : « *Dans le but de constater les infractions mentionnées aux articles 227-18 à 227-24 du code pénal et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont spécialement habilités par le procureur général près de la cour d'appel de Paris et affectés dans un service spécialisé, procéder aux actes suivants sans en être pénalement responsables :*

⁹⁵⁷ Source : Droit et Nouvelles Technologies : Actualités, « La France veut durcir sa position en matière de pornographie enfantine. Le grooming sera puni. », Arnaud Dimeglio, http://www.droit-technologie.org/1_2asp?actu_id=1238

⁹⁵⁸ La jurisprudence n'applique pas à ces actes la qualification légale de détention d'image pédophile. Ainsi certains pédophiles ont pu échapper à la répression : *Cour de cassation, Chambre criminelle 5 janvier 2005, MP/ J.L B.* Ceci est atténué par le fait que pour les tribunaux, le fait de télécharger sur Internet et détenir dans son ordinateur des images pédophiles est constitutif du délit de recel de diffusion d'image d'un mineur à caractère pornographique : *Procureur de la République c/ Philippe H, 16 février 1998, Tribunal de Grande Instance du Mans*, dans cette affaire le prévenu avait été condamné à six mois d'emprisonnement dont trois mois avec sursis.

1° Participer sous un pseudonyme aux échanges électroniques ;

2° Etre en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ;

3° Extraire et conserver des contenus illicites dans des conditions fixées par décret ;

4° Acquérir ou échanger des contenus illicites ;

A peine de nullité, ces actes ne peuvent constituer une incitation à commettre des infractions ».

Il reste que, ce dispositif n'est pas aussi précis que la procédure d'infiltration mise en place pour certains crimes et délits commis en bande organisée telle que visée aux articles 706-81 à 706-87 du code pénal. En 2003, la Cour de cassation a confirmé un arrêt de la Cour d'appel de Poitiers qui avait appliqué l'article 227-23 (soit l'infraction de détention de pornographie infantile) à un individu qui se disait pourtant victime d'une provocation policière⁹⁵⁹. Le prévenu avait été découvert sur un forum de discussion par un internaute qui avait joué le jeu en feignant d'être intéressé par des images de pornographie infantile avant de prévenir la police qui s'est substituée à lui lors de la rencontre prévue entre les deux hommes.

La référence à l'« extraction » et à la « conservation » des contenus illicites suppose t'elle que l'on puisse consulter des sites pédophiles, et télécharger des contenus illégaux ? Dans un arrêt du 11 mai 2006⁹⁶⁰, la Cour de Cassation a annulé les poursuites contre une personne ayant détenu et transmis des fichiers pédophiles, en raison du fait que l'agent de police, en se faisant passer pour un mineur de quatorze ans, avait provoqué l'infraction. Pour éviter toute confusion, il serait nécessaire que le législateur précise les actes autorisés par les agents de police. Il conviendrait aussi de préciser le statut juridique de la consultation de sites pédophiles, du téléchargement, et de la copie d'images pédophiles⁹⁶¹.

⁹⁵⁹ Cass. Crim., 1^{er} octobre 2003, cité dans Lamy droit de l'informatique et des réseaux, Bulletin n°165, janvier 2004, p.17.

⁹⁶⁰ Cour de cassation 11 mai 2006, Antoine X.../ Ministère public, voir sur http://www.legalis.net/jurisprudence-decision.php3?id_article=1725

⁹⁶¹ Source : Droit et Nouvelles Technologies : Actualités, « La France veut durcir sa position en matière de pornographie infantile. Le grooming sera puni. », Arnaud Dimeglio, op.cit.

La France et la Belgique ont été classées meilleures élèves du monde au regard de leur législation sur la pédopornographie sur Internet⁹⁶² par le prestigieux centre américain : National Center for Missing and Exploited Children (NCMEC) qui a réalisé une étude de la législation sur la pédopornographie dans les 184 membres d'Interpol. Seuls cinq pays reçoivent une cote de 10/10, dont la France et la Belgique.

2. Le rôle de la jurisprudence.

Les juges ont été prépondérants dans la mise en place de la répression de la cybercriminalité. Ils ont dû apprendre à connaître et à maîtriser Internet, ses fonctionnalités et ses effets. Cette « spécialisation » devait leur permettre de mieux appréhender les responsabilités de tous les intervenants dans le cyberspace : les cybercriminels, les intermédiaires techniques et de manière plus générale de tous les internautes. Ils devaient être à même de mesurer la portée des délits commis dans le cyberspace. Ils étaient en première ligne pour démontrer que le cyberspace ne constitue pas un vide juridique et devaient dans le même temps trouver un juste milieu avec la multitude de textes (de droit commun ou de droit spécial) applicables.

La jurisprudence a donc joué un rôle central dans la répression de la criminalité contre les mineurs dans le cyberspace. Il n'existe toutefois pas au sein des tribunaux français de chambres ou de sections spécialisées sur les questions liées au cyberspace.

2-a. Le travail d'interprétation et de sanction des juges.

Le rôle d'interprétation des juges a toujours eu une grande importance. Le juge ne se contente pas d'appliquer la loi de manière rigide, il doit l'adapter aux circonstances de l'affaire dont il a à connaître. Son rôle d'interprétation peut être extensif ou restrictif. Ce rôle d'interprétation crée de la jurisprudence qui peut être source d'évolutions de la réglementation.

Avant la loi du 17 juin 1998, l'article 227-23 du code pénal ne sanctionnait que « le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur » à caractère pornographique ou de diffuser une telle image par quelque moyen que ce soit. Cette incrimination visait directement les responsables de sites pédopornographiques, et

⁹⁶² Source : Droit et Nouvelles Technologies : Actualités, « Pédopornographie sur Internet : la France et la Belgique classées meilleures élèves du monde ! », Etienne Wery, 11 mai 2006, http://www.droit-technologie.org/1_2asp?actu_id=1178

ne prenait pas en compte les "consommateurs" de ces images (ceux qui avaient consulté et stocké ces images sur leur ordinateur). Les juges pour pallier cette carence ne se sont pas cantonnés à la stricte application du texte ; ils ont puisé dans le droit commun pour assimiler les "consommateurs" d'images pédocriminelles aux responsables de sites pédocriminels. Par une décision du 16 février 1998⁹⁶³, le tribunal correctionnel du Mans a condamné à six mois de prison dont trois mois assortis de sursis simple, une personne qui avait stocké sur un ordinateur un millier d'images pédophiles qu'elle avait téléchargées. Les juges ont retenu l'incrimination de recel de fichiers d'images de nature pédophile à l'aide de corruption de mineurs et le délit d'enregistrement, de transmission ou de diffusion d'image à caractère pédophile⁹⁶⁴. Pour ce faire les juges du Mans se sont fondés sur l'article 321-5 du code pénal⁹⁶⁵ portant le recel.

Désormais, en matière de pédocriminalité, la loi du 17 juin 1998 a étendu l'incrimination de pédocriminalité à un plus grand nombre de comportements que ceux initialement réprimés. En cela le législateur, a pris en considération la position des juges. Il a fait le choix de ne pas conforter l'incrimination de recel qui avait été retenue par les juges du Mans en 1998, puisqu'il a mis à la disposition du juge une « voie directe de sanction pénale » des consommateurs d'images pédopornographiques. Le juge n'aurait plus à recourir à des détours comme l'infraction de recel. Pourtant le juge a recouru à ce fondement dans des décisions rendues pour des faits survenus postérieurement à la loi de juin 1998⁹⁶⁶.

Le législateur s'est montré encore plus précis par une loi du 4 mars 2002 sur l'autorité parentale⁹⁶⁷ qui, par le biais de l'article 227-23 du code pénal incrimine désormais la simple

⁹⁶³Tribunal correctionnel du Mans, 16 février 1998, Monsieur le procureur de la République c/ Philippe H. Réseaux pédophiles : JCP G 1999, II, 10 011, note J. Frayssinet
<http://www.juriscom.net/txt/jurisfr/cti/tgimans19980216.pdf>

⁹⁶⁴ Ibid.

⁹⁶⁵ Article 321-5 du code pénal « *La recel est assimilé, au regard de la récidive, à l'infraction dont provient le bien recelé.*

La détention de cassettes à caractère pédo-pornographique est poursuivie, suivant les tribunaux et les dossiers, sous deux qualifications :

- *recel de corruption de mineurs,*
- *ou recel de fixation d'enregistrement ou de transmission de l'image pornographique d'un mineur. »*

⁹⁶⁶ TGI Chartres, 22 août 2000 condamnant le prévenu à 2 mois d'emprisonnement pour avoir « sciemment recelé l'image ou la représentation d'un mineur alors que cette image ou cette représentation présentait un caractère pornographique qu'il savait provenir d'une transmission à l'aide d'un réseau de télécommunications ». La décision ne précisait pas les circonstances de l'infraction.

⁹⁶⁷ Loi n°2002-305 du 4 mars 2002, Loi relative à l'autorité parentale, JO n° 54 du 5 mars 2002

détention d'images pédopornographiques. Il est fort à parier que les juges auront encore à faire œuvre d'interprétation sur ce sujet.

A la suite de l'adoption de la loi sur l'autorité parentale de 2002 incriminant la simple détention d'images pédopornographiques, des auteurs se sont enquis du sort qui serait réservé à l'internaute qui n'ayant pas entendu se procurer des fichiers délictueux aura simplement voulu les consulter ; ce faisant ces fichiers se sont temporairement⁹⁶⁸ fixés dans le disque dur de son ordinateur. N'y aurait-il pas importation au sens de l'article 227-23 du code pénal. Dès lors, il y a plusieurs questions qui peuvent émerger : comment doit être comprise la notion d'importation et quelles opérations pourront être juridiquement considérées comme des importations sur Internet⁹⁶⁹ ? Des précisions seront nécessaires, qu'elles soient jurisprudentielles ou normatives s'agissant de la notion d'importation d'image.

2-b. La jurisprudence en matière de pédopornographie sur internet.

Depuis quelques années, les décisions en matière de pédopornographie sur Internet se multiplient. Il faut y voir l'effet combiné de plusieurs facteurs : le volume galopant d'infractions générées par Internet ; la spécialisation des textes de plus en plus précis grâce à une meilleure appréhension du cyberespace et de ses applications ; les moyens des investigateurs sont en meilleure adéquation avec les infracteurs et les infractions qu'ils traquent. Tous ces éléments aboutissent au fait que les juges ont à connaître d'un nombre sans cesse croissant de litiges et que corrélativement ils disposent d'un panel normatif plus performant.

Il ne s'agit pas d'énoncer toutes les décisions rendues en la matière, nous en présenterons quelques unes. Ces décisions nous permettront de voir quelle part d'interprétation les juges intègrent dans leurs décisions.

Par un jugement du 24 octobre 2003, le Tribunal de grande instance de Villefranche a prononcé la relaxe d'un prévenu qui avait reconnu la consultation de son fait, de sites et images à caractère pédopornographique, alors que sa boîte aux lettres électroniques n'indiquait ni réception ni émission de message. Le prévenu était poursuivi pour détention

⁹⁶⁸ F.-J. Pansier et E. Jez, *La criminalité sur Internet*, PUF 2000, op.cit., p.84.

⁹⁶⁹ A. Lepage, *Libertés et droits fondamentaux à l'épreuve d'Internet*, préc., p.182.

d'images de mineurs présentant un caractère pornographique. Il avait vainement tenté d'enregistrer les images incriminées ; la preuve de la consultation des sites incriminés n'a pu être possible que par la consultation de la mémoire temporaire de l'ordinateur du centre multimédia à partir duquel le prévenu s'était connecté. La quatrième chambre de la Cour d'appel de Lyon a confirmé le jugement du tribunal de grande instance de Villefranche par un arrêt du 1^{er} avril 2004⁹⁷⁰ sur le fondement des articles 227-23 du code pénal et 412, 485, 509, 510, 512, 513, et 515 du code de procédure pénale. La Cour de cassation en sa chambre criminelle rejettera le pourvoi en cassation le 5 janvier 2005 et confirmera⁹⁷¹ l'arrêt rendu par la Cour d'appel de Lyon.

Malgré une coordination améliorée entre les acteurs internationaux de la régulation d'Internet, il subsiste des conflits de lois résultants de litiges dans le cyberspace.

3. Les conflits des lois résultant des litiges nés dans le cyberspace.

Le monde est composé d'Etats souverains et indépendants. Lorsque les individus d'un Etat n'en franchissent pas les frontières, le droit national s'applique⁹⁷². Les échanges internationaux ont vite fait naître des conflits de juridiction. Par sa nature transfrontalière, Internet a accru en nombre et en régularité les hypothèses de conflits de lois et d'exequatur des décisions de justice, ce d'autant plus qu'il n'est pas nécessaire qu'un internaute ait franchi des frontières géographiques pour que naisse un conflit de loi nécessitant un recours à l'application du droit international privé.

3-a. L'application du droit international privé.

Avec l'avènement de réseaux Internet, on aurait pu penser que le droit international privé n'aurait pas lieu d'être dans le cyberspace, étant donné que les frontières physiques y sont inopérantes. Or les réseaux Internet ont l'air de renforcer la nécessité du droit international privé. Cela tient au développement en apparence anarchique d'Internet. Il revient au droit international privé d'assurer la protection des individus dans leurs activités affectées d'extranéité dans le cyberspace. Le conflit de loi dans le cyberspace résulte comme dans la

⁹⁷⁰ Cour d'appel de Lyon 4^e chambre Arrêt du 01 avril 2004, Ministère public / Jean Luc B.

<http://www.e-juristes.org/Images-Pedophiles-Consulter-n-est>

⁹⁷¹ <http://www.e-juristes.org/Images-Pedophiles-Consulter-n-est>

⁹⁷² Pierre Mayer, Vincent Heuzé, Droit international privé, Domat droit privé, Montchrestien 8^e édition 2004, p.5.

vie réelle de la multiplicité de normes juridiques⁹⁷³ applicables au même litige, mais surtout de la disparité de ces normes. Les Etats se rapprochent ou s'opposent par leur tradition juridique. Le bloc européen est celui qui est le plus homogène sous l'impulsion de l'Union européenne et du Conseil de l'Europe. Les Etats-Unis se rapprochent de l'Europe par leurs idéaux démocratiques et de libertés, leurs divergences tiennent à l'étendue, au respect et à la mise en œuvre de ces idéaux. Il y a aussi des Etats peu soucieux de démocratie et de liberté, ce groupe se confond parfois avec celui des pays en voie de développement. Dans une solution idéale, pour éradiquer les conflits, il faudrait uniformiser tout le droit et doter les juges d'une compétence universelle ce qui est inenvisageable en l'état actuel du droit. Les Etats mêmes les moins importants sont attachés à leur souveraineté, et ne veulent pas sacrifier leurs individualités à une norme internationale et uniforme.

Préalablement à toute décision, le juge saisi doit s'assurer qu'il est compétent pour connaître d'un litige d'implication internationale. En pratique, et s'agissant de litiges nés dans le cyberspace, le juge s'estimera compétent chaque fois que le site Internet auquel se rattache le différent est accessible dans son Etat⁹⁷⁴ ; lorsque tout ou partie l'infraction a été commise dans son Etat ou encore lorsque l'infracteur ou la victime dépend de son Etat. En matière de litige concernant Internet, le juge est souvent saisi en référé ; l'urgence justifie pratiquement toujours sa compétence⁹⁷⁵.

Qu'ils soient saisis au fond ou en référé, les juges développent une sorte de « compétence universelle » s'agissant de litiges nés dans le cyberspace ce qui est peu conforme à l'esprit habituel du droit international privé. Les juges français vont plus loin en appliquant la loi française, sans systématiquement prendre la peine de vérifier si la règle du conflit de lois désignait une loi étrangère⁹⁷⁶. Une autre technique consiste à établir une règle de conflit unilatérale qui détermine uniquement le champ d'application de la loi française, sans préciser les cas où la loi étrangère est compétente. La solution extrême mais qui est pourtant la plus proche de la réalité judiciaire est celle qui consiste à retenir comme critère de compétence du juge français que, le site Internet auquel se rattache le différent soit accessible du territoire français.

⁹⁷³ Sous la direction de Georges Chatillon, *Le droit international d'Internet*, Actes du colloque, op.cit., p. 56.

⁹⁷⁴ *Ibid.*, p. 58.

⁹⁷⁵ *Ibid.*

⁹⁷⁶ TGI Paris, 1^{re} chambre, du 3 mai 2000, « Lamy droit de l'informatique », *Bulletin d'activité* n°125, mai 2000 ; il était question d'un service d'enchère en ligne.

Le tribunal compétent pour juger un litige international est en principe, celui du défendeur, à moins que le demandeur, s'il est français ne souhaite invoquer le privilège de juridiction des articles 14 et 15 du code civil, ce qui risque de compromettre l'exequatur à l'étranger de la décision obtenue⁹⁷⁷. De nombreux pays admettent pour leurs ressortissants un privilège de juridiction⁹⁷⁸.

S'agissant de délit, le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire est compétent⁹⁷⁹. Selon la théorie de « l'ubiquité » consacrée par l'article 113-2 du nouveau code pénal, la loi pénale française peut s'appliquer à des infractions commises à l'étranger ; il suffit qu'un seul des faits constitutifs de cette infraction ait été commis sur le territoire français⁹⁸⁰.

3-b. L'exequatur des décisions de justice rendues sur cyberspace pour les pays concernés.

Aucune autorité d'exécution n'est automatiquement reconnue à l'étranger à une décision répressive rendue dans un autre pays⁹⁸¹. Ceci soulève un problème d'efficacité de la répression à l'échelle internationale. L'affaire « Yahoo ! » est l'affaire par excellence qui a démontré les difficultés à faire appliquer aux Etats-Unis (notamment) une décision française. L'application d'une décision dans un pays autre que celui dans lequel elle a été rendue est largement tributaire de la volonté de coopération de l'Etat sollicité.

L'application des décisions de justice à une échelle internationale se heurte souvent aux contradictions législatives. L'extranéité qui est constitutive de l'essence d'Internet entraîne

⁹⁷⁷ Ceci est interdit dans le cadre de l'Union européenne par la Convention de Bruxelles de 1973, devenue en 2000 un règlement « concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale ».

⁹⁷⁸ Sous la direction de Georges Chatillon, *Le droit international d'Internet*, Actes du colloque, op.cit, p. 73.

⁹⁷⁹ Règlement 2000, art. 5-3 ; et Com. 7 mars 2000, *Légipresse* 2000, III, 78 ; ayant constaté que le service télématique dont le code d'appel était litigieux, était accessible de Paris, c'est à bon droit que la Cour d'appel en a déduit que des dommages ayant été subis dans cette ville, le Tribunal de grande instance de Paris était compétent, peu importait que le fait dommageable se soit également produit dans le ressort d'autres tribunaux. – TGI Paris, référé 22 mai 2000, affaire Yahoo ! en permettant la visualisation en France d'objets nazis et la participation éventuelle d'internaute installé en France à une exposition-vente, l'exploitant du site fût-il installé aux Etats-Unis commet une faute sur le territoire français laquelle est à l'origine d'un dommage pour la LICRA et l'UEFJ ayant tous deux vocation à poursuivre toute forme de banalisation du nazisme. Un tribunal français est donc compétent pour en juger.

⁹⁸⁰ A. Huet, « Droit pénal international et Internet », *Petites Affiches* 1999, n°224, p. 39 et s.

⁹⁸¹ Sous la direction de Georges Chatillon, *Le droit international d'Internet*, Actes du colloque, préc., p.87.

dans le même temps « des frustrations judiciaires »⁹⁸² comme celles qui ont marquées la jurisprudence de l'affaire Yahoo relative à l'exposition et à la vente aux enchères d'objets nazis sur Internet⁹⁸³. Il est évident que malgré l'unanimité de tous les Etats à condamner la cybercriminalité envers les mineurs les législations divergeant sur certains points nuisent aux demandes d'exequatur. C'est ainsi que les législations américaine et française divergent sur la licéité de la pédopornographie virtuelle dans le cyberspace. Il est inéluctable que des décisions rendues en la matière par l'un ou l'autre des Etats se verront difficilement reconnaître l'exequatur dans l'un ou l'autre de ces Etats.

Les traditions culturelle et judiciaire différentes des Etats demandeurs ou sollicités pour l'exequatur d'une décision de justice jouent un rôle déterminant dans la reconnaissance de cet exequatur : diversité des approches en matière de mœurs sexuelles (la pornographie interdite en Irlande ne l'est pas en Suède), les discours d'incitation à la haine raciale selon les pays peuvent être interdits comme étant attentatoires à la dignité humaine ou alors tolérés dans le cadre de la liberté d'expression. En pratique si un Etat a reconnu le trouble à l'ordre public international du fait que ses citoyens ont accès à un contenu illicite conformément à ses lois nationales, le juge étranger estimant qu'il n'y a pas violation de son propre ordre public international est en droit de refuser l'exequatur⁹⁸⁴. En effet les conventions internationales applicables en la matière, imposent comme condition de reconnaissance de l'exequatur d'une décision étrangère, la vérification que cette décision n'est pas en contradiction avec l'ordre public international de l'Etat dans lequel l'exequatur est sollicité⁹⁸⁵.

Le premier amendement américain est un véritable obstacle pour les Etats étrangers voulant faire reconnaître l'exequatur à leurs décisions sur des litiges portant sur la liberté d'expression. La répression de la cybercriminalité est également contrainte par le caractère

⁹⁸² Maximilien Amégée, « La protection des mineurs sur Internet : la problématique de la pornographie », voir site : www.themis.u3mrs.fr

⁹⁸³ Alors que les juges français avaient condamné Yahoo France à ne plus exposer ni vendre aux enchères des objets nazis aux internautes français, elle avait cherché à obtenir en vain de Yahoo aux Etats-Unis qu'il ne soit plus possible à des internautes français d'accéder à de tels contenus illégaux en France. La décision française n'a jamais pu s'appliquer aux Etats-Unis, car le fait de vendre de tels objets nazis ou d'en faire l'exposition n'était pas prohibé aux Etats-Unis..

⁹⁸⁴ Actes du colloque, le droit international d'Internet, sous la direction de Georges Chatillon op.cit., « La mise en application des décisions de justice » par Christiane Féral-Schuhl, p.554.

⁹⁸⁵ Jurisprudence de la Cour de cassation française, article 32 et s. du Règlement 44/2001 révisant la convention de Bruxelles du 27 septembre 1968 ; aux Etats-Unis l'Uniform Foreign Money-Judgments Recognition Act qui prévoit notamment comme moyen fondant une opposition à l'exequatur, la violation de l'ordre public américain.

extranational du cyberspace ; d'où une nécessaire adaptation des moyens de répressions de la criminalité générée par le cyberspace.

B. La répression dans les actes.

Le cyberspace est véritablement considéré par les internautes comme un monde parallèle au monde réel et non simplement comme un monde virtuel qui pourrait laisser supposer qu'il s'agisse d'un monde chimérique. Le cyberspace est régi par du droit commun, du droit spécial, du droit national et international et par des règles qui lui sont propres telles : la Netiquette, les chartes de bonne conduite, etc. Les internautes soucieux du bon fonctionnement de leur espace d'expression, entendent jouer un rôle dans la lutte contre les comportements répréhensibles et contre la cybercriminalité dont sont victimes les mineurs sur la Toile. Les "internautes-citoyens" utilisent toutes les ressources à leur disposition pour mener ce combat des moyens légaux et des moyens à la limite de la légalité. Ils se fédèrent dans des actions collectives plus ou moins structurées ou dans des actes spontanés et sporadiques.

1. La lutte spontanée de particuliers dans le cyberspace.

Eu égard à la volatilité des contenus illégaux et/ou nuisibles aux enfants, les internautes ne s'en remettent pas toujours aux autorités. Quelle que soit la promptitude de leur réaction, les autorités compétentes sont souvent prises de vitesse par les infracteurs qui en un seul clic peuvent faire disparaître l'objet du délit. Ces internautes sont souvent tentés de seconder les autorités en se dotant unilatéralement du pouvoir d'intervenir en temps réel face à des contenus nuisibles.

1-a. L'organisation et la dénonciation contre la cybercriminalité.

Les internautes peuvent agir individuellement ou se constituer en groupes d'intervention qui s'apparentent à de véritables groupes d'investigations. Ils peuvent par exemple remonter les traces numériques laissées par les infracteurs anonymes et livrer ensuite les informations aux autorités⁹⁸⁶ ou se faire justice. Ils se dotent d'outils techniques tels que des logiciels pour

⁹⁸⁶ En l'occurrence, il s'agissait d'internautes qui ayant eu le tort d'apporter la contradiction à des anonymes se répandant en propos racistes, se sont vu usurper leur identité sur Internet pour la commission entre autre de délits. Ce faisant il se sont réunis dans un noyau qu'ils ont appelé le « groupe V » (terminologie issue des temps héroïques des premières messageries électroniques). Ils vont mettre sur pied une traque qui va durer deux ans. Le

tracer les cybercriminels, « patrouillent » dans les sites et les forums. Ils veillent à rester dans la légalité. Le chef du Parquet des mineurs au Tribunal d'Instance de Paris⁹⁸⁷ a fait le constat d'une explosion en progression constante de signalements de cas de détention, de recel et de diffusion de contenus pédophiles sur les supports informatiques⁹⁸⁸.

L'une des manifestations des particuliers se fait par le biais de constitutions d'associations de protection de l'enfance qui n'hésitent pas à prendre des initiatives pour apporter leur contribution à l'assainissement du cyberspace pour les enfants. La recrudescence de la cybercriminalité à l'encontre des mineurs a générée la multiplication d'associations ayant vocation à contribuer à la prévention et à la répression des crimes dont sont victimes les mineurs sur la Toile : Innocence en danger, Child Focus, ECPAT, etc.

Sous l'impulsion de son Président Daniel Cardon⁹⁸⁹, Child Focus a initié un accord de collaboration avec le secteur bancaire⁹⁹⁰. Il a été lancé en mars 2006 aux Etats-Unis sous l'appellation « Financial Coalition against Child Pornography »⁹⁹¹. Le but de cette coalition qui regroupe des banques, des institutions de cartes bancaires et des fournisseurs de services de paiements sur Internet, est de rendre impossible le paiement de matériel pornographique impliquant des enfants aux producteurs et distributeurs de tels matériels⁹⁹². Il faut relativiser la portée de cette initiative d'un double point de vue :

groupe composé de trois membres au départ va évoluer, de même que le nom qui dans sa dernière mouture sera le « groupe V8 ». Au terme de cette traque, ils ont réunis un dossier qu'ils ont transmis à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) – Libération 29 octobre 2003, Traquer les caméléons du Net, Edouard Launet.

⁹⁸⁷ Yvon Le Tallec

⁹⁸⁸ Source : Le Forum des droits sur Internet, Recommandation du 25 janvier 2005, Les enfants du net (II) : Pédopornographie et pédophilie sur Internet. La Division nationale de la répression des atteintes aux biens et aux personnes (DNRAPB) et la Direction générale de la police judiciaire (DGPN) ont reçu près de 3000 signalements en 2003, il en résulte entre 40 et 50 interpellations par an.

⁹⁸⁹ Daniel Cardon est également le Président de l'International Centre for Missing and Exploited Children (ICMEC).

⁹⁹⁰ Cette initiative a quelque peu été inspirée des précédents d'intégration de questions éthiques dans la pratique bancaire s'agissant notamment de la problématique du blanchiment d'argent. Les banques et les entreprises de cartes crédit signalent et empêchent en accord avec la police et la justice les transactions suspectes. - Le blocage des paiements via les canaux bancaires habituels soutient la lutte contre la pornographie enfantine sur Internet. Par un texte du 4 mai 2006 Child Focus se réjouit de la réaction positive des banques européennes et expose les dispositions de cet accord. <http://www.childfocus-net-alert.be/fr/BlocagePaiements.pdf>

⁹⁹¹ http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2311
The financial coalition against child pornography adds four financial services leaders to its roster
http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2851

⁹⁹² Article du 4 mai 2006, « Le blocage des paiements via les canaux bancaires habituels soutient la lutte contre la pornographie enfantine sur Internet Child Focus se réjouit de la réaction positive des banques européennes, voir <http://www.childfocus-net-alert.be/fr/BlocagePaiements.pdf>

- elle ne vise que les Etats-Unis alors même qu'on a pu constater à maintes reprises que les mesures nationales ne sont que de faible portée quand il s'agit d'Internet. Mais l'Europe a très vite emboîté le pas à cette initiative. Le conseil de la Fédération Européenne des Banques qui représente 5000 petites et grandes organisations bancaires a décidé d'adhérer à cette coalition⁹⁹³.
- elle ne vise pas les utilisateurs individuels mais plutôt les organisations ou individus qui réalisent ou distribuent de la pornographie enfantine contre paiement.

Depuis la loi du 2 janvier 2004⁹⁹⁴, l'article 2-3 du code de procédure pénale permet aux associations de déclencher une action publique pour des infractions sexuelles contre des mineurs même lorsqu'elles sont commises à l'étranger alors même que ces délits n'y sont pas réprimés.

1-b. La légitimation du hacking au service de la lutte contre la cybercriminalité.

Certains des hackers qui se distinguent par une certaine éthique et la défense de certaines valeurs dans le cyberspace se rallient souvent à la lutte contre la cybercriminalité contre les enfants. On les appelle les « corsaires »⁹⁹⁵. Ils ont une double intervention :

- Ils mettent au service de la répression des moyens intellectuels en permettant la formation des agents de l'Etat qui ne peuvent suivre les évolutions technologiques incessantes. Ils agissent parfois de leur propre initiative en se constituant en escouades qui scannent le Net à la recherche de contenus illégaux.
- Ils s'affilient également à des associations de lutte contre la cybercriminalité contre les mineurs. Ils jouent lorsqu'on le leur permet un rôle précieux. Ils connaissent la perversité et les dangers de se situer à la limite de la légalité⁹⁹⁶, de ce fait ils sont parmi les mieux placés pour combattre des personnes ayant des comportements similaires mais avec des implications autrement plus dangereuses. Les Américains parmi les premiers ont saisi les enjeux de leur participation à l'assainissement du

⁹⁹³ Voir le site childfocus.be, Edition n° 14 – Avril 2006, Editorial de Dirk Depover « Continuer à se battre pour notre cause », <http://childfocus.be/uploads/documents/77-228-child%20focus%20news%2014.pdf>

⁹⁹⁴ LOI n° 2004-1 du 2 janvier 2004 relative à l'accueil et à la protection de l'enfance, J.O. 2 du 3 janvier 2004 page 184.

<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=SANX0300107L>

⁹⁹⁵ Daniel Martin et Frédéric-Paul Martin, Cybercrime : menaces, vulnérabilités et ripostes, préc., p.76

⁹⁹⁶ Ibid.

cyberespace. Les services américains écument les congrès de hackers comme le *Def Con de Las Vegas* tous les ans pour recruter les meilleurs hackers.

Pour preuve de la reconnaissance du rôle des « hackers » dans la lutte contre la cybercriminalité dont sont victimes les mineurs, il faut noter un adoucissement dans leur description. On ne se réfère plus systématiquement aux hackers comme à des pirates. L'Institut de formation et de recherche de l'ONU, dans son rapport « Information Insecurity » de novembre 2002, les a même classés dans la catégorie des « good guys »⁹⁹⁷, des « hackers éthiques ». Il leur a même été décerné une mention spéciale⁹⁹⁸.

Les interventions non structurées de particuliers sont cependant porteuses de risques. Ces « chevaliers blancs » lorsqu'ils ne sont pas expressément mandatés par les autorités légitimes de lutte contre la pornographie infantile peuvent entraver leur action quoique de bonne foi. En traquant les contenus illicites et les cybercriminels, ils peuvent générer des problèmes collatéraux. Dans leurs tentatives d'appâter les cybercriminels, ils peuvent se rendre coupables d'incitation d'autrui à commettre un crime qui peut aboutir à une relaxe du cybercriminel. Dans un souci de piéger des cybercriminels ils peuvent s'exposer aux mêmes poursuites que les cybercriminels qu'ils traquaient, dans l'hypothèse où ils ont commis des actes illégaux. La référence à l'infraction de provocation et incitation à commettre un crime semble en voie de disparition pour les policiers, mais en sera-t-il autant pour les particuliers soucieux de s'impliquer personnellement dans la lutte contre la cybercriminalité ?

Pour ne pas laisser des internautes (même de bonne volonté) mettre en péril leur travail d'investigation, les polices nationales et internationales ont entrepris depuis quelques années de se doter du matériel et du savoir-faire les plus à la pointe pour mener à bien cette lutte. De plus, ayant pris la pleine mesure de la nécessité d'une coopération internationale, elles s'emploient à y recourir autant que faire se peut.

⁹⁹⁷ Les gentils

⁹⁹⁸ Information Security , a survival guide to the uncharted territories of cyber-threats and cyber-security , Unitar 2002.

2. La (les) police (s) contre la cybercriminalité.

Toute décision rendue en matière de cybercriminalité suppose qu'aie eu lieu une enquête policière. Pour que cette enquête soit probante, elle doit être menée par des personnes compétentes et disposant de moyens adéquats pour mener à bien leur tâche. C'est pour cette raison que les polices nationales ont du s'adapter aux spécificités des enquêtes en matière de cybercriminalité. Ils ont du acquérir de nouvelles compétences (notamment en matière technologique) et se doter de nouveaux matériels pour ne pas se laisser distancer par les cybercriminels qui eux sont très au fait des nouvelles technologies. Dès le milieu des années quatre-vingt-dix, les polices de plusieurs pays ont créé des unités spécialisées, chargées de traquer la cybercriminalité telle la pédophilie sur Internet⁹⁹⁹.

2-a. La mutation du rôle de la police : les cyberpoliciers.

En France, 1994 a vu la création de la Brigade centrale pour la répression de la criminalité informatique (BRCI) chargée de traquer la délinquance cybernétique. Les fonctionnaires qui y travaillent sont aussi bien des policiers que des informaticiens confirmés¹⁰⁰⁰. Cette Brigade ne pratique pas de surveillance aléatoire des communications dans le cyberspace. Cette fonction est du ressort d'un service de la direction générale de la police nationale (DGPN).

La gendarmerie nationale dispose de deux service chargés de la cybercriminalité contre ou par les mineurs : le service technique de recherche judiciaire et de documentation (STRJD) et l'institut de recherche criminelle de la gendarmerie nationale (IRCGN). Le STRJD a été créé pour exploiter le fichier d'information judiciaire (à l'origine un fichier manuel) concernant les crimes, délits, recherche de personnes, d'objets et de véhicules. Au sein de ce service, la division Personnes âgées, Mineurs et atteintes aux Mœurs (PANAM) traite spécifiquement des infractions dont sont victimes les mineurs et celles dont ils sont les auteurs.

En 1997, fut créé « le groupe central des mineurs victimes » suite au traumatisme provoqué par « l'affaire Dutroux » en Belgique et en France. Depuis lors, six officiers de police en poste au siège de la direction centrale de la police judiciaire à Nanterre assurent le suivi des dossiers traités localement par les services spécialisés français ; ils assurent également

⁹⁹⁹ Cynthia Guttman, *journaliste au Courrier de l'UNESCO*, Internet et la pédophilie. http://www.unesco.org/courrier/1999_09/fr/connex:/txt1.htm

¹⁰⁰⁰ Le Monde de l'éducation, juin 1999. Marc Couty, Cyberflic. Des policiers au Net

l'échange d'informations avec leurs homologues étrangers. En huit ans¹⁰⁰¹, le nombre de « dossiers individuels » traités par le groupe a été multiplié par 100, passant de 400 à 4000¹⁰⁰².

L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)¹⁰⁰³ a été créé par décret en 2000¹⁰⁰⁴. Il est rattaché au ministère de l'intérieur. Sont associés aux activités de cet office, le ministère de la défense (direction générale de la police nationale, direction centrale de la police judiciaire), et le ministère de l'économie, des finances et de l'industrie (direction générale des douanes et droits indirects et direction générale de la concurrence, de la consommation et de la répression des fraudes). Cet office a pour domaine de compétence les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication. Conformément à l'article 3 de son décret créateur, sa compétence s'étend aux infractions dont la commission a été facilitée ou est liée à l'utilisation de ces technologies. Outre son activité qui relève de la Direction des affaires économiques et financières, la police technique et scientifique a développé un Service de l'informatique et des traces technologiques (SITT¹⁰⁰⁵). Ce service a pour double mission d'assurer la gestion du réseau et la maintenance informatique de la police judiciaire et, de développer les fonctions d'analyse et d'expertise afin d'élaborer des logiciels spécifiques au monde policier. L'OCLCTIC compte 35 collaborateurs et gère environ 150 dossiers par an.

Parmi les méthodes utilisées par les cyberpoliciers de manière générale il en est quelques unes notoirement réputées efficaces :

- La veille technologique : elle permet d'identifier la personne qui a déposé le « nom de domaine » d'un site Internet, ou de repérer l'ordinateur d'une personne téléchargeant fréquemment des contenus illicites. Sur réquisition d'un Magistrat, le matériel peut être saisi et analysé par le département « info-électronique » chargé d'apporter la preuve scientifique de l'infraction.

¹⁰⁰¹ La dernière mesure a été effectuée en 2005.

¹⁰⁰² L'Express.fr, 21 mars 2005, Police. SOS mineurs, par Eric Pelletier.

¹⁰⁰³ Le commissaire divisionnaire Catherine Chambon est à la tête de l'OCLCTIC.

¹⁰⁰⁴ Décret n° 2000-405 du 15 mai 2000 publié au JORF du 16 mai 2000.

¹⁰⁰⁵ C'est à ce service qu'il revient d'exploiter et d'analyser les disques durs des ordinateurs impliqués dans des affaires judiciaires. Le SIIT est basé dans le Rhône (Ecully) gère les demandes émanant des policiers de toute la France.

- La veille du réseau permet également une étude comportementale sur Internet d'un individu suspecté de pédophilie, s'ensuit un travail en liaison avec des spécialistes de « l'analyse comportementale ».

Cependant, l'évolution des technologies a vu l'avènement de la technique de « peer to peer », il s'agit de transférer des fichiers sans transiter par des serveurs. Cette technique complique la localisation des échanges entre pédophiles sur la Toile.

La section de police qui est en charge de la lutte contre la cybercriminalité dont sont victimes les mineurs est le Groupe d'Opération de Recherche (GOR). Il est abrité dans l'immeuble de la brigade des mineurs de Paris.

2.a'. Les moyens mis à la disposition des policiers dans la lutte contre la cybercriminalité.

i. L'utilisation de la technique.

Une attention particulière est portée à la pédophilie. Le réseau est surveillé en permanence par les agents du Centre national de lutte contre la délinquance de haute technologie au STRJD, grâce au logiciel PI@net. Ils analysent en fonction de thèmes spécifiques, toute information circulant sur Internet (sites ou forums) lieu de recrutement privilégié des pédophiles¹⁰⁰⁶. L'IRCGN va plus loin dans la surveillance ; sur commission rogatoire, il procède à des interceptions ciblées, écoutes téléphoniques et développement de logiciels permettant de déceler des images à caractère pédophile sur les ordinateurs saisis lors de perquisitions. Il existe désormais plusieurs fichiers informatisés (fichiers de personnes à rechercher, fichiers des empreintes digitales, etc.) et une base de données appelée JUDEX¹⁰⁰⁷ qui répertorie les personnes mises en cause dans une infraction. Le fichier est alimenté par le travail quotidien des enquêteurs appartenant aux 3800 brigades territoriales et aux 30 sections de recherche, ainsi que les informations émanant de la police nationale, d'Interpol, d'Europol et d'associations de victimes.

Lors d'un congrès à Yokohama au Japon, des cyberpoliciers européens ont laissé entendre que l'anonymat n'existait pas véritablement sur Internet et que cela pouvait pleinement jouer

¹⁰⁰⁶ Le site du Défenseur des enfants, Interview de la Gendarmerie nationale, avril 2002, <http://www.defenseurdesenfants.fr/actu/texte3h.htm>

¹⁰⁰⁷ Système JUDiciaire de Documentation et d'EXploitation, Selon le ministère de la Défense, JUDEX daterait de 1985, et visait à "remplacer progressivement le système PROSAM de 1967. Véritable mémoire informatique, JUDEX offre la possibilité d'effectuer des rapprochements (dans le cadre d'un crime par exemple), d'identifier des empreintes digitales, ou encore de déterminer la provenance d'objets volés

dans la traque des délinquants sexuels sévissant sur la Toile. A les entendre, il ne tient qu'aux décideurs politiques de rendre possible la traque technologique des cybercriminels sur le Web¹⁰⁰⁸. Le frein à l'utilisation des moyens technologiques pour lutter contre la délinquance sexuelle sur la Toile tiendrait pour partie à la volonté de protection de la vie privée, et des autres libertés qui ont cours sur la Toile.

ii. L'acquisition de compétences technologiques.

Les policiers ont du se mettre activement à la pratique d'Internet car, pour pouvoir être opérationnels dans le cyberspace, ils ne doivent pas se laisser distancer. On pourrait tracer un parallèle avec les Brigades du Tigre¹⁰⁰⁹; corps de la police qui avait été créé et doté de véhicules à tractions pour ne plus se laisser distancer par les bandits lors de courses poursuites. Il s'était équipé du même matériel que les hors la loi pour mieux les combattre sur leur terrain. De même les cyberpoliciers ont du s'équiper de matériels et de compétences similaires aux cybercriminels afin de pouvoir les traquer dans le cyberspace.

Au mois de janvier 2005, la police a procédé à une série d'interpellations dans les milieux pédophiles à travers la France. La police agissait sur commission rogatoire du juge d'instruction de Colmar Stéphane Galland. Soixante-huit personnes ont été placées en garde-à-vue. Cette opération a permis de saisir des films et des images pédophiles sur des ordinateurs¹⁰¹⁰.

iii. La perquisition électronique

C'est un des instruments des policiers dans le cyberspace. Elle leur permet de limiter les lourdeurs géographiques susceptibles d'entraver des enquêtes transnationales et de limiter l'impact des lourdeurs administratives pour des perquisitions à l'étranger. A l'échelle

¹⁰⁰⁸ De l'avis de John Carr alors directeur de l'unité de lutte contre la cyberpornographie infantile de l'ECPAT (End Child Prostitution And Trafficking) « *Quiconque surfe sur le Web laisse une signature électronique. Si la volonté est là et que les lois nous y autorisent, les moyens technologiques nous permettent de remonter jusqu'à la source[...]* L'illusion de l'anonymat fait que beaucoup d'amateurs de pornographie infantile prennent sur le Net des risques qu'ils ne prendraient jamais dans le monde réel... ». Voir l'article de Richard Werly, Offensive en règle contre la pédophilie, Libération 21 décembre 2001.

¹⁰⁰⁹ Les brigades mobiles régionales (ou Brigades du Tigre) étaient l'ancêtre de l'actuelle police judiciaire française. Elles ont été créées sur les conseils de Célestin Hennion (directeur de la Sûreté Générale) par le Président du Conseil et ministre de l'intérieur Georges Clemenceau en 1907 afin d'avoir une police mobile. Sa création a trouvé une solution à l'augmentation de criminalité dans des proportions d'autant plus inquiétantes qu'une délinquance nouvelle est née qui s'appuie, elle, sur le progrès technique et fait échec à une police archaïque dont les méthodes et le matériel n'ont guère évolué depuis Vidocq. Cette nouvelle police d'élite disposait de tous les moyens modernes pour atteindre leurs objectifs: télégraphes, téléphones, et bientôt automobile. http://fr.wikipedia.org/wiki/Brigades_du_Tigre

¹⁰¹⁰ Source Reuters Strasbourg 25-01-2005.

nationale, une perquisition ne peut avoir lieu que si un juge d'instruction a délivré une commission rogatoire aux officiers de police judiciaire, ou si il se présente de lui-même pour l'effectuer. C'est l'article 56 du code de procédure pénale qui régit la matière¹⁰¹¹. La transposition de cette procédure dans le cyberspace a du dépasser certaines difficultés.

- La première difficulté tenait aux contingences frontalières. La compétence des officiers de police judiciaire est en effet limitée à leur juridiction, ils ne peuvent au-delà intervenir sans faire appels à leurs homologues de la juridiction concernée. Le principe de territorialité de la loi pénale interdit de dépasser le territoire de la République.
- La volatilité des contenus rend difficile les perquisitions électroniques. Comment saisir de l'immatériel, des données. L'article 56 du code de procédure pénale ne prévoyait que la saisie de papiers, documents ou autres objets. Aucune mention n'était faite de données informatiques.

La loi française a évolué sous l'effet de la Convention relative à la cybercriminalité adoptée à Budapest le 23 novembre 2001. La perquisition à distance est désormais inscrite dans le droit français¹⁰¹². Mais cette perquisition est très encadrée et très limitée. Les enquêteurs peuvent accéder à un ordinateur distant mais à plusieurs conditions :

- l'accès à distance n'est possible que par l'intermédiaire d'un système implanté sur les lieux où se déroule la perquisition physique ;
- l'utilisateur du système perquisitionné à distance doit saisir lui-même son identifiant et son mot de passe pour se connecter au serveur distant ;
- dans le cas où les données sont situées en dehors du territoire national, les autorités compétentes doivent se conformer aux engagements internationaux de coopération et

¹⁰¹¹ Il rappelle que la perquisition n'est possible que « si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces ou objets relatifs aux faits incriminés ». L'officier de police peut se rendre « au domicile de ces derniers pour y procéder à une perquisition dont-il dresse procès-verbal ». Il ne peut toutefois saisir que les « objets et documents utiles à la manifestation de la vérité ».

¹⁰¹² LOI 2002-1094 du 29 août 2002, Loi d'orientation et de programmation pour la sécurité intérieure. - Les parlementaires créent un accès direct aux données informatiques. - Les députés ont adopté le 16 janvier 2003 plusieurs amendements à la loi sur la sécurité intérieure (LSI) facilitant l'accès direct et la consultation à distance par les autorités judiciaires des données de connexion conservées notamment par les opérateurs de télécommunications ; <http://www.foruminternet.org/actualites/lire.phtml?id=489>

d'entraide. Hors à ce jour, ces accords font défaut¹⁰¹³, ce qui signifie l'impossibilité à ce jour d'une perquisition électronique transnationale.

2.a". Les limites au travail des policiers dans leur lutte contre la cybercriminalité.

Les policiers français souffrent de quelques difficultés dans leur croisade contre la criminalité dans le cyberspace.

i. Les limites d'ordre logistique.

Le matériel de travail (ordinateurs, logiciels). Les matériels techniques pour traquer la cybercriminalité sont coûteux ; d'une part car ils comportent de la technologie de pointe, mais aussi et surtout parce qu'ils nécessitent une mise à jour constante, leur obsolescence est très rapide eu égard à l'évolution continue des technologies qui sont souvent très vite assimilées et mises à profit par les cybercriminels.

La traçabilité des paquets d'information sur Internet relève de techniques criminalistiques complexes qu'il faut acquérir. Des logiciels performants mais onéreux peuvent permettre de reconstituer le cheminement (source et destination) des données numériques. Les enquêteurs doivent être à la pointe des évolutions cryptographiques¹⁰¹⁴, sténographiques¹⁰¹⁵ qui sont autant de méthodes utilisées par les cybercriminels pour dissimuler des informations sensibles qu'ils font circuler dans le cyberspace.

Les limites humaines. L'un des plus grand frein à l'action des cyber-enquêteurs tient au manque d'effectifs comparativement à la tâche à accomplir. Si le nombre de dossier a été multiplié par cent au cours de ces dernières années, le nombre d'enquêteurs affectés à leur traitement n'a pas évolué¹⁰¹⁶.

La limite tient également à la difficulté de mettre en place la coopération entre les polices. Cela tient au fait que les preuves sont difficiles à recueillir dans les pays étrangers. Il peut

¹⁰¹³ Loi sur la sécurité intérieure du 18 mars 2003, article L.57-1 du code de procédure pénale.

¹⁰¹⁴ La Cryptographie c'est une science des messages secrets ou art d'écrire un message qui soit indéchiffrable pour tout autre que soi-même et le destinataire par un code ou par un chiffre. Cela permet de crypter les communications de manière à ce qu'elles soient incompréhensibles pour quiconque les intercepterait. Dans le domaine informatique on utilise des logiciels de cryptographie. Source Dictionnaire d'informatique et d'Internet Anglais – Français, Jean-Guy Grenier, La Maison du dictionnaire Paris 2000.

¹⁰¹⁵ Procédé qui consiste à fondre des données son, texte ou image dans un autre fichier de façon à dissimuler des informations sensibles. Source Actes du colloque, sous la direction de Georges Chatillon Le droit international d'Internet, Paris, 19 et 20 novembre 2001, « Internet et enquête judiciaire » par Jean-Wilfrid Noël (Juge au Tribunal d'instance de Vanves), p. 248.

¹⁰¹⁶ L'Express.fr, 21 mars 2005, Police. SOS mineurs par Eric Pelletier.

s'avérer difficile d'obtenir des agents de polices locales l'autorisation de se déplacer et d'intervenir dans leur juridiction. Ceci est notamment le cas pour les agressions sexuelles contre mineurs qui ont eu lieu dans des pays (souvent peu développés) dans le cadre notamment du tourisme sexuel¹⁰¹⁷.

ii. Les limites normatives.

- Les limites de l'arsenal juridique français.

La principale limite pour les cyberpoliciers tient à l'insécurité de la situation juridique des enquêteurs dans ce type d'investigation. Contrairement à d'autres systèmes juridiques comme celui américain, il n'est pas légal de recourir en France à la provocation au cours d'une enquête policière, il est illégal de piéger des suspects en les poussant à la faute. C'est le cas notamment dans des affaires où des enquêteurs se sont fait passés pour des pédophiles ou des mineurs pour piéger des pédophiles.

Le fait pour un agent de police ou un intermédiaire de se connecter sur Internet en se présentant comme un mineur recherchant des relations sexuelles constitue une provocation au délit de transmission de fichiers pédophiles. La Cour de cassation dans un arrêt du 11 mai 2006¹⁰¹⁸ a cassé un arrêt de la cour d'appel de Bordeaux, chambre correctionnelle, en date du 8 juin 2005, qui condamnait le prévenu à 6 mois d'emprisonnement avec sursis, pour détention d'images de mineurs présentant un caractère pornographique. La cour de cassation a conclu à la nullité des poursuites ainsi que celle des aveux du prévenu¹⁰¹⁹. La procédure adoptée par les policiers allait à l'encontre du principe de la loyauté des preuves, la cour d'appel avait annulé les poursuites au titre de la transmission d'images pédophiles et non celles au titre de la détention de telles images. Les juges d'appel avaient distingué l'infraction de transmission de celle de détention d'images pédophiles au motif que la détention était antérieure à la transmission et donc à la provocation. La Cour de cassation réfute la distinction opérée par les juges. Les aveux du prévenu ont eu lieu lors d'une audition « *consécutive à la*

¹⁰¹⁷ Rapport de propositions remis au Ministre de la famille et de l'enfance Marie-Josée Roig et au Ministre délégué au tourisme Léon Bertrand, « La lutte contre le tourisme sexuel impliquant des enfants. Pour une stratégie française », http://www.famille.gouv.fr/rapports/tourisme_sex/rapport

¹⁰¹⁸ Cour de Cassation, chambre criminelle 11 mai 2006 Antoine X.../ Ministère public
http://www.legalis.net/jurisprudence-decision.php3?id_article=1725

¹⁰¹⁹ En l'espèce, les policiers de la brigade des mineurs avaient demandé à un intermédiaire de se connecter sur un site de rencontres sous la fausse identité d'un mineur de 14 ans. Ce dernier était entré en contact avec un internaute et l'avait incité à lui transmettre des photographies à caractère pédophile. Les deux interlocuteurs ont ensuite fixé un rendez-vous au cours duquel l'internaute a été interpellé par les policiers. Durant son audition, il a avoué détenir sur son ordinateur des fichiers pédophiles.

provocation ayant déterminé l'ensemble des poursuites ». Sans provocation, il n'y aurait pas eu d'aveux.

Cette décision tend à encadrer les procédures d'investigation sur internet. Les policiers doivent veiller à ne pas provoquer l'infraction. Si les policiers s'étaient contentés de répondre à une annonce préexistante, même sous l'identité d'un mineur de 14 ans, il n'y aurait pas eu provocation. Le fait d'être à l'origine de la demande vicie l'ensemble de la procédure¹⁰²⁰. Le Forum des droits sur Internet a fait une recommandation transmise au Ministre de la Famille¹⁰²¹, préconisant la sécurisation de la situation juridique des enquêteurs. Il faudrait leur permettre sous contrôle judiciaire d'avoir recours à une identité fictive et de réaliser des opérations de paiement pour accéder à certains serveurs de contenus pédopornographiques par extension du champ de la loi Perben II du 9 mars 2004 ou par une création de dispositions spéciales.

- La condition de double incrimination.

Elle sert de fondement juridique à un refus d'entraide, lorsque les faits à l'origine de la demande de l'Etat requérant ne sont pas réprimés par le droit pénal de l'Etat requis. Cela constitue un handicap insurmontable pour l'enquête. L'Etat peut opposer un refus direct à la demande d'entraide si conformément à l'article 2 (b) de la Convention du 20 avril 1959, il « estime que l'exécution de la demande est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de son pays ». L'article 30 de la Convention sur le cyberspace du Conseil de l'Europe reprend presque à l'identique cette formulation.

iii. Les limites géographiques.

Internet remet en question le principe de compétence territoriale des services d'enquête tel que posé par l'article 18 du code de procédure pénale : « *les officiers de police judiciaire ont compétence dans les limites territoriales où ils exercent leurs fonctions habituelles* ». La question se pose donc de déterminer dans quelle mesure un officier de police judiciaire peut récupérer par Internet des données utiles à l'enquête mais situées en dehors de sa juridiction. Si l'on considère que la récupération de données Internet intervient en dehors de la

¹⁰²⁰ LEGALIS.NET- Jurisprudence et actualité du Droit d'Internet

¹⁰²¹ Le Forum des droits sur Internet, Pédopornographie et pédophilie sur Internet, 25 janvier 2005, http://foruminternet.org/texte/activities_evenements/lire.phtml?id=96&PHPSESSID=5

circonscription de l'enquêteur, un dépassement de sa compétence territoriale doit respecter les exigences de l'article ci-dessus cité qui n'admet les extensions de compétence territoriale que de manière limitée¹⁰²².

Il existe une piste pour contourner les différents obstacles rencontrés par les cyber-enquêteurs, l'entraide répressive demeurerait mais tendrait de plus en plus à se dématérialiser.

- Les téléperquisitions : l'article 32 de la convention du Conseil de l'Europe n'admet les perquisitions que lorsqu'elles portent sur des données disponibles en libre accès ou lorsque celles-ci sont remises avec le consentement légal et volontaire de leur titulaire.
- La vidéoconférence prévue par l'article 10 de la convention d'entraide judiciaire de l'Union européenne du 29 mai 2000. Les Etats pourront substituer aux traditionnelles demandes d'entraide judiciaire des demandes d'auditions par webcams.
- Le point 33 des conclusions du Conseil de l'Union européenne de Tampere (15-16 octobre 1999) invite les Etats à permettre aux décisions judiciaires rendues par les Etats membres de produire des effets extraterritoriaux selon le principe de reconnaissance mutuelle (des Etats dont les systèmes juridiques satisfont aux mêmes règles fondamentales en matière de droits de l'Homme).

Ces dispositions n'ont qu'une portée limitée ; d'une part elles n'ont aucune valeur contraignante, d'autre part elles se circonscrivent à l'Union européenne (où de manière générale la coopération est plus aisée eu égard à des systèmes judiciaires similaires et à l'existence de l'Union européenne) et délaisse les Etats-Unis qui sont pourtant le système judiciaire avec lequel les conflits de loi sont les plus nombreux.

2-b. L'interdépendance des polices au niveau international.

Les infractions commises sur Internet ont un caractère transnational qui engage la compétence de plusieurs juridictions. Ce n'est pas la règle de droit quelle qu'elle soit qui est défailante mais les moyens d'appréhender les criminels¹⁰²³.

La cybercriminalité est un « *problème global grave qui nécessite, qui exige une réponse globale adéquate* »¹⁰²⁴. La cybercriminalité est rapidement apparue comme une criminalité

¹⁰²² Sous la direction de Georges Chatillon, Le droit international d'Internet, Actes du colloque, op.cit., p. 247.

¹⁰²³ Christiane Féral-Schuhl, Cyberdroit. Le droit à l'épreuve d'Internet, op.cit, p.664.

difficile à endiguer au seul échelon national. La mise en place d'une entraide internationale s'est révélée nécessaire¹⁰²⁵. En 1996 déjà, le Livre Vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, la Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions sur le contenu illégal et préjudiciable sur Internet¹⁰²⁶, ont attiré l'attention sur la nécessité d'instaurer une coopération entre Etats, notamment en matière de lutte contre la pédophilie sur Internet¹⁰²⁷. En matière de pédophilie, une harmonisation des législations est nécessaire, de même que le renforcement de la coopération judiciaire et policière internationale et une sensibilisation du public¹⁰²⁸.

Internet a ouvert un champ nouveau aux pédophiles : anonymat, sites difficilement traçables et domiciliés dans des pays légalement inaccessibles, facilités d'accès offertes par les forums de discussions, etc.¹⁰²⁹. Internet ne connaît pas de frontières matérielles, les enquêteurs nationaux qui ne prennent pas en compte cette caractéristique seront en peine de trouver à long terme des solutions aux enquêtes dont ils ont à connaître. La coopération internationale doit venir au secours des politiques de répression nationales. La coopération des polices nationales peut s'organiser de manière institutionnelle (c'est le cas d'Interpol par exemple) ou de manière ponctuelle pour la nécessité d'une enquête¹⁰³⁰.

2.b'. Le rôle d'Interpol dans la lutte contre la cybercriminalité.

Interpol s'est depuis de nombreuses années, attaqué à la cybercriminalité contre les enfants. Dès 1992, il initie le premier Colloque mondial sur la lutte contre les infractions dont sont victimes les enfants. En août 1996 Interpol participe également à la préparation du premier Congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales à

¹⁰²⁴ Propos tenus par Federico Mayor, alors directeur général de l'Unesco, s'agissant de la pédophilie dans le cyberspace.

¹⁰²⁵ S. El Zein, L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie in Les libertés individuelles à l'épreuve des NTIC, sous la direction de M.-C. Piatti, PUL, p.153 et s.

¹⁰²⁶ Livre Vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information. Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions sur le contenu illégal et préjudiciable sur Internet : Rev. DIT 1997/1, p.44 et s., observations S. Picard.

¹⁰²⁷ A. Lepage, Libertés et droits fondamentaux à l'épreuve d'Internet, préc., p.183.

¹⁰²⁸ C'est le constat fait par l'UNESCO dans la lutte qu'elle a engagé contre la cyberpédophilie. Il a été question un temps d'ajouter à la Convention des droits de l'enfant un protocole additionnel sur Internet, Fabrice Rousselot, L'Unesco veut traquer les cyberpédophiles, 19 janvier 1999.

¹⁰²⁹ Le Nouvel Observateur 5 juin 2003, Notre Epoque, Traque sur le Web, La grande pieuvre d'Internet, Hubert Prolongeau, p. 84-86.

¹⁰³⁰ Cette coopération a pu être mise en place dans des affaires aussi retentissantes que l'affaire Cathédrale

Stockholm. Il en sort une Déclaration et un Plan d'action mondial¹⁰³¹, qui aboutiront à une régionalisation de ses initiatives¹⁰³².

En mai 1997, un groupe de travail d'Interpol réunissant des policiers spécialisés de 25 pays s'est réuni à Salonique pour étudier la pornographie infantile sur Internet et remédier aux difficultés de la coopération policière. A la même date, une autre réunion regroupant des policiers de 31 pays se tenait en Norvège. Les Etats du G7-P8 adopteront au sommet de Washington, dix principes et un plan d'action pour lutter contre la criminalité de haute technologie¹⁰³³. Une série de rencontre se tiendront dans cette continuité : en 1999 à Séoul, en mai 2000 à Paris, juillet 2000 Okinawa. Les ministres de la justice et de l'intérieur du G8 évoqueront également la cybercriminalité lors d'une réunion à Milan en février 2001.

Il résulte de toutes ces initiatives une collaboration efficace entre les représentants de 29 pays réunis au sein d'un groupe de travail ; ces derniers mettent en commun leurs informations ce qui permettra l'opération « Cathédrale » en septembre 1998¹⁰³⁴.

En 1999 par la voix de Agnès Fournier de Saint Maur du Secrétariat général d'Interpol, a été annoncée la création du site d'Interpol axé sur trois secteurs :

- le premier secteur concernant les enfants disparus,
- le deuxième portant sur les abus sexuels avec une présentation des différentes législations en vigueur dans les pays,
- le troisième et dernier secteur étant réservé aux aspects confidentiels du travail d'Interpol avec une base de données pour informer les différentes polices travaillant sur des enquêtes¹⁰³⁵.

¹⁰³¹ Cette Déclaration et ce Plan d'action mondial visent à favoriser d'ici l'an 2000 la prévention des agressions, la protection des victimes, leur réinsertion sociale et la participation des jeunes à la mise en œuvre de ces actions.

¹⁰³² Dès 1997 se tient une Conférence internationale sur les crimes contre les enfants à Buenos Aires, elle est organisée sous les auspices de la Police Fédérale argentine. En collaboration avec les organes du MERCOSUR (Mercado Comùn Sudamericano), un Comité régional voit le jour pour que les forces de police des pays de la région s'unissent et s'organisent afin de mettre en place des structures spécialisées en coopération étroite avec le groupe de travail permanent Interpol.

¹⁰³³ Les principes adoptés prévoient [...] l'adaptation des législations répressives nationales, le renforcement des capacités techniques, l'amélioration de l'entraide judiciaire mutuelle, ainsi que l'engagement de ressources pour la formation et l'équipement des personnels d'enquête et la création d'un point de contact au niveau national chargé de recevoir les demandes d'enquêtes venues de l'étranger, voir Rapport CE, « Internet et les réseaux numériques, Doc.fr., 1998.

¹⁰³⁴ Réunion internationale organisée par l'UNESCO à Paris, les 18 et 19 janvier 1999, Henrikas Yushkiavitis, Sous-Directeur général pour la communication et l'information et l'informatique de l'UN, « Exploitation sexuelle des enfants, pornographie impliquant des enfants et pédophilie sur Internet : un défi international. – Vers un plan d'action à l'échelle globale » <http://www.unesco.org/general/fr/events/pedophilie/action.html>

En 2000 l'Américain Ronald Noble fraîchement nommé à la tête d'Interpol, avait affiché la volonté de cet organisme de se pencher sérieusement sur la cybercriminalité en dépit des décalages constatés entre les capacités technologiques et la législation¹⁰³⁶.

Parmi ses chantiers, Interpol compte mettre sur pied une équipe spéciale pour combattre la présence de pédophiles sur Internet qui créent de faux sites Internet pour embaucher des mannequins d'âge mineur. Il ne s'agit pas d'images ou de représentations pédopornographiques, mais plutôt d'appâts pour les enfants par le biais de leurs parents désireux d'en faire des mannequins. A l'occasion de la réunion de Paris sur les enfants disparus et sexuellement exploités qui s'est tenue à l'Élysée à l'initiative de Bernadette Chirac, le 17 janvier 2007, Ronald Noble, secrétaire général d'Interpol, a annoncé la création d'une cellule spéciale chargée de lutter contre les abus commis contre les enfants sur Internet. Pour ce faire, il a entrepris de mettre sur pied une équipe qui doit relayer les services de polices nationaux. L'équipe appelée « Projet Gardien »¹⁰³⁷ sera chargée d'enquêter sur les liens possibles de ces sites avec le crime organisé.

Une trentaine de cyberpédophiles ont été interpellés dans six pays d'Europe dont la France dans le cadre d'une opération internationale coordonnée par Europol en septembre 2005. Le coup de filet concernait environ 80 suspects en Italie, au Danemark, en France, aux Pays-Bas, en Suède et en Grande-Bretagne. Des ordinateurs, DVD, CD-ROM, cassettes vidéo et cartes de mémoires pour caméras numériques ont été saisis. Ce coup de filet fait suite à une opération baptisée « Icebreaker »¹⁰³⁸ les 14 et 15 juin 2005 à travers 13 pays européens et débouchant à l'interpellation de 150 internautes. Les suspects avaient recours à des techniques sophistiquées pour dissimuler les identités des membres du réseau et crypter leurs communications.

2.b". La coopération des polices nationales au cas par cas.

La coopération internationale des polices est le moyen le plus efficace d'appréhender la cybercriminalité dans toute sa dimension transfrontalière. Il est essentiel que les services

¹⁰³⁵ UNESCOPRESSE, Nouvelle réunion de l'UNESCO consacrée à la lutte contre la pédophilie sur Internet, Paris 22 juin 1999, <http://www.unesco.org/opi/science/vf/content/news/upresse/99-137f.htm>

¹⁰³⁶ Ronald Noble a dit à ce propos que : « *La technologie a pris des années-lumière d'avance sur la législation et sur le savoir-faire policier* ». Source Reuters, Yahoo ! Actualités, 3 novembre 2000, Jeremy Gaunt.

¹⁰³⁷ Cyberpolice.org ; Lundi 29 Janvier 2007, Les enfants, protégés par le gardien d'Interpol, <http://cyberpolice.over-blog.com/article-5446065.html>

¹⁰³⁸ Article paru le 14 juin 2005, Grande opération commune contre la pédophilie <http://www.tsr.ch/tsr/index.html?siteSect=200001&sid=5869297&cKey=1118759221000>

répressifs d'un Etat puissent effectuer des actes d'enquêtes pour le compte d'un autre Etat (lorsqu'il s'agit de preuves électroniques par nature volatiles), et les communiquent avec la célérité nécessaire¹⁰³⁹. L'entraide policière n'est qu'un des aspects de cette coopération internationale pénale, l'entraide judiciaire et l'extradition sont les autres éléments qui rendent toute coopération internationale efficace.

Depuis la fin des années quatre-vingt-dix, les polices nationales multiplient les occasions de collaborations tant en prévention de la commission d'infractions¹⁰⁴⁰ que pour des enquêtes¹⁰⁴⁰.

L'opération « cathédrale ». Il s'agit d'une opération de grande envergure qui a été déclenchée par vingt-et-un pays. Il s'agissait d'appréhender une centaine de personnes suspectées d'appartenir à un réseau de pédophiles diffusant des images sur Internet. Cette opération a été préparée sous le nom de code « Cathédrale » ; les modalités d'interventions avaient été mises au point lors de réunions entre les responsables des polices impliquées dans l'enquête. L'objectif était l'identification des cent cinquante à deux cents habitués du site baptisé « Wonderland Club ». Les principaux pays concernés étaient la Grande-Bretagne, l'Allemagne, les Etats-Unis, la France, l'Italie ; les autres pays impliqués étaient le Brésil, la Russie, l'Australie, la Belgique, la Finlande, la Norvège, le Portugal et la Suède. Une interpellation simultanée fut organisée le 2 septembre 1998 dans les 21 pays. Au total il sera procédé à une centaine d'arrestations simultanées, plus de cent mille clichés et des centaines de disquettes seront saisis.

L'opération « Cathédrale » est la conséquence du travail des douanes américaines ; dès 1996 lors du démantèlement du réseau « Orchid Club »¹⁰⁴¹, elles avaient pu établir un lien avec la Grande-Bretagne. La police britannique ayant pris le relais, elle a pu constater à son tour l'existence de réseaux internationaux, d'où la mise en place de cette coopération internationale qui aura conduit à ce gros coup de filet¹⁰⁴². La technique a eu un rôle prépondérant à jouer dans la réussite de cette opération internationale. L'utopie de l'anonymat

¹⁰³⁹ Sous la direction de Georges Chatillon, Le droit international d'Internet, Actes du colloque, op.cit., p.243.

¹⁰⁴⁰ Les 28 et 29 mai 1998 à Lyon, des experts (policiers et associations de lutte contre l'exploitation sexuelle des enfants) se sont retrouvés pour échanger des informations sur les actions contre la pornographie impliquant des enfants sur le réseau Internet. En septembre de la même année, s'est tenue à Munich une réunion internationale sur le même sujet et qui vise à mettre en place une coordination plus efficace. Enfin en octobre, se tient à Londres une conférence internationale sur l'exploitation sexuelle des enfants, elle réunit des experts de quinze pays européens et de dix pays d'Asie ; y est annoncé la création d'une librairie électronique à la disposition des afin de recenser toutes les images pornographiques impliquant des enfants proposés sur Internet.

¹⁰⁴¹ Cynthia Guttman, , Internet et la pédophilie, op.cit.

¹⁰⁴² Le Monde, 4 septembre 1998, Philippe Broussard, Un vaste réseau de pédophilie opérant sur Internet a été démantelé par les polices de vingt et un pays.

des internautes a joué en faveur des enquêteurs. Pour se connecter au réseau, les internautes doivent passer par un fournisseur d'accès auprès duquel ils s'acquittent d'un abonnement, ce faisant ils doivent décliner une identité à leur fournisseur, par ailleurs les paiements en ligne laissent également des traces pouvant à terme conduire à leur identification¹⁰⁴³. Les enquêteurs n'ont eu qu'à tisser leur toile pour récolter les données personnelles qui avaient été essaimées par les cybercriminels afin de remonter jusqu'à eux.

La technologie a un rôle prépondérant dans la cybercriminalité. Elle intervient en effet à tous les stades de l'acte cybercriminel. Elle peut servir la prévention de la cybercriminalité, elle peut servir à la commission de l'infraction. Enfin elle intervient après la commission de l'acte dans le cadre de l'enquête consistant en la recherche de preuves et de l'identification du délinquant¹⁰⁴⁴. La technologie est donc au même rang que les textes et les hommes, un instrument prépondérant dans la lutte contre la cybercriminalité contre les mineurs.

¹⁰⁴³ Le Monde, 4 septembre 1998, Michel Alberganti, Pas d'anonymat dans le cyberspace.

¹⁰⁴⁴ Olivier Iteanu, Tous cybercriminels. La fin d'Internet ? préc., p.214-215 ;

CONCLUSION

L'étude de la protection du mineur dans le cyberspace s'est articulée sur une double problématique visant à savoir si la spécificité du cyberspace et du statut juridique du mineur pouvait se suffire d'une réglementation par le droit préexistant, ou si il était nécessaire de recourir à un droit spécifique lié statut juridique du mineur dans le cyberspace.

Le Conseil d'Etat dans son rapport « Internet et les réseaux numériques » a dit d'Internet qu'il était un nouvel espace d'expression, renvoyant à diverses activités (commerce, édition, etc.). Il peut être appliqué à chacune des activités d'Internet un droit sectoriel tel qu'existant dans le droit commun¹⁰⁴⁵. Internet serait donc le point de convergence de (presque) tous les droits¹⁰⁴⁶. Ce faisant le Conseil d'état a clairement énoncé que pour sa part, Internet pouvait se satisfaire du droit existant et ne nécessitait pas la création d'un droit qui lui soit spécifique. Certaines activités inédites et spécifiques au cyberspace (telles certaines formes de cybercriminalité comme le téléchargement illégal) nécessitent un aménagement des textes existants ou la création de textes inédits. Pour le reste, les évolutions technologiques d'Internet supposent que certaines infractions sanctionnées par le droit commun puissent faire l'objet de l'aménagement de leur réglementation. La justification tient au fait que Internet est un facteur aggravant de ce type d'infractions (par exemple la diffusion de pornographie infantine) qui du fait de son utilisation, ont des effets plus dévastateurs.

Une réglementation optimale du cyberspace suppose que l'on recoure autant au droit commun, qu'à un droit spécifique à certaines matières du cyberspace. La protection des mineurs obéit à ce postulat.

Le mineur du fait de son statut juridique bénéficie de dispositions spécifiques et d'aménagements dans le droit commun. Le droit commun dans le souci de protection du mineur de son fait ou du fait d'autrui, restreint l'exercice et la portée des droits et libertés du mineur. Il est sous le tutorat de ses parents ou tuteurs légaux dans la majorité de ses activités, notamment celles de nature à engager sa responsabilité.

¹⁰⁴⁵ Internet et les réseaux numériques, Rapport du Conseil d'Etat, op.cit.

¹⁰⁴⁶ Ch. Debbasch, H. Isar, X. Agostinelli, Droit de la communication, op.cit.

La matérialité du monde “réel“ permet assez aisément de vérifier d’une part le statut de mineur, d’autre part qu’il dispose bien de l’autorisation parentale pour accomplir des actes de nature à engager sa responsabilité (c’est le cas notamment pour la conclusion de contrat et prise d’engagement de manière générale), enfin qu’il n’accède pas à des activités qui lui sont interdites (accès à de la pornographie par exemple). A l’inverse dans le cyberspace, la virtualité et l’anonymat ambiants de cet espace ne permettent pas facilement l’identification comme tel d’un mineur. Ce faisant les mécanismes les plus simples de protection des mineurs sont difficiles à mettre efficacement en œuvre.

Les mineurs ont une grande latitude d’actions dans le cyberspace, pour des actes ou non délictuels. En contradiction avec leur personnalité juridique le contraignant à une activité juridique restreinte, le mineur est (par la force des choses ou par défaillance technique) un internaute à part entière dans le cyberspace. Faute de moyens techniques restrictifs effectifs, le mineur a dans le cyberspace une activité similaire à celle d’un majeur. De ce point de vue, le véritable problème qui s’est posé n’était pas tant la réglementation juridique de son activité, que celle de l’identification du mineur comme tel afin que, puissent être mis en œuvre les dispositifs juridiques existants et visant sa protection. Cette identification est au centre de toute la problématique de la prévention et de la sanction de la cybercriminalité par et contre le mineur. Le droit commun n’a pas suffi à trouver une solution adéquate. En droit commun français il n’existe pas de droit spécifique aux mineurs, il existe des dispositions disparates traitant du statut du mineur. Il n’y a pas de code du mineur comme il existe un code de la propriété intellectuelle par exemple. Le seul texte dédié exclusivement aux enfants est un texte international : la Convention internationale des droits de l’enfant de 1989 dont les dispositions ne sont pas d’application directe dans les Etats. Le droit des mineurs n’existe pas dans la majorité des pays comme un droit spécifique, des dispositions spécifiques aux mineurs viennent parfois préciser un point de droit commun.

L’ampleur de la cybercriminalité contre les mineurs semble orienter les législateurs vers une codification du statut juridique du mineur dans le cyberspace. L’explosion de la cybercriminalité a eu pour effet de rendre les autorités étatiques et internationales prolifiques sur la régulation en matière de protection des mineurs dans le cyberspace. Le droit français a entrepris depuis quelques années d’aménager sa législation existante pour prendre en compte les spécificités du cyberspace et des délits mettant en cause des mineurs. Dans le même

temps il s'est doté de textes inédits spécifiques au cyberspace. Une part importante de ces travaux législatifs s'est faite sous l'impulsion de textes de l'Union européenne par le mécanisme de transposition.

Il existe un statut juridique du mineur dans le cyberspace, mais ce statut n'a pas d'entité propre. Le mineur peut poser des actes dans le cyberspace, mais sa responsabilité est limitée eu égard à sa personnalité juridique. Le statut juridique du mineur dans le cyberspace n'a de raison d'être que par les mesures juridiques, techniques et physiques qui l'encadrent afin que son intégrité physique et morale soit préservée.

Une insatisfaction demeure au terme de cette étude ; elle tient à la difficulté des Etats à s'accorder pour une répression unique et universelle de la cybercriminalité contre les mineurs. La technique n'est pas seule en jeu, il semblerait que la volonté politique y soit pour beaucoup. Les Etats s'accordent sur le principe d'une nécessaire répression, mais leurs moyens et leurs méthodes divergent. Peut-on espérer dans l'avenir voir émerger "Une" norme internationale régissant la matière, faisant l'unanimité des Etats au point qu'ils prennent les mesures pour qu'elle soit applicable de manière équivalente partout dans le cyberspace sans contingences frontalières ? Une telle disposition peut sembler utopique en l'état actuel du droit, mais elle ferait disparaître les paradis cybernétiques pour les cybercriminels tels qu'ils semblent exister (même) dans des pays démocratiques et soucieux des libertés. Une telle norme devrait s'accompagner d'institutions internationales (policières et judiciaires¹⁰⁴⁷) auxquelles les Etats auront « cédés » des parcelles de souveraineté. Le risque est que le cyberspace devienne un « Monde virtuel » à part entière coupé du monde réel, avec une réglementation propre, obéissant à des institutions qui lui seront propres, sans tutelle étatique.

La capacité d'évolution du cyberspace est très grande, elle n'appartient à aucun Etat, elle se joue des frontières et des limites juridiques et policières inhérentes à ces frontières. Avant qu'elle n'échappe complètement à toute ingérence étatique le risque d'une autorité et d'une réglementation internationale unique d'Internet serait-il la seule option pour garder un « contrôle relatif » sur les dérapages du cyberspace ?

¹⁰⁴⁷ Interpol et la Cour Internationale de Justice pourrait être adaptée, des services spécifiques créés pour s'adapter et se consacrer uniquement au cyberspace.

INTRODUCTION.....	9
PREMIERE PARTIE : LES DROITS ET OBLIGATIONS DU MINEUR DANS LE CYBERESPACE.....	24
Titre 1. LES DROITS ET LIBERTÉS FONDAMENTAUX DU MINEUR DANS LE CYBERESPACE.....	27
Chapitre 1. LES DROITS INDIVIDUELS DU MINEUR DANS LE CYBERESPACE.	31
§1. Les données personnelles du mineur dans le cyberespace.....	33
A. Le régime juridique des données personnelles dans le cyberespace.....	33
1. Les données personnelles : une valeur commerciale.....	34
1-a. Valeur économique.....	34
1-b. Objet patrimonial.	35
2. Les données personnelles, information à caractère personnel.	38
2-a. Les données personnelles électroniques et le service public.	39
2-b. Les données personnelles à vocation informative.....	41
2.b'. Les fichiers informatiques pour les besoins du fonctionnement d'une entreprise.	41
2.b''. Les données personnelles à vocation purement informative.	42
2-c. Les données sensibles du mineur : les données médicales.	45
B. Le traitement des données personnelles du mineur.....	46
1. La collecte des données personnelles des mineurs et auprès des mineurs. ..	48
1-a. La collecte directe.....	49
1.a'. La collecte par le biais des formulaires et jeux.	51
1.a''. La réglementation de la collecte des données auprès des mineurs.	52
1-b. La collecte indirecte.	56
1.b'. La collecte indirecte sur les forums de discussion.	57
1.b''. La collecte indirecte par le biais des traces électroniques.	59
i. Les cookies.	59
ii. La collecte par les données de connexion.....	61
2. Le transfert des données personnelles des mineurs.....	62
2-a. Le transfert des données personnelles du mineur au sein de l'Union Européenne.	63

2.a'. Le système de la loi informatique et liberté du 6 janvier 1978.	63
2.a''. Le système de la directive du 24 octobre 1995.	65
2-b. Le transfert vers les pays tiers.....	66
2.b'. Les pays tiers à protection « adéquate »	66
2.b''. Les systèmes dérogatoires de transfert de données en l'absence de protection adéquate.	71
i. Le recours à un cadre contractuel pour assurer la protection des données personnelles.	71
ii. Le compromis entre l'Union Européenne et les Etats-Unis : l'accord Safe Harbor	73
§2. Le droit à la vie privée du mineur dans le cyberspace.	78
A. L'image du mineur.	78
1. L'autorisation de diffusion de l'image du mineur.....	79
1.a. Les détenteurs du droit d'autorisation.....	80
1.b. La forme de l'autorisation.....	81
1.c. La preuve de l'autorisation.....	81
1.d. La finalité visée dans l'autorisation.....	82
1.e. Le délai de l'autorisation.....	82
2. Le droit à l'image et la particularité d'Internet : la webcam.....	83
2.a. Définition et origine.....	83
2.b. Le statut juridique de la Webcam.....	84
2.c. L'autorisation de diffusion et de reproduction de l'image par la Webcam.	84
B. La correspondance privée du mineur dans le cyberspace.....	87
1. Le droit commun : le droit à la correspondance privée du mineur.	87
2. La remise en question par la Loi pour la Confiance dans l'Economie Numérique de la détermination du courrier électronique comme correspondance privée.....	92
Chapitre 2. LES LIBERTÉS INDIVIDUELLES DU MINEUR DANS LE CYBERESPACE.....	97
§1. La liberté d'expression du mineur dans le cyberspace.....	97
A.Les manifestations de la liberté d'expression des mineurs dans le cyberspace. .	98
1. La liberté d'expression du mineur dans un espace public.	99

1-a. Les communications privées du mineur dans des espaces publics.	99
1.a'. Les pages ou les sites personnels.	99
1.a''. Le blog ou weblog	101
1-b. Les communications publiques du mineur.	104
2. La liberté d'expression du mineur dans un espace privé.	107
2-a. La correspondance électronique du mineur.	107
2.a'. Le courrier électronique.	107
2.a''. Les messageries instantanées.	108
2-b. La communication privée du mineur.	110
2.b'. La téléphonie via Internet.	110
2.b''. La Webcam.	111
B. Les limites à la liberté d'expression des mineurs.	112
1. L'autorégulation de la liberté d'expression sur Internet par le mineur.	112
1.a. La Netiquette.	114
1.b. La dénonciation ou notification de contenus illicites.	116
2. L'intervention des intermédiaires dans la liberté d'expression.	118
2.a. La charte de participation.	119
2.b. La modération.	119
2.b'. La modération a priori.	119
2.b''. La modération a posteriori.	120
2.c. La gestion des litiges par les organisateurs.	120
§ 2. La liberté créatrice du mineur : le droit d'auteur du mineur dans le cyberspace.	121
A. Les droits d'auteur du mineur dans la forme.	123
1. Les titulaires des droits d'auteur.	123
1-a. L'auteur.	123
1-b. Les créateurs.	125
2. Les objets du droit d'auteur.	126
2-a. Les supports numérisés.	126
2-b. Les supports numériques	129
B. La matière des droits d'auteur du mineur dans le cyberspace.	131
1. La nature juridique des droits d'auteur du mineur.	132
1-a. Les droits d'auteur, droits de la personnalité : l'aspect moral.	132

1.a'. Le droit au nom et à la paternité.	133
1.a''. Le droit de divulgation	133
1.a'''. Le droit au respect de l'œuvre.	133
1.a'''' . Le droit de retrait ou de repentir	133
1-b. L'aspect patrimonial du droit d'auteur	134
1.b'. Le droit de suite	134
1.b''. Le droit de reproduction	135
1.b'''. Le droit de représentation.	136
2. La mise en œuvre des droits d'auteur du mineur.	137
2-a. Le principe de la protection des droits d'auteur du mineur.	137
2.a'. La protection temporelle.	137
2.a''. La protection technologique.	137
2-b. Les exceptions du droit d'auteur.	139
2.b'. Les exceptions pour copies techniques	140
2.b''. Les exceptions d'utilisations privées.	141
2.b'''. Les exceptions d'utilisations publiques.	142
Titre 2. LA SANCTION JURIDIQUE DES DROITS ET OBLIGATIONS DU MINEUR DANS LE CYBERESPACE.....	143
Chapitre 1. LA CAPACITÉ JURIDIQUE DU MINEUR DANS LE CYBERESPACE.	144
§ 1. Le contrat électronique conclu par un mineur.	145
A. La validité des contrats électroniques conclus par le mineur.	147
1. La capacité juridique du mineur.....	147
2. La sanction de l'incapacité juridique du mineur.....	151
B. La validité intrinsèque du contrat électronique.	154
1. Le consentement du mineur dans un contrat électronique	154
2. L'effectivité de la formation du contrat électronique conclu par un mineur : le double clic.....	155
2.a. La vérification de la commande.	156
2.b. La confirmation de la commande.....	157
2.c. L'accusé de réception.	157
3. La sanction des contrats électroniques illégalement conclus par un mineur. .	158

§2. Les responsabilités du mineur découlant de l'exercice de ses droits et libertés fondamentaux dans le Cyberspace.....	158
A. La responsabilité pénale du mineur dans le cyberspace.	159
1. Le droit commun de la responsabilité pénale du mineur.....	160
1-a. L'âge de la responsabilité pénale.	160
1-b. Les mesures applicables aux mineurs.	161
1.b'. Les mesures éducatives.	161
1.b''. Les mesures de médiation – réparation.	161
1.b'''. Les mesures d'enfermement.	162
2. Les hypothèses de responsabilité pénale du mineur dans le cyberspace. .	162
2-a. Les infractions communes commises via Internet ou aggravées par l'utilisation d'Internet.	162
2-b. Les infractions spécifiques à Internet.	163
B. La responsabilité civile.	165
1. La responsabilité civile délictuelle ou quasi délictuelle du mineur dans le cyberspace.....	166
2. La responsabilité civile contractuelle du mineur dans le cyberspace.	167
Chapitre 2. LA SANCTION DES MANQUEMENTS DU MINEUR AUX DROITS D'AUTRUI DANS LE CYBERESPACE.	170
§1. Les infractions liées au statut d'auteur ou d'éditeur de contenus du mineur.	170
A. Les infractions de presse.....	172
1. La diffamation, l'injure.....	173
1-a. La diffamation.	173
1-b. L'injure.	177
2. L'apologie des crimes contre l'humanité et leur contestation.	179
2-a. L'apologie des crimes contre l'humanité.....	179
2-b. La contestation des crimes contre l'humanité.....	180
B. Les infractions par voie de presse.	182
1. La rumeur.....	182
2. Le montage de paroles et d'images.	185
§2. La criminalité informatique du mineur.	186
A. Le piratage informatique.....	186
1. Le « hacking » et les notions voisines.	187

1-a. Hacker.....	187
1-b. Les notions voisines.	189
1.b'. Les Crackers	190
1.b''. Les Script-kiddies	190
2. Le téléchargement illégal.....	191
B. Les nuisances informatiques.....	196
1. Le spamming et l'e-mail bombing.	196
1-a. Le spamming.....	196
1-b. L'e-mail bombing.....	198
2. La création et la diffusion de virus informatiques.....	200
DEUXIEME PARTIE : LES DROITS ET OBLIGATIONS DES TIERS A L'ÉGARD DU MINEUR DANS LE CYBERESPACE.	202
Titre 1. LES TUTEURS LÉGAUX RESPONSABLES DES MINEURS.	203
Chapitre 1. LES MOYENS DE PROTECTION DU MINEUR DANS LE CYBERESPACE.....	204
§1. La protection <i>a priori</i> du mineur dans le cyberspace.....	205
A. La sensibilisation.....	205
1. Les cibles de la sensibilisation.	205
1.a. La sensibilisation des mineurs aux dangers du cyberspace.....	206
1. b. La sensibilisation des parents et/ou tuteurs légaux aux dangers du cyberspace.....	207
1. c. La sensibilisation des éducateurs aux dangers du cyberspace.....	208
2. La nature et la forme de la sensibilisation.	209
B. Le contrôle parental pour la sécurité du mineur dans sa navigation dans le cyberspace.....	212
1. Une présence physique et dissuasive lors de la navigation.	213
2. L'utilisation de la technologie pour la prévention.	216
2-a. Les logiciels de filtres parentaux.....	217
2.a'. Les listes noires et les listes blanches	218
i. Le filtrage par liste blanche	218
ii. Le filtrage par liste noire	218
2.a''. Les filtres basés sur certains mots clefs	219
2.a'''. Le filtrage des intermédiaires du cyberspace	220

i. Le filtrage PICS des navigateurs.....	220
ii. Le filtrage des fournisseurs d'accès.	220
2.a'''. Les logiciels dédiés ou le filtrage basé sur les données.	221
i. Le filtrage basé sur les données : l'exemple du filtre mis sur pied par l'association Innocence en danger.	221
ii. Le logiciel Logprotect.	221
2.a'''''. Les filtres d'analyse des contenus et des images.....	222
2.a'''''''. Les filtres de contrôle d'applications.....	222
2-b. Les certificats électroniques.....	224
§2. La protection <i>a posteriori</i> du mineur dans le cyberspace.....	228
A. Une « atteinte justifiée » aux droits du mineur.	228
1. Atteinte à la liberté d'expression du mineur.	228
2. Atteinte aux droits à la vie privée et à la correspondance privée du mineur.	231
B. La dénonciation pour un cyberspace plus propre.	234
1. Les points de contacts généraux et spécifiques.....	234
2. La constitution en association.	237
Chapitre 2. LA RESPONSABILITÉ DES TUTEURS LÉGAUX DU FAIT DES MINEURS.....	240
§ 1. La responsabilité civile des tuteurs légaux du mineur.	240
A. Les conditions de la mise en cause de la responsabilité civile des tuteurs légaux.	240
1. Une responsabilité objective.	241
2. La cohabitation, condition de la légitimité de la responsabilité civile du tuteur légal du mineur.....	243
B. Les exceptions à l'engagement de la responsabilité civile des père et mère du mineur.....	244
1. La rupture de la condition de cohabitation avec les parents : le placement judiciaire du mineur.	244
2. La faute exonératoire de responsabilité de la victime.	245
§2. La responsabilité pénale des tuteurs légaux du mineur.....	246
A. La responsabilité pénale pour des faits commis par le tuteur légal en complicité avec le mineur.....	246

1.	Responsabilité selon le critère de la complicité.....	246
1-a.	La complicité par un acte volontaire des parents du mineur infracteur...	247
1-b.	La complicité objective des parents du mineur infracteur.....	247
2.	Le recel.....	249
B.	La responsabilité pour abstention du tuteur légal.....	250
1.	La négligence préjudiciable au mineur.....	250
2.	La charge morale des parents à l'égard des enfants mineurs.....	252
Titre 2.	LES RESPONSABLES DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE.....	254
Chapitre 1.	LA RESPONSABILITÉ DES INTERMÉDIAIRES DU FAIT DES CRIMES COMMIS CONTRE LES MINEURS DANS LE CYBERESPACE.....	255
§1.	Le régime de responsabilité de droit commun des intermédiaires techniques du cyberespace.....	256
A.	La détermination des intermédiaires techniques responsables dans le cyberespace.....	257
1.	Les fournisseurs de contenu.....	257
2.	Les fournisseurs d'hébergement.....	258
3.	Les fournisseurs d'accès.....	259
4.	Les exploitants de forums de discussion et les fournisseurs de moteurs de recherche.....	259
B.	La nature de la responsabilité des intermédiaires techniques.....	261
1.	La responsabilité civile des intermédiaires techniques.....	261
1-a.	La responsabilité sans faute.....	262
1-b.	La responsabilité pour faute.....	264
1.b'. L'obligation d'information.	264
1.b''. L'obligation de vigilance.	265
1.b'''. L'obligation de réaction.	265
2.	La responsabilité pénale des intermédiaires techniques : le principe de la responsabilité en cascade.....	268
2-a.	Le régime de la responsabilité en cascade.....	269
2-b.	Les limites de la responsabilité en cascade.....	270
§2.	Le régime spécifique de la responsabilité des Intermédiaires techniques dans le cyberespace : <i>la Loi pour la Confiance dans l'Economie Numérique (LCEN)</i>	271

A.	La responsabilité délictuelle pour faute caractérisée.....	273
1.	La responsabilité des hébergeurs.....	273
2.	La responsabilité des fournisseurs d'accès.	275
3.	La requalification de la responsabilité de l'organisateur de forum de discussion.....	276
B.	Une obligation minimum de surveillance pour certaines infractions.....	277
1.	Le devoir de vigilance pour les contenus illicites	279
2.	Le devoir de vigilance contre le délit de téléchargement illicite.	280
Chapitre 2. LA RÉPRESSION DE LA CRIMINALITÉ CONTRE LES MINEURS		
DANS LE CYBERESPACE.....		
§1.	La cybercriminalité à l'encontre des mineurs.....	287
A.	L'enfant spectateur de la cybercriminalité.	287
1.	L'incitation à la haine et à la violence.....	288
1-a.	Les crimes d'opinion.	288
	1.a'. Le révisionnisme et l'incitation à la haine raciale.	288
	1.a''. Les dogmes nocifs à l'intégrité physiques des mineurs.	289
	i. Incitation au suicide.	289
	ii. L'apologie de l'anorexie.	290
1-b.	Les contenus violents ou incitants à la violence.	291
	1.b'. Les contenus violents par nature.	291
	1.b''. Les contenus incitatifs à la violence.	293
	i. Incitation au crime	293
	ii. Incitation à la violence contre les autorités publiques et de police.	294
	iii. Incitation aux actes de terrorisme	294
2.	Les contenus choquants et illicites pour les mineurs.....	297
B.	L'enfant objet de la cybercriminalité.	301
1.	Le « commerce » des enfants en ligne.....	301
1- a.	“L'adoption en ligne“.	302
1-b.	Les réseaux de trafics de mineurs en ligne.	304
	i. Le tourisme sexuel impliquant des enfants.	305
	ii. Le trafic d'enfants en ligne à des fins sexuelles.	307
2.	La pédophilie sur Internet ou pédopornographie.	309

2-a. La pédopornographie « réelle ».....	311
2.a'. La participation à l'échange de pornographie infantine.	312
2.a''. La détention de pornographie infantine.	313
2-b. La « pseudo pornographie » infantine ou pornographie infantine virtuelle.	315
3. L'utilisation d'Internet facteur aggravant de la pédophilie.	316
§2. La sanction des cybercriminels.....	318
A. Les moyens de répression contre les infractions sexuelles commises sur le mineur.....	319
1. L'élaboration d'une réglementation répressive.....	319
1-a. Les textes internationaux.	319
1.a'. La Déclaration de Genève de 1924 sur les droits de l'enfant.	319
1.a''. La Déclaration des droits de l'enfant du 20 novembre 1959.	320
1.a'''. Le Pacte international relatif aux droits civils et politiques de 1966	320
1.a'''. La Convention internationale des droits de l'enfant du 20 novembre 1989.	321
1.a'''''. Convention sur la cybercriminalité.	322
1-b. Les textes communautaires	322
1-c. Les législations nationales.	326
1.c'. Les constantes dans les législations nationales.	326
1.c''. Belgique	328
1.c'''. Les Etats-Unis	329
1. c'''. France	333
2. Le rôle de la jurisprudence.....	338
2-a. Le travail d'interprétation et de sanction des juges.....	338
2-b. La jurisprudence en matière de pédopornographie sur internet.....	340
3. Les conflits des lois résultant des litiges nés dans le cyberespace.....	341
3-a. L'application du droit international privé.....	341
3-b. L'exequatur des décisions de justice rendues sur cyberespace pour les pays concernés.	343
B. La répression dans les actes.	345
1. La lutte spontanée de particuliers dans le cyberespace.	345

1-a. L'organisation et la dénonciation contre la cybercriminalité.	345
1-b. La légitimation du hacking au service de la lutte contre la cybercriminalité.....	347
2. La (les) police (s) contre la cybercriminalité.	349
2-a. La mutation du rôle de la police : les cyberpoliciers.....	349
2.a'. Les moyens mis à la disposition des policiers dans la lutte contre la cybercriminalité.....	351
i. L'utilisation de la technique.....	351
ii. L'acquisition de compétences technologiques.	352
iii. La perquisition électronique	352
2.a''. Les limites au travail des policiers dans leur lutte contre la cybercriminalité.....	354
i. Les limites d'ordre logistique.	354
ii. Les limites normatives.	355
iii. Les limites géographiques.	356
2-b. L'interdépendance des polices au niveau international.....	357
2.b'. Le rôle d'Interpol dans la lutte contre la cybercriminalité.....	358
2.b''. La coopération des polices nationales au cas par cas.....	360
CONCLUSION.....	363

I/ Ouvrages, monographies

ALBERGANTI Michel, Le Multimédia, la révolution au bout des doigts, Collection Marabout, Éditions Le Monde Poche, 1996.

ANDRIEU Olivier, Internet : Guide de connexion, Eyrolles, 1995

BAUDOUIN Jean-Louis et **DESLAURIERS Patrice**, La responsabilité civile, 6^e édition, Editions Yvon Blais, 2003.

BEAUCHE Gilles, Tout savoir sur Internet, ARLEA 1996.

BEAUDOUIN V. et **J. VELKOVSKA**, Un univers relationnel sur l'Internet : forum et pages personnelles en Comprendre les usages de l'Internet, sous la direction de **E. GUICHARD**, Editions Rue D'Ulm, 2001.

BEIGNER B., L'honneur et le droit, LGDJ, Bibliothèque de droit privé, Tome 234, 1995.

BENSOUSSAN Alain, Internet : aspect juridiques, HERMES 1997.

BILGER Philippe, Le droit de la presse, Que sais-je ? PUF 2003.

BITAN Hubert, Contrats informatiques, Paris : Litec - Juris-Classeur 2002.

BOCHURBERG Lionel, Internet et commerce électronique (site web, application multimédia, contrats, responsabilité, contentieux), Delmas 2001, 2^e éd.

BOURÉ Philippe, Le droit et l'Internet. Les enjeux présents et futurs de la société de l'information, Guides Essentiels Droit sous la direction de : Alain Chatty, Collection Doctrine, Textes et jurisprudence, 1^{ère} édition L'Hermès 2002.

BREESE Pierre, Guide juridique de l'Internet et du commerce électronique, Vuibert 1999.

CABRILLAC Rémy, **M.A. FRISON ROCHE** et **Th. REVET**, Libertés et droits fondamentaux, Dalloz 2006.

CAPRIOLI Eric A., Règlement des litiges internationaux et droit applicable dans le commerce électronique, Jurisclasseur Droit @ Litec2002.

CARBONNIER Jean, Droit civil Tome 2, La famille, l'enfant, le couple, Thémis Droit privé 21^e édition 2002.

CONTE Philippe, Droit pénal spécial, Litec, 2003.

DEBBASCH Charles, ISAR Hervé et AGOSTINELLI Xavier, Droit de la communication : audiovisuel, presse Internet, Editions Paris Dalloz 2002.

DELMAS-MARTY M. et C. Lucas de LEYSSAC, Introduction in Liberté et droits fondamentaux, Points Essais 2002.

DERIEUX E., Droit de la communication, LGDJ, 1999.

DETRICK Sharon, A commentary on the United Conventions on the rights of the child, Publication The Hague, M. Nijhoff Publishers, 1999.

DUFOUR Arnaud et GHERNAOUTI-HELIE Solange, Internet, Collection Que-sais-je? 2006.

FAVOREU L. et alii, Droit des libertés fondamentales, Dalloz 2002. 1ere édition.

FENOLL-TROUSSEAU Marie-Pierre et HAAS Gérard, Internet et protection des données personnelles, LexisNexis Litec 2000.

FERAL-SCHUHL Christiane, Cyberdroit. Le droit à l'épreuve de l'Internet, 3^e et 4^e éditions, Dalloz Dunod 2002 et 2005.

FINKIELKRAUT A. et P. SORIANO, Fatale liberté, Internet. L'inquiétante extase, Mille et Une nuits 2001.

FLORIDI Luciano, Internet, Paris Flammarion 1998.

FRAYSSINET J., Nouvelle technologies de l'information et de la communication et protection des libertés des consommateurs, Libertés individuelles à l'épreuve des NTIC, Lyon PU 2001

FUENTES-CAMACHO Teresa (Directrice de la publication), Les dimensions internationales du droit du cyberspace, Collection droit du cyberspace, Economica éditions UNESCO 2000.

GAUTIER P.-Y., L'e-mail in Clés pour le siècle, Université Panthéon-Assas-Paris II, D.2000.

GAUTRAND J., L'empire des écrans, Le pré aux clercs 2002.

GRALLA Preston et **KINKOPH Sherry**, Internet et les enfants, les précautions à prendre, Pearson Education, 2000.

GRENIER Jean-Guy, Dictionnaire d'informatique et d'Internet Anglais – Français, La Maison du dictionnaire Paris 2000.

GROUPEMENT FRANÇAIS DE L'INDUSTRIE DE L'INFORMATION, Sept clés juridiques pour Internet, AFNOR 1998.

GUEDON Jean-Claude, La planète Cyber, Découvertes, Gallimard Techniques 1997.

GUISNEL Jean, Guerre dans le cyberspace, La découverte 1995.

HIMANEN P., L'Ethique hacker et l'esprit de l'ère de l'information, Exils Editeur 2001

HUET J., La diversité culturelle sur le net, in Le droit de l'informatique au tournant du millénaire, sous la direction de Xavier Linant de Bellefonds, Publibook 2001.

HUET Pierre, **MAIS Herbert**, **HUET Jérôme** et **LUCAS André**, Le Droit du Multimédia, de la Télématique à Internet, AFTEL, Editions du téléphone 1995.

HUITEMA C., Et Dieu créa l'Internet, Eyrolles 1999.

HYDE Margaret O and **Forsyth Elisabeth H**, The sexual abuse of children and adolescent, A Millbrook Press Library, Edition Brookfield, Connecticut 1997.

FILLIEULE Renaud et **MONTIEL Catherine**, Pédophilie, Paris IHESI (Institut des Hautes Etudes de la Sécurité Intérieure) 1997.

INSTITUT DES RELATIONS INTERNATIONALES, Liberté, risque et responsabilité: nouveaux repères à l'heure de la mondialisation et du terrorisme international. Conférence organisée à Paris le 13 novembre 2001 par l'IFRI (Institut Français des Relations Internationales), Collection Cahiers et Conférences/ IFRI.

ITEANU Olivier, Tous cybercriminels, Jacques-Marie Laffont Editeur 2004.

JADOUL P., SAMBON J. et VAN KEIRSBLICK B., L'autonomie des mineurs, Publications des Facultés Universitaires Saint-Louis Bruxelles, 1998.

KAPFERER J.-N., Rumeurs. Le plus vieux média du monde, Seuil, Points 1995.

LAROCHE GISSEROT Florence, Les droits de l'enfant, 2^e Edition Dalloz 2003.

LARRIEU Jacques, Droit de l'Internet, Ellipses 2005.

LARROUMET Christian, Droit civil. Les obligations. Les contrats, Tome 3, Economica 3^e Edition 2003.

Le TOURNEAU Philippe, Contrats informatiques et électroniques, Dalloz Référence, 3^e Edition 2004.

LEPAGE Agathe, Libertés et droits fondamentaux à l'épreuve de l'Internet, Paris Litec 2002.

LINANT de BELLEFONDS Xavier, Le droit du commerce électronique, Que-sais-je ?, PUF 2005.

LUCAS A., J. DEVÈZE et J. FRAYSSINET, Droit de l'informatique et de l'Internet, Collection Thémis, Paris PUF 2001.

HALPERN Céline, Droit et Internet, Editions de Vecchi 2003.

MARTIN D. et F.-P. Martin, Cybercrimes : menaces, vulnérabilités et ripostes, PUF 2001.

MARTIN D., La criminalité informatique, PUF, 1997.

MARTIN-LALANDE Patrice, L'Internet un vrai défi pour la France, Paris La documentation française 1998.

MAYER Pierre et **Vincent HEUZÉ**, Droit international privé, Domat droit privé, Montchrestien 8^e édition 2004.

OLIVIER Frédérique et **BABRY Eric**, Le droit du Multimédia, Que-sais-je ? Numéro 3219, PUF 1996.

OUELLET Caroline, Que fait la loi sur Internet : censure ou liberté, droit et responsabilité, Canada, Les presses de l'Université Laval, 1998

PANSIER F.-J. et **JEZ E.**, La criminalité sur l'Internet, PUF 2000, collection « Que sais-je ? »

PANSIER Frédéric Jérôme et **JEZ E**, Initiation à l'Internet juridique, Litec 2000.

PIATTI Marie-Christine (Etudes réunies par...), Les libertés individuelles à l'épreuve des nouvelles technologies de l'information ou Les libertés individuelles et les NTIC, Presses universitaires de Lyon 2001.

PIETTE-COUDOL Thierry et **BERTRAND André**, Internet et la loi, Dalloz-Sirey 1996.

RAPP L., Le courrier électronique (E-mail), PUF 1998, collection « Que sais-je ? ».

RAYMOND Guy et **BARRETEAU-RAYMOND Christiane**, Droit de l'enfance et de l'adolescence : le droit français est-il conforme à la Convention internationale des droits de l'enfant ? 3^e édition Paris Litec 1995.

REGOUD Serge, Droit de la communication audiovisuelle, Paris PUF 2001

Rémy Cabrillac, Dictionnaire du vocabulaire juridique, Jurisclasseur, Litec 2004.

SEDALLIAN Valérie, Droit de l'Internet : réglementation, responsabilité, contrats, Collection Association des Utilisateurs d'Internet (AUI) Net Press 1997.

SIRINELLI P., Conclusion in *La Galaxie Internet. L'impératif de la conquête*, Edition Unicomm 1999.

TERRÉ F., La vie privée, in La protection de la vie privée dans la société de l'information, sous la direction de P. Tabatoni, PUF, 2002.

Travaux de l'association **Henri Capitant**, Le contrat électronique ; **Arnaud Raynouard**, La formation du contrat électronique, Journées nationales Tome V – Toulouse 2000, Edition Panthéon Assas, LGDJ.

TURNET Mark, UNESCO, Les droits de l'homme dans le cyberspace, Collection Droit du cyberspace, Mark Turnet, Economica 2005.

VIER Charlotte et **Ecole doctorale de droit public et de droit fiscal Paris**, L'Internet et le droit : droit français, européen et comparé de l'Internet, Victoire-édition PUF 2001, Légipresse.

WERY Etienne, Sexe en ligne : aspects juridiques et protection des mineurs, Droit des technologies, Larcier 2007.

WOLTON D. et **O. Jay**, Internet. Petit manuel de survie, Flammarion 2000.

II/ Articles

Articles de périodiques

HANS Julien, « Cookies et vie privée : le Conseil de l'Union Européenne adopte une position commune », 18 février 2002 <http://www.droit-technologie.org/actuality-511/cookies-et-vie-privee-le-conseil-ue-adopte-une-position-commune.html>

ADER B., « La loi de 1881 à l'épreuve d'Internet », Légipresse n°142, juin 1997. II.

AUVRET P., « L'application du droit de la presse au réseau Internet » JCP G 1999, I, 108, n°11.

AUVRET P., « La détermination des personnes responsables (Réflexion sur l'application de la responsabilité en cascade à Internet) », Gazette du Palais 12-14 mai 2002, p.17 et s., spéc., n°23.

BALASSOUPRAMANIANE Indragandhi, « *Une approche différente* », Le journal du barreau volume 33 n°19 15 novembre 2001.

BENOÎT-ROHMER F. ; « *La charte des droits fondamentaux de l'Union Européenne* ». Dalloz .2001 chronique. page.1423.

BERGHE Stéphanie et Laurent COHEN-TANUGI « *Droit d'auteur et copyright face aux technologies numériques : comparaisons transatlantiques* », Chroniques et opinions, p.4.

BIGOT Christophe, « *Connaître la loi de 1881* », Guide Légipresse 2004.

BISCHOFF Pierre, « *L'Union Européenne et la protection des données. La société de l'information à l'épreuve des droits de l'homme* », Revue du Marché Commun et de l'Union Européenne n°421, septembre 1998, page 538.

BOYER J., « *L'Internet et la protection des données personnelles et de la vie privée* », Cahier français, mars-avril 2000, p.74 et suivant, page 75.

CADOUX L., et **TABATONI P.**, « *Internet et protection de la vie privée* », Commentaires, printemps 2000, page 57 et suivant.

CHABAS, « *La réforme de la clause pénale* » Dalloz. 1976, chronique. page.229.

CHAMPEIL-DESPLATS V ; « *La notion de droit "fondamental" et le droit constitutionnel français* ». Dalloz.1985, chronique, page 323.

CHASSAING J.-F., « *L'Internet et le droit pénal* », Dalloz 1996, chronique, page 329, n°1.

Clic-Droit.com . Dossier du 30 mars 2004, « *L'interception des données sur le réseau d'une école* ».

DAMARTIN S., « *L'ordinateur, l'employeur et le salarié* », Droit social, juin 2000, p.580 et s.

De BELLESCIZE D., « *La loi du 29 juillet 1881 à l'aube de l'an 2000* » in *Clés pour le siècle*, Université Panthéon-Assas-Paris II, Dalloz 2000, p.1413 et s., spéc., p.1424.

De la LOYERE Georges, « *Quand les données personnelles traversent les frontières de l'Europe* », 30 mai 2005 – Tribune.

Dossier du forum des droits sur l'Internet, 18 juillet 2002, « *Les responsabilités liées à l'activité des forums de discussion* », Légipresse n°194, septembre 2002 IV 75

DREYER Emmanuel, Légipresse N° 214-septembre 2004, « *La responsabilité des internautes et éditeurs de sites à l'aune de la loi pour la confiance dans l'économie numérique* », p.92.

DREYER, « *Interrogations sur la responsabilité pénale des fournisseurs d'hébergement* », Légipresse juin 2004.

Droit et Nouvelles Technologies : Actualités. « *Au centre des débats actuels : la protection des mineurs sur l'Internet* », **Guillaume DESGENS-PASANAU** 24 Juillet 2001.

El ZEIN S., « *L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie* » in Les libertés individuelles à l'épreuve des NTIC, sous la direction de **M.-C. PIATTI**, PUL, p.153 et s.

FALQUE-PIERROTIN Isabelle; « *La liberté d'expression dans la société de l'information* », 15-16 novembre 2002 UNESCO.

GAUTIER P.Y; « *De la prescription des infractions commises sur l'Internet...et dans le monde physique* » Dalloz 2002, chroniques .p.1852.

GAUTIER Pierre-Yves, « *Du droit applicable dans le « village planétaire », au titre de l'usage immatériel des œuvres* », Dalloz 1996 I p.131

GRYNBAUM L., « *Contrats entre absents : les charmes évanescents de la théorie de l'émission de l'acceptation* », Dalloz 2003, chroniques, p. 1707.

HAUSS Patrick, « *Vie privée et communications électroniques : où en sommes nous ?* », avril 2006.

HUET A., « *Droit pénal international et Internet* », Petites Affiches 1999, n°224, p. 39 et s.

« *Internet et les réseaux numériques* » : Les études du Conseil d'Etat, La documentation française 1998, p.190.

« *Internet serait-il un no man's land juridique ?* » Lamy droit de l'informatique, n° 81 mai 1996 B p.1.

Le GUNEHCEK F., « *Aperçu rapide de la loi n° 98-468 du 17 juin 1998 renforçant la prévention et la répression des infractions sexuelles* », JCP G 1998, article. n°28.

LEJEUNE Ph., « *Cher écran...Journal personnel, ordinateur, Internet* », Seuil 2000 Le Monde des livres, 12 janvier 2001.

LOISEAU G., « *L'autonomie du droit à l'image* », Legicom n°20, 1999/4, p.71 et s.

LOUVEAUX Sophie, « *Comment concilier le commerce électronique et la protection de la vie privée ?* » Droit des technologies de l'information. Regards prospectifs, sous la direction d'Etienne Montero, Cahier du centre de recherche informatique et droit, Bruylant. Bruxelles 1999, p.151-152.

MARTIN-VALENTE Sophie, « *La place de l'article 1382 du code civil en matière de presse depuis les arrêts de l'Assemblée plénière du 12 juillet 2000* », Approche critique (2^e partie), Légipresse N° 203 – juillet/août 2003, p. 90.

MONTERO Etienne (Sous la direction de...), « *Droit des technologies de l'information. Regards prospectifs* » ; Cahier du centre de recherche informatique et droit, Bruylant Bruxelles 1999.

OLIVIER F. et **BARBERY E.** « *Des réseaux aux autoroutes de l'information : Révolution technique ? Révolution juridique ?* » J.C.P. 1996 éd. G I n° 3926.

PÉCHEUL A ; « *La charte des droits fondamentaux de l'Union européenne* ». RFDA.2001.P 688.

PELTIER Virginie, « *Le secret des correspondances* », PU Aix-Marseille, 1999.

RAPP L. « *Secret des correspondances et courriers électroniques* ». : D.2000 n°41, p.III.

REBUT D. « *Prescription des délits de presse sur l'Internet* », Légipresse, juin 2001, II-63.

SWETENHAM Richard, « *Le plan d'action pour une utilisation plus sûre d'Internet* », Société de l'information, NTI et Union européenne, Revue du Marché commun et de l'Union européenne n°436 mars 2000, p.161.

TÉSAR Yann et **TABAKA Benoît**, « *Loi pour la confiance dans l'économie numérique : un nouveau cadre juridique pour l'Internet* », Extraits du dossier du Forum des droits sur l'Internet, Légipresse n°213, juillet/août 2004, commentaire, p.68.

VERBIEST Th. et **Etienne Wéry**, « *La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés* », Légipresse, mai 2001, II-49.

VÉRON M., « *La responsabilité pénale du directeur de la publication. Infractions de presse et infractions par voie de presse* », Droit pénal, février 1996, chronique, p. 1.

WERY Etienne, 28 janvier 2004, « *L'Europe adopte une nouvelle décision pour mieux lutter contre la pédopornographie* ».

Articles de presses

ALBERGANTI Michel, Le Monde, 4 septembre 1998, *Pas d'anonymat dans le cyberspace*

ALBERGANTI Michel, Le Monde 4 mai 1999, *Yoann, dix-sept ans, informaticien professionnel grâce au piratage.*

ARTETA Stéphane, **M. Lemonnier**, **S. Noucher** et **C. Soula**, *Votre enfant et Internet, Comment suivre sa trace ?*, Le Nouvel Observateur, 22 novembre 2001.

BOUCHER Ph. *Safari ou la chasse aux Français*, Le Monde 21 mars 1974.

BRISSET Claire, Le Monde, 21 mars 2000, *Enfants vendus, enfants bafoués, enfants trahis*

BROUSSARD Philippe, Le Monde, 4 septembre 1998, Un vaste réseau de pédophilie opérant sur Internet a été démantelé par les polices de vingt et un pays.

CARDAN Claire, Télérama N° 2565-10 mars 1999, Les ados tissent leur Toile, p.88

CHAYETTE Sylvie, Le Monde, 5 juillet 2001, p.8, Grâce aux webcams, des « Loft Story » en miniature se jouaient déjà sur le Net.

COJEAN A., Le Monicagate, brûlot des médias américains, Le Monde, 13 février 1999, p. 15.

COUTY Marc, Le Monde de l'éducation, juin 1999, Cyberflic. Des policiers au Net

DORÉ Christophe, Des pirates français poursuivis par les Etats-Unis, Le Figaro, 30 avril 1998,

Dossier de Monde Interactif, 23 mai 2001, p. I à III, Rien n'arrête la rumeur sur la Toile

DUMESNIL Annette, Le Nouvel Observateur, 22 novembre 2001 ; Votre enf@nt et internet, S. Arteta, M. Lemonier, S. Noucher et C. Soula.

FARCHY Joëlle, Internet et le droit d'auteur. La culture Napster, CNRS communications, CNRS éditions 2003, p.116-117.

France 5. Les maternelles ; Dossier : Surveiller les enfants à tout prix : Webcams dans les crèches. Ce sujet de Sophie Pasquier a été diffusé dans l'émission Les maternelles du 17 avril 2003 (9h-10h30)

FROISSART P., Les images rumorales. Une nouvelle imagerie populaire sur Internet, Média Morphose, n°5, juin 2002, p. 27 et s.

GROSJEAN Blandine et **ROUSSELOT Fabrice**, Libération 13-14 janvier 2001, Quand la Toile rapièce les liens familiaux, p.2-4

KRAUSE J., Can anyone stop Internet porn? ABA journal, sept. 2002.

LAUNET Edouard, Libération 29 octobre 2003, Traquer les caméléons du Net

Le Monde 21 mars 2002, p. 18 et 23 ; Libération 26 mars 2002, p. 6 – 31 mars 2002, p. 4 et 6 ; Le Nouvel Observateur 28 mars et 3 avril 2002, p.68.

Libération, 19 mars 2002, p.30 ; Libération, 19 avril 2002.

MACHEREL Cathy en collaboration **WILLEMIN Nicolas** et **BLASSEL Frédéric**
Pirates : des crimes et des châtements, L'Hebdo n° 7 – 17 février 2000,
http://www.webdo.ch/hebdo/hebdo_2000/hebdo_07/hacking5_07.html

MARRIE M.C., *Internet, la loi et l'éthique*, MédiasPouvoirs, n°4, 1998, p.153.

MAUSSION Catherine, Libération, 9 juillet 1996, *Première intrusion de la Cnil sur l'Internet*, p.13.

PELLETIER Eric, *Police. SOS mineurs* L'Express.fr, 21 mars 2005

PROLONGEAU Hubert, Le Nouvel Observateur 5 juin 2003, *Notre Epoque, Traque sur le Web, La grande pieuvre d'Internet*, p. 84-86

RICHE Pascal, Libération 18 avril 2002, Etats-Unis : *la pédophilie virtuelle n'est plus un crime*.

ROUSSELOT Fabrice, *L'Unesco veut traquer les cyberpédophiles*, 19 janvier 1999.

SABATIER Patrick, *Le Net accusé d'incitation au meurtre*, Libération, supplément Multimédia du 16 avril 1999.

SCWARTZ John, *Votre Internet avec ou sans filtre ?* Courrier International n° 455 du 22 au 28 juillet 1999, p.34.

SIGAUD Marie, *Mineurs : un site pour les protéger*, Le Figaro 17 novembre 2001

WERLY Richard, *Offensive en règle contre la pédophilie*, Libération 21 décembre 2001.

Articles Internet

► **AMÉGÉE Maximilien**, La protection des mineurs sur Internet : la problématique de la pornographie www.themis.u3mrs.fr

► Article de Muriel Cahen paru sur le site Avocat Online, Quelles démarches accomplir pour poursuivre l'auteur d'une injure ou d'une diffamation ? Le droit de la preuve en la matière. http://www.murielle-cahen.com/p_forum2.aspp

► Article du 4 mai 2006, « Le blocage des paiement via les canaux bancaires habituels soutient la lutte contre la pornographie infantine sur l'Internet Child Focus se réjouit de la réaction positive des banques européennes,

<http://www.childfocus-net-alert.be/fr/BlocagePaiements.pdf>

► Article L.131-3 CPI.- Pierre Perez, Le droit d'auteur, <http://www.educnet.education.fr/jur/auteur1.htm>

► Bienvenu au Sénat, La responsabilité pénale des mineur , http://www.senat.fr/lc/lc52_mono.html

► **BONDOIS Nicole** et **SAMARCQ Nicolas**, Les Blogs, un service d'édition en ligne soumis aux mêmes règles que les sites Internet, source : BRM avocats

<http://www.droit-ntic.com/news/afficher.php?id=314>

► **BRIAT M.** et **PITRAT Ch. M.**, « Urgent : Concepts à clarifier »

http://www.dit.presse.fr/infolib/french/arti_pitrat.htm

► **CANEVET Sébastien**, Qui est l'auteur d'une œuvre ?, 18 janvier 2005: www.canevet.org/article.php3?id_article=24

► Capacité et incapacité. <http://www.notanamur.be/articles/CAPACITE.html>

► **CAZENEUVE Olivier**, Internet et diffamation. Existe-t-il une liberté d'expression de l'internaute ? 3 novembre 2005

http://reseaudesbahuts.lautre.net/article_print.php3?id_article=152

► *Charte d'engagement pour le développement de l'offre légale de musique en ligne*, 28 juillet 2004, www.culture.gouv.fr

► **CHASSIGNEUX Cynthia**, *La protection des données personnelles en France*, Lex Electronica, vol. 6, n°2, hiver 2001 <http://www.lex-electronica.org/articles/v6-2/chassigneux.htm>

► *Contrôle parental sur Internet :*
www.teteamodeler.org/conditionstravail/encadrement/controparent.htm

► *Courriels pornos : quand les juges trébuchent sur les liens*
<http://www.jursicom.net/actu/visu.php?ID=344>

► De **LUMBÉE Faustine**, **GAY Carole** et **CARVAIS Johanna**, e-Juristes, *Les atteintes à la dignité humaine sur Internet*, dans le cadre des cours de M. Ferry et de M. Neveu; 7 février 2005, http://www.e-juristes.org/article.php?id_article=669

► De **MARCO Estelle** et **Serge Aumont**, modérateurs FAQ de la liste droit-net: Communication électronique : publique ou privée ? : *Quelle est la nature juridique d'un message électronique?* 25 octobre 2004

► De **MARCO Estelle** et **Serge Aumont** ; Modérateur FAQ de la liste droit-net : Communication électronique : publique ou privée ? *Quelle-est la nature juridique d'une liste de diffusion?* 30 avril 2002

► **DIMEGLIO Arnaud**, Droit et Nouvelles Technologies : Actualités, *La France veut durcir sa position en matière de pornographie enfantine. Le grooming sera puni*
http://www.droit-technologie.org/1_2asp?actu_id=1238

► **DUSOLLIER S.**, Le site Droit & Nouvelles Technologies, *Internet et le droit d'auteur*, in Actualités du droit des technologies de l'information et de la communication, Formation Permanente CUP, février 2001 - Vol. 45, p. 161-220

http://www.droit-technologie.org/2_1.asp?dossier_id=56

► Exhaustif.com, « *Statistiques sur la pédophilie sur Internet* », publié le 21 juillet 2006, http://www.exhaustif.com/statistiques_sur_la_pedophilie_sur_internet-0225.actu.htm

► Forum des droits de l'Internet, « *Les Enfants du Net. Les mineurs et les contenus préjudiciables sur l'Internet* », 2004
http://www.foruminternet.org/telechargement/documents/reco-enfance1-20040211_2.pdf

► *Fourniture d'accès à l'Internet et responsabilité pénale*
<http://www.canevet.com/doctrine/resp-fai.htm>

► **GUERRIER Philippe**, *Issy-les-Moulineaux victime d'une rumeur sur Internet*. Journal Du Net <http://www.journaldunet.com/0102/010228issy.shtml>

► **GUTTMAN Cynthia**, journaliste au Courrier de l'UNESCO, *Internet et la pédophilie*.
http://www.unesco.org/courrier/1999_09/fr/connex:/txt1.htm

► *Internet et la liberté d'expression :*
www.cyberworkers.com/ledroit.fr/index_int_et_laliberte.shtml

► *Internet et les réseaux numériques*
<http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm>

► IRIS-MEDIATION, F.A.Q Conseils juridiques
<http://www.iris.sgdg.org/mediation/faqs/faq-conseil.html>

JAKUSIC Magali, *Historique de la loi sur la signature*.
<http://www.securite.teamlog.com/publication/3/4/53/index.html>

► *La loi du 29 juillet 1881 sur la liberté de la presse. Responsabilité et procédure :*
http://www.ddm.gouv.fr/article.php3?id_article=597

► *La nouvelle LCEN et l'école. Ce que la loi sur la confiance dans l'économie numérique change pour les utilisations de l'informatique à l'école*, 22 juin 2004, http://www3.ac-nancy-metz.fr/tice/imprimer.php3?id_article=427

► *La pédo-ponographie – La pornographie infantile*,
<http://users.swing.be/criminologie/contenus/.../pornodown.ht>

► La protection des données à caractère personnel dans le cadre du commerce électronique.

<http://www.ipr-helpdesk.org/docs.FR/personalData.html#N1004B>

► La protection des mineurs face aux sites pornographiques

<http://www.journaldunet.com/printer:juridique040203.shtml>

► La responsabilité des intermédiaires techniques.

<http://www.educnet.education.fr/legamedia/juriscol/fiche08.htm>

► La responsabilité pénale des mineurs, Le site du sénat.

<http://www.senat.fr/lc/lc52/lc525.html>

► Le droit à l'image, février 2004 <http://www.educnet.education.fr/juri/vieprivée/image.htm>

► Le Forum des droits sur l'Internet, Assurer la protection de l'enfant sur l'Internet,

05/09/2001, http://www.foruminternet.org/documents/en_pratique/lire.phtml?id=118

► Le Forum des droits sur l'Internet, Pedo-pornographie et pédophilie sur Internet, 25 janvier 2005,

http://foruminternet.org/texte/activities_evenements/lire.phtml?id=96&PHPSESSID=

► Le site du Défenseur des enfants, Interview de la Gendarmerie nationale, avril 2002,

<http://www.defenseurdesenfants.fr/actu/texte3h.htm>

► Les conditions de collecte des données.

<http://www.educnet.education.fr/juri/vieprivée/collecteA.htm>

► Les hackers ces inconnus, article publié le 24 mai 2003, http://crie-paca.org/article.php3?id_article=27

► Microsoft Sécurité ; 14 décembre 2004 ; Eviter le piratage en ligne à la maison : Apprenez à vos enfants à ne pas télécharger ou partager de films, de musique, ni de logiciels, illégalement

<http://www.microsoft.com/france/securite/gpublic/children/kidspiracy.mspx>

► **MUGNERE Eric**, 2 mars 2000, *A la Poste, le certificat numérique fera foi* : <http://www.transfert.net/a520>

► **Murielle Cahen** Article : *La protection des outils de référencement : l'articulation entre contrefaçon et concurrence déloyale*

http://www.murielle-cahen.com/p_referencement.asp

► **PERREAULT Charles**, *Logiciels de filtrage : pour ou contre ?* Infos rapides sur Juriscom.net le 26 janvier 2001 : <http://www.juriscom.net/actu/achv/200101.htm>

► **POIDEVIN Blandine**, *Le cadre juridique de la responsabilité des blogs*, 28 février 2006.

► **POULLET Yves**, *Les safe harbor principles – une protection adéquate ?* juriscom.net 17 juin 2000. Texte présenté lors du colloque de l'IFCLA, Paris, 15 et 16 juin 2000. <http://www.juriscom.net/uni/doc/20000617.htm>

► *Protection des données dans l'Union Européenne, Europe direct, Dialogue avec les citoyens et les entreprises*, p.3

http://europa.eu.int/comm/justice_home/fsj/privacy/guide/index_fr.htm

► *Protection des mineurs contre la pornographie et lutte contre la pédophilie sur Internet*. Source le site du Sénat : Bienvenue au Sénat, « Projet de loi relatif à la prévention de la délinquance. <http://www.senat.fr/rap/a05-477/a05-47713.html>

► *Protection et éducation des mineurs à la maison*,

<http://delegation.internet.gouv.fr>

► Responsabilité des hébergeurs : http://www.murielle-cahen.com/p_hebergeurs3.asp

► **RICCIO Giovanni Maria**, *La Cour de cassation crée une différence entre la diffusion de pédo-pornographie via chat room et via web*, 23 mai 2003, <http://www.droit-technologie.org>

► **SEDALLIAN Valérie**, Internet et droit d'auteur, article présenté lors des rencontres de la manifestation « *Autour du Libre 2002* » INT Evry 19.05.2002, paru sur le Site l'Internet juridique.

- ▶ **SÉDALLIAN Valérie**, *La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique*. <http://www.juriscom.net/pro/1/resp19990101.htm>

- ▶ Site du Sénat français : Bienvenue au Sénat, *La lutte contre la pornographie infantine*, Service des affaires européennes Mai 2001.

- ▶ **TABAKA Benoît**, Le Journal du Net, 19 juillet 2006, *LCEN : quel bilan deux ans après ?*, <http://journaldunet.com/juridique/juridique06719.shtml>

- ▶ *Téléchargement illégal : attention à la répression*. http://www.cyberjeune.org/ddj/44_telechargement.html

- ▶ Un article de Wikipédia, *Hacker*, <http://fr.wikipedia.org/wiki/Hacker>

- ▶ **VALLETEAU De MOULLIAC Delphine**, *Copyright et droit d'auteur - Définition de l'œuvre multimédia*, Avocats-publishing.com, 28 août 2004. <http://www.avocats-publishing.com/Qualifier-1-oeuvremultimedia-I-A>

- ▶ *Vengeances sur Internet* http://www.murielle-cahen.com/p_vengeances.asp

- ▶ **VERBIEST Th.** et **Etienne Wery**, 16 mars 2005, *Le dossier médical informatisé : la délicate protection des données personnelles*, voire les sites Sixi Soins Infirmiers et Informatiques et Droit et Nouvelles Technologies respectivement

- ▶ **WANG Fabrice**, Le Droit de l'Achat en ligne, *Un mineur peut valablement contracter, même lors d'un achat en ligne*, 30 novembre 2004, http://www.droitai.net/article.php3?id_article=18

- ▶ **WÉRY Etienne**, Source : Droit et Nouvelles Technologies : Actualités, *Pédopornographie sur l'Internet : la France et la Belgique classées meilleures élèves du monde !* 11 mai 2006, http://www.droit-technologie.org/1_2asp?actu_id=1178

IV/ Jurisprudence

Jurisprudence de première instance

Tribunal d'instance

TI Strasbourg 3 février 1998, RIDA avril 1998, n°176, p.410 ;

TI Paris 14 avril 1999, Gaz. Pal. 23-24 juillet 1999, p.38.

TI Puteaux, 28 septembre 1999 : Légipresse, janvier-février. 1999, III-19, note C. Bigot ;
Communication et commerce électronique Février 2000, commentaire n°26, obs. A. Lepage.

Tribunal commercial

Tribunal commercial. Paris, réf., 29 juin 2000 : Communication et commerce électronique
Septembre 2000, commentaire. n° 91, obs. J.C. Galloux.

Tribunal correctionnel

Tribunal correctionnel du Mans, 16 février 1998, Monsieur le procureur de la République c/
Philippe H. Réseaux pédophiles : JCP G 1999, II, 10 011, note J. Frayssinet.

Tribunal correctionnel 17^e ch. 2 novembre 2000 : jurisdata n°2000-139077 ; D. 2000, p.286 ;
Communication et commerce électronique. Janv. 2001, p.11

Tribunal correctionnel Lyon, 20 février 2001 : Comm. com. électr. Janvier 2002,
commentaire n°5, observation Ch. Le Stanc ; JCP E 2002, p.78, observations A. Bertrand-
Doulat.

Tribunal correctionnel de Paris 13^e chambre prononcé le 13 février 2002, Antoine C.
/ministère public, T., et de l'arrêt de la cour d'appel de Paris, rendu le 30 octobre 2002 dans
cette même affaire.

Tribunal de grande instance

TGI Paris 14 août 1996, Société Ed. Pouchenel, Brel et autres contre Ecole centrale de Paris
et autres ; Société Art Music France, Warner Chappel France et autres contre Ecole nationale

supérieure des télécoms et autres, Gabriel de Broglie, Le droit d'auteur et l'Internet, préc., p.34., RIDA janvier 1997, n°171, p.361

TGI Paris 5 mai 1997, JCP 1997.II.22906 ;

TGI Le Mans, chambre correctionnel, 16 février 1998, Expertises, juin 1998, N°216, p.194 ;
voire <http://www.droit-technologie.oeg> , rubrique « Jurisprudence

TGI Paris, réf. 9 juin 1998 : Dalloz affaires, p.1702, note F.-D. Golstein ; JCP E 1999, p.953,
obs. M. Vivant et Ch. Le Stanc.

TGI de Strasbourg, 7^e ch. corr., 27 août 1999, Procureur de la République et Sté Infonie c/M.
X, voir sur <http://www.juriscom.net>

TGI Puteaux, 28 septembre 1999, Axa/Infonie, www.legalis.net

TGI Nanterre, 1^{ère} ch., 8 décembre 1999 : L. Lacoste/Multimania, D. 2000, sommaire. p.274,
obs. C. Caron ; Communication et commerce électronique Mars 2000, commentaire n°40,
obs. A. Lepage ; JCP G 2000, I, 10279, note F. Olivier et E. Barbry. www.legalis.net

TGI Nanterre, réf., 31 janvier 2000, Les 3 Suisses, D. 2001, p.292 en annexe de l'article de G.
Haas et O. de Tissot, Communication et commerce électronique Juillet – août 2000,
chronique. P.16.

TGI Paris, 1^{re} chambre, du 3 mai 2000, « Lamy droit de l'informatique », Bulletin d'activité
n°125, mai 2000.

TGI Nanterre, 18 mai 2000 : Communication et commerce électronique, novembre 2000,
commentaire n°117, obs. J.-C. Galloux ; JCP E 2002, p.78, obs. A. Bertrand-Doulat.

TGI Paris Réf., 22 mai 2000 : Communication et commerce électronique. septembre 2000,
commentaire n°92, obs. J.-C. Galloux

TGI Paris 20 septembre 2000, Communication et commerce électronique Décembre 2000,
commentaire n° 131, obs. J.C. Galloux

TGI Paris, Ch. Presse 12 décembre 2000, Communication et commerce électronique. 2001, commentaire A. Lepage ; JCP E 2002, p.75, obs., C. Vivant.

TGI Paris 6 février 2001 : Communication et commerce électronique, Mai 2001, commentaire n° 50, observation. Ch. Le Stanc.

TGI Paris, 3ème chambre - 1ère section 23 mai 2001, *Monsieur S. P., PBME, Midi Musique, SPPI c/ Messieurs J. P., E. D., Grolier Interactive Europe, Free, Monsieur J.-L. H.*
www.juriscom.net

TGI Paris, réf., 30 octobre 2001 : Communication et commerce électronique janvier 2002, commentaire n°8, observation. Ch. Le Stanc.

TGI Meaux, 3^e ch. 19 novembre 2001 : Communication et commerce électronique. Février 2002, commentaire n°30, observation. A. Lepage ; D. 2002, sommaire. p. 2373, obs. C. Caron :

TGI Paris, 1ere ch., 1ere sect., 12 déc. 2001 : Communication et commerce électronique. Juin 2002, commentaire. n°92, obs. A. Lepage.

TGI Paris, réf., 4 janvier 2002 : Communication et commerce électronique Juin 2002, commentaire, n°93, obs. A. Lepage ; Légipresse 2002, n°190, III-63, note C. Rojinsky ; D. 2002, sommaire, p.2299, obs. C. Caron.

TGI Paris 17^e chambre 25 janvier 2002, Légipresse 2002-I, p. 26, n° 190-01.

TGI Paris, réf. 1^{er} février 2002, SA SPPI/T, www.legalis.net

TGI Paris, réf., 18 février 2002 : Communication et commerce électronique. Juillet.-août 2002, commentaire. n°102, obs. L. Grynbaum.

TGI Paris, 17^e ch. 26 mars 2002 : Communication et commerce électronique. Mai 2002, commentaire. n°78, obs. A. Lepage.

TGI Paris, 12^e chambre correctionnelle, 24 mai 2002 : www.01net

TGI Lyon, 28 mai 2002 : Communication et commerce électronique, Décembre 2002, obs. A. Lepage.

Tribunal de Grande Instance de Paris, 3ème chambre, 1ère section, 29 mai 2002, S.A. SPPI, Madame V. F. B., Madame S. C. F., Madame A. E. M. B.

<http://www.davidtate.fr/spip.php?article296>

TGI Toulouse, réf., 5 juin 2002 : Communication et commerce électronique, Septembre 2002, obs. L. Grynbaum.

TGI de Paris, Ordonnance de référé 12 mai 2003, Mlle Laure Pester dite Lorie c/ M. Géraume Schweitzer, Légipresse n°205, octobre 2003, commentaire Laurence Tellier-Loniewski (avocat au barreau de Paris, Cabinet Alain Bensoussan), p.150 et s.

TGI de Paris du 26 mai 2003, FSU et autres c/ La Droite Libre, www.legalis.net

TGI. Paris 17^e ch. 7 juillet 2003, Légipresse décembre 2003, n°207.III.196.

TGI de Paris, ordonnance sur requête, 3^e chambre, SCCP c/ Wanadoo, 8 octobre 2004, publié par le Forum des droits sur l'Internet le 10 janvier 2005.

TGI de Lyon, 14^e chambre, 21 juillet 2005 Groupe Mace c/ Monsieur Gilbert D., <http://www.foruminternet.org/texte/documents/jurisprudence/lire.phtml?id=1027>

Jurisprudence Cour d'appel

CA Colmar, 6 décembre 1957, Dalloz 1958, jurisprudence p.357, note P. Bouzat.

CA. Paris 14 mai 1975 : Dalloz 1976, J. 291 note Linon

CA Paris, 1^{ère} Ch., 6 octobre 1987, Polac c/ Romanet.

CA Paris, 14 décembre 1994,

CA Paris, 2 mars 1995, Droit pénal, 1995-121, observations Véron.

CA Paris 14^e ch. A 10 février 1999, Estelle Halliday / Valentin Lacambre, décision et commentaires sous : http://www.legalis.net/jnet/internet_illicites.htm voir également Gazette du Palais, 5-6 avril 2000, jur., p.19, not Christophe Caron ; JCP éd G, 1999, II, 10-101, note Eric Babry et Frédéric Olivier ; voir encore Légipresse n° 160, III, p.52 ; voir aussi Dalloz 1999, jur.p. 389, note Mallet-Pujol ; Communication Commerce Electronique 1999, commentaire, n°134, obs., R. Desgorces.

CA Paris chambre d'accusation 12 octobre 1999, inédit et TGI Paris, ch. presse, 10 janvier 2000, cités par E. Pierrat, Les infractions de presse sur l'Internet : Légicom, 2000/1 et 2, n°21-22, p.74 et s., spéc., p.75.

CA Paris, 11^e ch. A, 15 décembre 1999 : JCP G 2000, II, 10281, note Ph. A. Schmidt et V. Fachina ; Communication et commerce électronique, mai 2000, commentaire n° 58, 2^e esp., A. Lepage ; Rev. sc. crim. 2000, p. 644, obs., J. Francillon ; JCP E 2000, p. 1905, note N. Mallet-Poujol ; Légipresse, mars 2000, p.38 et s., note B. Ader.

CA Versailles, 12^e ch., 8 juin 2000 : JCP E 2000, p.1858, obs. N. Mallet-Poujol et M. Vivant ; Communication et commerce électronique Juillet-août 2000, commentaire. n° 81, obs. J.C. Galloux ; Légipresse, sept. 2000, p.139, note C. Rojinsky.

CA. Paris 15 mai 2001 : CCE novembre 2001, commentaire. n°118, note Lepage.

CA Aix-en-Provence, 30 nov. 2001: CCE janv. 2003, commentaire. n° 11, note Lepage

CA. Paris 14 février 2002, D.20 février 2002, J.2004.

CA. Versailles 21 mars 2002, sommaire. 2374 obs. Caron, Légipresse juillet-août 2002, n°193.III.137.

CA Paris, 13^e chambre, 2 avril 2002, E.L. c/Ministère public, D. 2002, p.1900, obs. C. Manara ; Communication et commerce électronique 2002, commentaire 111 et obs.

CA Bordeaux, 10 févr. 2003: JCP 2003. IV. 2991.

CA. Paris 6 novembre 2002 : CCE mars 2003, commentaire. n°32, note Lepage ; CA Paris, 11^e ch. A, 22 février 2005, B. G..., J. M..., Sté New Vidéo Production c/ le Ministère public,

Jurisdata n° 2005-275291 ; voir Commentaire. com. électr., oct. 2005, p. 41 s., obs. A. Lepage.

CA Pau, chambre correctionnelle, 17 mars 2005, PP/Ministère public, n°04/00683, Jurisdata n°273677 ; Lamyline Reflex 2 décembre 2005, p.5, obs. L. Costes ; RLDI 2005/11, n°299, p.28 ;

CA Paris, 11^e ch. A, 22 mars 2005, L. B.. c/ministère public et L. A..., Communication et commerce électronique Novembre 2005, p.37.

Jurisprudence Conseil d'Etat

CE 3 février 1956 Thouzellier, Recueil p.49

CE 19 décembre 1969.

CE 11 avril 1973, Département de la Marne. 11 avril 1973, Département de la Marne, T. p. 1105

Jurisprudence Cour de cassation

Cass. Assemblée plénière 9 mai 1984, Fullenwarth c/ Felten, Dalloz 1984.525.

Cass. 6 juin 2002 (3 arrêts)de la Cour de cassation, Dalloz 2002, jurisprudence p. 2750.

Chambre civile

Cass. Civ. 1^{ère}, 4 novembre 1970, JCP 1971 II 16631.

Cass. Civ. 2eme, 16 mai 1988, Gaz. Pal. 1989, 2 sommaire. 371

Cass. 2^{ème} civ. 19 février 1997, Bertrand, Bull. n° 55,

Cass. 1ere civ. 30 mai 2000: Bull. civ. I n°167.

Cass. 1^{re} civ. 5 juillet 2000 : Communication et commerce électronique commentaire. n°21, obs. A. Lepage.

Cass. Civ. I, 20 février 2001.

Cass. 1ere civ. 12 juillet 2001, D.2002, p.1380 note C. Bigot et sommaire p.2298, obs. L. Marino, Communication et commerce électronique, novembre 2001, commentaire. n°117, obs. A. Lepage.

Chambre sociale

Cass. soc. 2 octobre 2001 : Arrêt Nikon : D.2001, jurisprudence p.3148, - note P.Y Gautier, D.2001, sommaire, p.2296, obs., C. Caron ; Communication et commerce électronique. Nov. 2001, commentaire. n°120, obs. A. Lepage, JCP E 2001, p.1918, nute C. Puigelier ; JCP E 2002, p.73, observation M. Vivant et J.M. Bruguière; RTD civ., p.72, obs. Hauser ; Dr.soc. novembre 2001, p.915 et s., note J.E. Ray ; TPS 2001, commentaire. n°384, note P.Y. Verkind ; Droit et patrimoine 2002, n°101, p.112, note G. Loiseau.

Chambre criminelle

Cass. Crim., 26 avril 1890 : DP 1890, I, p. 454.

Cass. Crim., 18 janvier 1950, Bull. n° 23

Cass. Crim., 18 mai 1954, Bull. crim n°186

Cass. Crim., 5 janvier 1974, Bulletin criminel n°4.

Cass. Crim . 23 octobre 1978, Bulletin criminel n°284.

Cass. Crim 15 juillet 1981 Bull. Crim. n° 231 p.615

Cass. Crim., 1^{er} décembre 1981, Bulletin criminel n°320.

Cass. Crim., 15 novembre 1990, Ulla Bull. crim. N° 388

Cass. Crim. 17 novembre 1992 PPX et Neron,

Cass. Crim. 17 mai 1994 : Bull. n° 184.

Cass. Crim., 13 juin 1995 : Bull. crim., n°217

Cass. Crim. 10 octobre 1996, Dalloz 1997 jurisprudence, p.309

Cass. Crim. 26 mars 1997 Bull crim. n° 127

Cass. Crim. 8 décembre 1998, Expertises juillet 1999, p.234.

Cass. Crim., 8 décembre 1998, Légipresse n° 161-III, p.57

Cass. Crim. 30 mars 1999, Dalloz. 1999, IR 130

Cass. Crim. 12 septembre 2000, Droit pénal, 2001, paragraphe 4, observations Véron.

Cass. Crim. 10 octobre 2000 : Droit pénal 2001, p.16, n°2 observations M. Véron.

Cass. Crim, 16 octobre 2001 : Comm. com. électr. Décembre 2001, commentaire n° 132, observations A. Lepage ; Droit pénal février 2002, commentaire n°12, obs. M. Véron ; Légipresse, décembre 2001, III-205, note E. Dreyer.

Cass. Crim., 27 novembre 2001 : Comm. com. électr. Février 2002, commentaire n° 32, obs. A. Lepage.

Cass. Crim. 22 octobre 2002, Bull. n° 199

Cass. Crim., 18 juin 2003, voire Lamy droit de l'informatique et des réseaux, Bull. actualité, n° 163, novembre 2003.

Cass. Crim. 1^{er} octobre 2003, cité dans Lamy droit de l'informatique et des réseaux, Bulletin n°165, janvier 2004, p.17.

Cass. Crim. 9 novembre 2004, n°04-82.199, F-D, RLDI 2005, n° 101, p.38, obs. L. Costes.

Cass. Crim. 5 janvier 2005, MP/ J.L B.

Cass. Crim., 28 septembre 2005, n° 04-85.024, Lamyline Reflex 2 décembre 2005, p. 6 s., obs. L. Costes ; RLDI 2005/11, n° 300, p.38 s. ; Comm. com. électr. Mars 2006, p. 39, commentaire A. Lepage.

Jurisprudence Cour suprême des Etats-Unis

Cour suprême, Reno vs American Civil Liberties Union (ACLU) rendu le 26 juin 1997
www.courts.state.ny.us et www.foruminternet.org

Cour suprême du 16 avril 2002 Communication commerce électronique, juin 2002, act. p.5,
obs. P. Kamina.

V/ Documents

Mémoires, Thèses

De MARCO Estelle, « *Le droit pénal applicable sur Internet* », DEA Informatique et Droit sous la direction du Professeur Michel Vivant, Université de Montpellier 1 :
www.juriscom.net/uni/mem/06/crim01.htm

FAUREL Julien, « *La labellisation des sites Internet* », DESS Droit du multimédia et de l'informatique sous la direction de Gaël Kostic, Université Paris II – Assas 2000-2001

LABOURDIQUE Daphnée, Mémoire sous la direction de Madame le Professeur N. Mallet-Poujol, « *La protection des mineurs sur l'Internet : comparaison entre le droit français et le droit américain* », Université Panthéon Assas – Paris II, DESS Droit du Multimédia et de l'Informatique 2002-2003,

THOUMYRE Lionel, « *Abuses in the Cyberspace : The regulation of illicit messages diffused on the Internet* », Mémoire présenté en vue de l'obtention du diplôme ESST (European Society-Science-Technology) codéveloppé par l'Université Louis Pasteur de Strasbourg et la Faculté de Droit de Namur

MIGNARD Jean-Pierre, « *Cybercriminalité et cyber-répression entre désordre et harmonisation mondiale* », Université Paris I Panthéon Sorbonne

ORENGO E., « *La protection des personnes dans le cadre des flux transfrontières de données personnelles* », DESS droit de l'informatique et du multimédia sous la direction de Monsieur J. Huet, 2001-2002

Rapports, livres (blancs et verts)

ALVERGNAT Cécile, Rapport de la CNIL du 12 juin 2001, rédacteurs, Fatima Hamdi et Jean-Paul Macker, « *Internet et la collecte de données personnelles auprès des mineurs* », www.cnil.fr

De BROGLIE Gabriel, « *Le droit d'auteur et Internet* », Rapport du groupe de travail de l'Académie des sciences morales et politiques, Cahier des sciences morales et politiques, PUF 2001,p.31.

ELIE Michel, Le Forum des droits sur l'Internet, Rapport d'activité 2003, La documentation française, Michel Elie (Observatoire des usages de l'Internet) « *Quelle responsabilité pour les organisateurs de forums de discussion sur le web ?* » Recommandation adoptée le 8 juillet 2003, La documentation française

Le forum des droits sur l'Internet, Rapport d'activité 2003, La documentation française 2004, p.243.

Le Forum des droits sur l'Internet, Recommandation, « *Les enfants du Net (II) : Pédo-pornographie et pédophilie sur l'Internet* », 25 janvier 2005.

Le Forum des droits sur l'Internet-Fiches pratiques, « *Assurer la protection de l'enfant sur l'Internet* », 05 septembre 2001.

Rapport du Conseil d'état « *Internet et les réseaux numériques* », La Documentation Française, 1998 également disponible sous : <http://www.internet.gouv.fr/francais/index.htm>

TRUCHE P., J-P. Faugère et P. Flichy, Livre blanc ; « *Administration électronique et protection des données personnelles* », Rapport au ministre de la fonction publique et de la réforme de l'Etat, La documentation française 2002, p. 19.

Livre Blanc du groupe de travail audiovisuel et multimédia de 1994, voire page 7.

Livre Vert sur « *La protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information* ». Communication au Parlement européen, au Conseil, au

Comité économique et social et au Comité des régions sur le contenu illégal et préjudiciable sur Internet : Rev. DIT 1997/1, p. 44 et s., obs. S. Picard, spéc., p.45. J.-M. ORION, : Légipresse, juin 1997, II-72.

Rapport au premier ministre, La documentation française, Paris 1998, p.14. **BRAIBANT Guy**, « *Données personnelles et société de l'information* », Collection des Rapports officiels

RASSAT M-L., Droit pénal spécial, Ed. Dalloz 1997, p.550 « *La violence à la télévision* » : Rapport de Blandine Kriegel à M. Jean-Jacques Aillagon Ministre de la culture et de la communication.

Réunion internationale organisée par l'UNESCO à Paris, les 18 et 19 janvier 1999, Henrikas Yushkiavit Sous-Directeur général pour la communication et l'information et l'informatique de l'UN, « *Exploitation sexuelle des enfants, pornographie impliquant des enfants et pédophilie sur l'Internet : un défi international. – Vers un plan d'action à l'échelle globale* » <http://www.unesco.org/general/fre/events:pedophilie/action.html>

Rapport au Premier ministre, « *Du droit et des libertés sur Internet* », Christian PAUL, Collection des rapports officiels, La documentation française 2001, p.33.

Rapport CE, « *Internet et les réseaux numériques*, Doc.fr., 1998.

Rapport de Jean-Claude Merlin, Avril 1999, « *La Téléphonie sur Internet* », Rapport présenté par Jean-Claude Merlin, Ingénieur Général, Rapporteur, avec la collaboration de Pierre Fritz, Ingénieur Christian Malet, Inspecteur général ministère de l'Economie et des Finances et de l'industrie, SEI, Conseil Général des technologies de l'Information (CGTI)

Rapport de la mission interministérielle sur l'Internet, 16 mars-16 juin 1996, Isabelle Falque-Pierrotin, « *Internet. Enjeux juridiques* », La documentation française 1997.

Rapport de propositions remis à Marie-Josée Roig Ministre de la famille et de l'enfance, et à Léon Bertrand Ministre délégué au Tourisme, « *La lutte contre le tourisme sexuel impliquant des enfants* », http://www.famille.gouv.fr/rapports/tourisme_sex/rapport.pdf

Rapport de propositions remis à Philippe Douste-Blazy sous la Présidence de Joël Thoraval, « *Protection de l'enfant et usages de l'Internet* », Conférence de la famille 2005, p. 74

Rapport de propositions remis au Ministre de la famille et de l'enfance Marie-Josée Roig et au Ministre délégué au tourisme Léon Bertrand, « *La lutte contre le tourisme sexuel impliquant des enfants. Pour une stratégie française* », http://www.famille.gouv.fr/rapports/tourisme_sex/rapport

Rapport du Conseil d'état « *Internet et les réseaux numériques* », La Documentation Française, 1998, p.177, également disponible sous : <http://www.internet.gouv.fr/francais/index.htm>

Rapport du Conseil d'Etat, Internet et les réseaux numériques : La documentation française, Paris 1998, étude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998.

Colloques et conférences

Acte du colloque Paris 19 et 20 novembre 2001, Université Paris I Panthéon Sorbonne et l'Association ARPEGE, Le droit international de l'Internet sous la direction de Georges CHATILLON, Bruylant Bruxelles 2002 ; « *Internet et enquête judiciaire* » par Jean-Wilfrid Noël (Juge au Tribunal d'instance de Vanves), p. 248 ; « *La mise en application des décisions de justice* » par Christiane Féral-Schuhl, p.554.

CNIL, Délibération n°85-080 du 22 octobre 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 18 novembre 1985.

CNIL, Rapport d'activité 1996, La Documentation Française, p.92

Communication du Colloque « *La gratuité, une question de droit ?* » organisé les 26 et 27 avril 2000 par le Centre d'étude et de recherche : Fondement du droit public (Université de Cergy Pontoise et Paris X Nanterre) publié par les éditions de L'Harmattan en 2003, Paru sur le site de Sébastien Canevet « Le Chêne et le Gland » en date du 16 janvier 2005.

Conférence de la famille 2005, « *Protection de l'enfant et usages de l'Internet* », Rapport de propositions remis à Philippe Douste-Blazy, par le Président du groupe de Travail Joël Thoraval (Président de la Commission nationale consultative des droits de l'homme) et le rapporteur Olivier Peraldi (Adjoint au Délégué interministériel à la famille).

FALQUE-PIERROTIN Isabelle, Mission interministérielle sur l'Internet, « *Internet Enjeux juridiques* » : La documentation française, Paris 1997

FRAYSSINET Jean, « *L'Internet et la protection juridique des données personnelles* », Colloque International, l'Internet et le droit, Droit européen et comparé de l'Internet, 25-26 septembre 2000

« *Les enfants du net (I) : l'exposition des mineurs aux contenus préjudiciables sur l'Internet* ». Publication 11.02.2004.

LUCAS André (professeur à l'Université de Nantes) « *La responsabilité des différents intermédiaires de l'Internet* », Université Paris-I Panthéon-Sorbonne Ecole doctorale de droit public et de droit fiscal, Colloque International : L'Internet et le Droit sous le patronage du Sénat, du Ministère des Affaires Etrangères, du Ministère de l'Education nationale, du Ministère de la Recherche et de l'Académie des Sciences Morales et Politiques, http://droit-internet-2000.univ-paris1.fr/di2000_19.htm

UNESCOPRESSE, Nouvelle réunion de l'UNESCO consacrée à la lutte contre la pédophilie sur Internet, Paris 22 juin 1999, <http://www.unesco.org/opi/science/vf/content/news/upresse/99-137f.htm>

Textes communautaires

Décision n° 276/1999/CE, 25 janvier 1999 du Parlement européen et du Conseil, *Décision adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux* : JOCE n° L33, 6 février 1999, p.1 ; Légipresse, mars 1999, IV-29

Décision 2000/518/Ce de la Commission du 26 juillet 2000 *relative à la constatation du caractère adéquat de la protection des données personnelles en Suisse*, JOCE L.218 du 25 août 2000.

Décision 2000/519/Ce de la Commission du 26 juillet 2000 *relative à la constatation du caractère adéquat de la protection des données personnelles en Hongrie*, JOCE L.218 du 25 août 2000.

Décision cadre 2004-68-JAJ du Conseil du 22 décembre 2003 *relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie*, JO n° L13 du 20 janvier 2004, pp.44-48.

Décision de la Commission 2002/2/EC du 20.12.2002 - J.O. L 2/13 du 4.1.2002

Décision de la Commission 2004/411/CE du 28.4.2004 constatant le niveau de protection adéquat des données à caractère personnel dans l'Île de Man

Décision de la Commission C (2003)1731 du 30 juin 2003 - JO L 168, 5.7.2003

Décision de la Commission du 21 novembre 2003 sur la protection adéquate des données personnelles en Guernesey - J.O. L 308, 25.11.2003

Directive 1999/93/CE <http://www.marianne-village.fr/reglement/SMW00363.htm>

Directive 2000/31/CE, JOCE 17 juillet 2000, n° L 178, p. 1 et s. ; voir également Légipresse 172-IV, p. 51.

Directive 24.10.1995 n°95/46/CE du Parlement européen et du Conseil relative à la protection des données à caractère personnel et à la libre circulation de ces données, JO n°L.281, 23 novembre 1995.

Directive du 8 juin 2000, art. 11 point 2, article 1369-5 al. 1 nouveau inséré par ordonnance du 16 juin 2005, Document disponible sur le site : http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/1998_fr.htm

JOCE 10 janvier 2002 décision de la commission 2002/16/CE du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnels vers les sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE.

JOCE L.201, 31 juillet. 2002, p.0037-0047, voir P.-Y Gautier, le droit au respect de la « vie privée électronique » est en marche : Comm. Com. Electr. Octobre 2002, p.2 et 3.

JOCE n° L 270, 7 octobre 1998, p.48 ; Légipresse, novembre 1998, IV-99.

Textes nationaux

Avis n° 608, présenté par Mme Michèle Tabarot, Député, au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n°528) pour la confiance dans l'économie numérique, 11 février 2003, p.61.
www.assemblee-nationale.fr

Décret n° 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication publié au JORF du 16 mai 2000.

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, Journal Officiel Numéro 77 du 31 Mars 2001
http://www.legifrance.gouv.fr/citoyen/jorf_no.ow?numjo=JUS

Décision n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique

Délibération n°80-010 1^{er} avril portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés

Loi n°2004-575 pour la Confiance dans l'économie numérique du 21 juin 2004 parue au JO du 22 juin 2004.

Ordonnance n°2000-916 du 19 septembre 2000 article 3, Journal Officiel du 22 septembre 2000 entrée en vigueur le 1^{er} janvier 2002

VII/ Adresses des sites référencés

<http://ec.europa.eu>

<http://europa.eu.int>

<http://fr.wikipedia.org>

<http://interetsprives.grouperf.com>

<http://juriscom.net>

<http://listes.cru.fr/droit-net>

[http://padawan.info/fr/len/len et correspondance privée mise au point de mm ollier et di onis du sejour.html](http://padawan.info/fr/len/len_et_correspondance_privée_mise_au_point_de_mm_ollier_et_dionis_du_sejour.html)

<http://www.agessa.org>

<http://www.apeg.info>

<http://www.barreau.qc.ca>

<http://www.canevet.com>

<http://www.childfocus-net-alert.be/fr>

<http://www.childnet-int.org>

<http://www.clic-droit.com>

<http://www.cnil.fr>

<http://www.conseil-constitutionnel.fr>

<http://www.crin.ch>

<http://www.cybersciences.com>

<http://www.diplomatie.fr>

<http://www.dit.presse.fr>

<http://www.dit.presse.fr>

<http://www.droit-ntic.com>

<http://www.droitshumains.org>

<http://www.droitsurinternet.ca>

<http://www.droit-technologie.org>

<http://www.ecpat.net>

<http://www.edsb.ch>

<http://www.educaunet.org>

<http://www.en-droit.com>

<http://www.finances.gouv.fr>

<http://www.fntc.org>

<http://www.foruminternet.org>

<http://www.france5.fr/maternelles/parents/W00315/5/87165.cfm>

http://www.france5.fr/SCIENCES_NATURE/W00133/1/62478.CFM

<http://www.franceculture.com>

<http://www.info.fundo.ac.be>

<http://www.inhope.org>

<http://www.internautica.tm.fr>

<http://www.internenettes.fr>

<http://www.internet.gouv.fr>

<http://www.internet-juridique.net>

<http://www.internet-mineurs.gouv.fr>

<http://www.interpol.int>

<http://www.journaldunet.com>

<http://www.journalintime.com>

<http://www.jurisexpert.net>

<http://www.legalbiznet.com>

<http://www.llrx.com>

<http://www.loi-internet.org>

<http://www.murielle-cahen.com/>

<http://www.net-iris.com>

<http://www.senat.fr>

<http://www.sit.ulaval.ca>

http://www.sixi.be/Ledossier-medical-informatise-la-delicate-protection-des-donnees-personnelles_a245.html

<http://www.social.gouv.fr/>

<http://www.tice-hg.net>

<http://www.unesco.org/>

<http://www.unicef.org>

<http://www.web.net>

<http://www.webdo.ch/>

<http://www.wikipedia.org>

<http://www.wipo.int/copyright>

<https://www.internet-mineurs.gouv.fr>

www.actioninnocence.org

www.benchmark.fr

www.c-i-a.com

www.citizencard.com

www.cnil.fr

www.cnrs.fr/

www.credoc.asso.fr

www.culture.gouv.fr

www.cyberverify.com

www.droit-technologie.org

www.education-medias.ca

www.e-privacy.be

www.legalis.net

www.logprotect.net

www.net-dico.com

www.pointdecontact.net

www.safeinternet.be

www.u-paris2.fr/dess-dmi/rep_travaux/16_julienfaurel.pdf