UNIVERSITÉ
PANTHÉON-ASSAS
– PARIS II –

BANQUE DES MEMOIRES

Master 2 Droit de la Communication
Dirigé par les Professeurs Jérôme PASSA et Camille BROYELLE
2014

La protection de l'enfance à l'ère numérique

Anne DIOT

Sous la direction de Laurence FRANCESCHINI

Les opinions exprimées dans ce mémoire sont propres à son auteur et n'engagent pas l'Université Panthéon-Assas

SOMMAIRE

INTRODUCTION

« Nous disons : le futur homme, le futur travailleur ; le futur citoyen. Ce qui veut dire que la vraie vie, les choses sérieuses commenceront pour eux plus tard, dans un avenir lointain. […] Eh bien non, puisque les enfants ont toujours été et seront toujours. Ils ne nous sont pas tombés du ciel par surprise pour ne demeurer avec nous qu'un peu de temps. »[1]

La Convention Internationale des Droits de l'Enfant définit l'enfant comme « tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable »[2].
L'enfance et l'adolescence sont les périodes de la vie qui permettent à l'individu de se développer physiquement et psychologiquement, de construire et d'affirmer sa personnalité et sa réflexion. Ainsi, jusqu'à ce qu'il atteigne la majorité, l'enfant est considéré comme n'étant pas assez doué de réflexion pour pouvoir prendre des décisions seul. Sa fragilité et son immaturité requièrent qu'il lui soit accordée une protection particulière. Cette idée d'une protection spéciale a été consacrée pour la première fois par la Déclaration de Genève sur les droits de l'enfant du 26 septembre 1924. La Déclaration envisage ainsi que « l'enfant doit être mis en mesure de se développer d'une façon normale, matériellement et spirituellement »[3]. Il revient à ses parents d'assurer son bien-être, mais la société et les pouvoirs publics ont également un rôle à jouer dans la protection de l'enfant, notamment à l'heure de l'ère numérique.

Au sens strict, le numérique est un dispositif permettant de transformer des données, sons, images dans un langage universel exprimé en séries binaires de 0 et 1. Il est l'alternative qui s'est imposée face à l'analogique. L'emploi du terme « numérique » s'est ensuite généralisé et désigne désormais, dans l'esprit commun, le réseau Internet et les activités qui y sont menées[4].

[1] « Le droit de l'enfant au respect », J. Korczak, Ed. Laffont/Unesco, 1929, p 39.
[2] Article 1 de la Convention relative aux droits de l'enfant, adoptée par l'Assemblée Générale des Nations Unies le 20 novembre 1989 et entrée en vigueur le 2 septembre 1990.
[3] Article 1 de la Déclaration de Genève sur les Droits de l'Enfant.
[4] Pratiques de l'édition numérique, Michael E. Sinatra et Marcello Vitali-Rosati, collection « Parcours Numériques », Montréal, mars 2014

Les enfants sont nés avec Internet et maîtrisent de manière instinctive les technologies numériques. Cependant, ils n'ont pas toujours conscience des dangers présents sur ce réseau. Les enfants passent entre 3h40 pour les plus jeunes et 13h30 pour les plus âgés de leur temps par semaine à naviguer sur Internet[5]. Ils sont ainsi constamment exposés à des menaces diverses : contenus inappropriés (choquants, violents ou pornographiques), internautes malveillants, divulgation d'informations personnelles, harcèlement en ligne. En outre, et sans nécessairement le savoir, les enfants peuvent adopter des comportements répréhensibles sur Internet. Ainsi, ils engagent leur responsabilité lorsqu'ils portent atteinte aux droits d'autrui, et notamment au droit à l'image et au droit d'auteur.

Il est donc impératif de protéger l'enfant de ces dangers du numérique. Comment, dès lors, assurer la protection de l'enfance alors que les dangers du numérique sont variés, les contenus protéiformes, librement et facilement accessibles, les supports multiples ? Comment s'assurer qu'un enfant de 17 ans puisse jouir de plus de liberté qu'un enfant de 3 ans tout en bénéficiant du même degré de protection ? Comment, enfin, protéger l'enfance tout en garantissant le respect de la liberté de communication, liberté fondamentale consacrée respectivement par les articles 11 et 10 de la Déclaration des Droits de l'Homme et du Citoyen et de la Convention Européenne des Droits de l'Homme ?

L'organisation de la protection de l'enfance à l'ère numérique s'avère être délicate. Elle repose sur une réglementation fragmentée, qui appréhende les différents dangers encourus par l'enfant aussi bien dans son activité de spectateur du numérique (Titre I) que dans son activité d'acteur du numérique (Titre II).

[5] Junior Connect' 2015 : la conquête de l'engagement, Etude Ipsos, 7 avril 2015.

Titre I. L'enfant spectateur du numérique

L'encadrement des opérateurs intervenant sur Internet est nécessaire pour assurer la protection de l'enfance sur ce réseau (Chapitre I) mais il n'est pas suffisant à lui seul, devant être complété par des mesures visant les internautes et plus généralement l'éducation aux médias (Chapitre II).

Chapitre I. Réglementation et régulation des opérateurs

L'enfant est un gros consommateur d'Internet. Si cet outil peut apparaître indispensable, sa dangerosité est avérée, spécialement pour le jeune public. Naïf du fait de son jeune âge, l'enfant n'a pas toujours conscience du caractère choquant de certains contenus. Dans l'objectif de lui offrir une protection, le législateur impose aux services de médias audiovisuels (Section 1) aussi bien qu'aux services de communication au public en ligne (Section 2) des règles destinées à atténuer le risque d'exposition des enfants à du contenu inapproprié.

Section 1. Réglementation et régulation des services de médias audiovisuels

Les services médias audiovisuels, qu'ils soient linéaires (I) ou délinéarisés (II) doivent s'assurer que les contenus qu'ils diffusent sont respectueux de l'enfance.

I. Les médias audiovisuels linéaires

La loi du 29 juillet 1982 sur la communication audiovisuelle, dite loi Fillioud, a ouvert le secteur de la communication audiovisuelle à des opérateurs privés, mettant fin au monopole étatique[6].

Au sens de l'article 2 de la loi du 30 septembre 1986 relative à la liberté de communication, il faut entendre par communication audiovisuelle « toute communication au public de services de radio ou de télévision, quelles que soient les modalités de mise à disposition auprès du public, toute communication au public par voie électronique de services autres que de radio et de télévision et ne relevant pas de la communication au public en ligne telle que définie à l'article 1er de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que toute communication au public de services de médias audiovisuels à la demande »[7].

La communication audiovisuelle recouvre les services linéaires et les services délinéarisés. Les services linéaires sont ceux fournis pour le visionnage simultané de programmes sur la base d'une grille de programmes, qui implique une attitude

[6] Loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle.
[7] Article 2 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication (loi Léotard).

passive du spectateur[8]. Vulgairement, les services linéaires correspondent donc aux médias traditionnels, à savoir la télévision et la radio, mais également la web tv.

Le Conseil supérieur de l'audiovisuel est l'autorité indépendante qui garantit l'exercice de la liberté de communication audiovisuelle. Le CSA est doté de prérogatives diverses. Il est notamment chargé de veiller à la protection de l'enfance et de l'adolescence et au respect de la dignité de la personne par ces services[9]. Il est apparu nécessaire d'aménager la liberté de communication audiovisuelle afin de protéger l'enfance et l'adolescence. Cette nécessité a d'abord été consacrée au niveau communautaire. En effet, l'objectif de protection des mineurs a été consacré par la directive « Télévision sans frontière » du 3 octobre 1989.

Les dispositions communautaires ont été transposées en droit français par une loi du 1er août 2000[10]. Cette loi détermine les aménagements permettant de concilier liberté de communication et protection des mineurs. D'une part, les programmes mis à la disposition du public par les services de communication audiovisuelle ne doivent contenir aucune incitation à la haine ou à la violence pour des raisons de race, de sexe, de mœurs, de religion ou de nationalité. D'autre part, les programmes susceptibles de « nuire gravement » à l'épanouissement physique, mental ou moral des mineurs ne doivent pas être mis à la disposition du public. Enfin, les programmes susceptibles de « nuire » à l'épanouissement physique, mental ou moral des mineurs ne peuvent être mis à la disposition du public que s'il est assuré que les mineurs n'y ont normalement pas accès. Cette condition est par exemple remplie lorsque le programme est diffusé à une heure tardive. Le cas échéant, le CSA doit « veiller à ce que ces programmes soient précédés d'un avertissement au public et soient identifiés par la présence d'un symbole visuel tout au long de leur durée ».

Le CSA a donc été consacré comme garant de la protection des mineurs. Afin de mener à bien cette mission, le Conseil a publié le 5 mai 1989 une directive prônant une sorte d'autorégulation des opérateurs. Cette directive s'adresse aux éditeurs de services audiovisuels et « fait appel à la responsabilité éditoriale des chaînes

[8] Article 1 e) de la directive 2010/13/UE du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels.
[9] Article 15 loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.
[10] Loi n°2000-719 du 1er août 2000 modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.

publiques et privées »[11]. Elle fixe les grands principes que les chaînes doivent respecter pour garantir de manière efficace la protection des mineurs. Ainsi, il leur est demandé de ne pas diffuser de programmes à caractère érotique ou violent entre 6 heures et 22h30. Il faudra attendre 1996 pour avoir un dispositif national de classification des programmes audiovisuels. En effet, le 2 juillet 1996 le CSA a demandé aux différentes chaînes de l'époque, à savoir TF1, France 2, France 3, RFO, Canal + et M6, la mise en œuvre d'un système commun de classification des œuvres visible à l'écran. La signalétique anti-violence a ainsi été mise en place le 18 septembre 1996[12].

Le dispositif repose sur une classification des programmes. Il a été légèrement modifié en 2002[13] afin d'être plus compréhensible. Désormais, cinq catégories de programmes sont définies[14] :

- Catégorie I : programmes tout public, majeurs comme mineurs.
- Catégorie II : programmes déconseillés aux moins de 10 ans.
- Catégorie III : programmes déconseillés aux moins de 12 ans.
- Catégorie IV : programmes déconseillés aux moins de 16 ans.
- Catégorie V : programmes déconseillés aux moins de 18 ans.

A chaque catégorie est associé un pictogramme. Les pictogrammes des catégories III, IV et V doivent être visibles pendant toute la durée de la diffusion. En outre, la mention « déconseillé aux moins de … » ou « interdit aux moins de … » doit apparaître une minute avant le début du programme ou pendant le générique, et une minute après les interruptions du programme, ainsi que pendant les éventuelles bandes annonces du programme.

Si le dispositif de la signalétique s'adresse donc à toutes les chaînes, leur régime n'est pas le même. Ainsi, le régime des chaînes hertziennes diffusées en clair est le suivant :

[11] Directive du 5 mai 1989 relative à la protection de l'enfance et de l'adolescence dans la programmation des émissions diffuées par les services de télévision publics et privés.
[12] Les dix ans du CSA 1989-1999, CSA.
[13] Décision du CSA, Le CSA adopte une nouvelle signalétique, 17/09/2002.
[14] Recommandation CSA du 7 juin 2005 aux éditeurs de services de télévision concernant la signalétique jeunesse et la classification des programmes.

- Catégorie II : les programmes ne doivent pas être diffusés dans les émissions destinées aux enfants, les horaires précis de la diffusion étant laissés à la libre appréciation de la société.
- Catégorie III : les programmes ne doivent pas être diffusés avant 22 heures, sauf diffusions exceptionnelles réservées à des œuvres cinématographiques interdites aux moins de 12 ans lors de leur sortie en salle, dans la limite de 4 exceptions par an, et sous réserve que la diffusion n'intervienne pas avant 20h30.
- Catégorie IV : les programmes ne peuvent être diffusés qu'à partir de 22h30.
- Catégorie V : ces programmes font l'objet d'une interdiction totale de diffusion en clair.

Cette signalétique anti-violence a permis de mettre en place ce que le CSA appelle lui-même un régime de responsabilité partagée entre les diffuseurs et les téléspectateurs[15]. Les téléspectateurs ne peuvent ignorer le caractère violent ou choquant des programmes et il ressort de leur responsabilité de ne pas exposer les mineurs à de tels contenus. De leur côté, les diffuseurs sont chargés de classer les programmes qu'ils diffusent et ont la responsabilité de cette classification.

Afin d'assurer le respect par les opérateurs de leurs obligations, et donc notamment l'application de la signalétique jeunesse, le CSA a été doté de pouvoirs de sanction. Le CSA agit soit sur auto-saisine, soit sur plainte (plainte de particuliers, d'associations…). Le CSA vérifie alors la classification et peut mettre en garde les opérateurs après avoir constaté des manquements. Le cas échéant, il peut avoir recours à des sanctions législatives, conventionnelles et saisir le juge des référés[16]. Sans dresser de liste exhaustive, le CSA peut prendre des mesures à l'encontre des diffuseurs. Il peut ainsi mettre en demeure les chaînes de respecter leurs obligations[17], suspendre leur autorisation d'émettre[18], en réduire la durée voire la retirer[19].

[15] Article 22 alinéa 3 de la directive 97/36/CE du 30 juin 1997 modifiant la directive 89/552/CEE.
[16] L'évolution récente du régime des sanctions du Conseil supérieur de l'audiovisuel, JP Thiellay, AJDA 2003, p 475.
[17] Article 42 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.
[18] Article 41-1 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.
[19] Article 42-3 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.

Le CSA est donc chargé d'assurer que les contenus diffusés par les médias audiovisuels linéaires sont respectueux de l'enfance et ne sont pas de nature à lui causer un préjudice. Il dispose d'un pouvoir de contrôle similaire des contenus diffusés par les médias audiovisuels non linéaires, quoique adapté à la nature originale de ces médias.

II. Les médias audiovisuels non linéaires

Deux types de services de médias audiovisuels se distinguent : les services de radiodiffusion télévisuelle (services linéaires) et les services de médias audiovisuels à la demande (services non linéaires). Le critère distinctif réside dans la faculté de choix et de contrôle que l'utilisateur peut exercer[20]. Ainsi, « est considéré comme service de médias audiovisuels à la demande tout service de communication au public par voie électronique permettant le visionnage de programmes au moment choisi par l'utilisateur et sur sa demande, à partir d'un catalogue de programmes dont la sélection et l'organisation sont contrôlées par l'éditeur de ce service »[21].

Les services au public par voie électronique dont le contenu audiovisuel est secondaire sont exclus de cette définition. C'est-à-dire les sites web dont le contenu audiovisuel n'est qu'accessoire, à savoir par exemple les sites qui contiennent des spots publicitaires brefs[22]. Les sites qui fournissent ou diffusent du contenu audiovisuel créé par des utilisateurs privés à des fins de partage et d'échanges, les sites qui stockent ces contenus audiovisuels, et les sites dont le contenu audiovisuel est sélectionné et organisé sous le contrôle d'un tiers sont également exclus. Ainsi, les sites d'hébergement et les plateformes de partage telles que Youtube et Dailymotion ne sont pas considérés comme des services de médias audiovisuels à la demande (SMAD) et ne sont donc pas soumis à leur régime, ce qu'il conviendra d'approfondir au cours de cette étude. Enfin, les sites qui ne relèvent pas d'une activité économique au sens de l'article 256 A du Code général des impôts ne sont pas soumis au régime des SMAD. Les sites d'associations à but non lucratif en sont

[20] Article 2 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication (loi Léotard).
[21] Article 1 g) de la Directive 2007/65/CE.
[22] La culture de service public de radiodiffusion, Observatoire Européen de l'Audiovisuel, 2007, p65.

donc exclus, mais les Web TV institutionnelles des entreprises sont soumises à cette réglementation.[23]

La directive pose le principe d'une application distributive du régime juridique des SMAD. Ainsi, une entreprise qui proposerait à la fois un service relevant de la définition des SMAD et également un service, du type hébergement de contenus fournis par les utilisateurs, ne devra se soumettre au régime des SMAD qu'au regard de sa première activité.

Au terme de cette définition, il faut relever que les médias relevant du régime de la communication audiovisuelle sont donc essentiellement la télévision de rattrapage (TVR) et les vidéos à la demande, par abonnement (VaDA), payants à l'acte (VàD à l'acte) ou gratuit (VàD gratuite)[24]. La télévision de rattrapage permet de regarder, pendant une durée limitée, des programmes diffusés sur un service de télévision[25]

Le régime des services non linéaires a été aligné sur celui des services linéaires par la directive européenne 2007/65/CE du 11 décembre 2007, appelée « directive SMA »[26]. Ils doivent ainsi respecter le principe de protection de l'enfance. L'article 15 de la loi de 1986, modifiée, soumet les SMAD au contrôle du CSA. Le CSA ne requiert l'accomplissement d'aucune formalité préalable pour développer un service de médias audiovisuels à la demande. Il veille cependant à ce que soit respectée la protection de l'enfance et de l'adolescence dans les programmes mis à disposition du public par le service.
Le CSA a dû adopter des règles spécifiques pour les SMAD, car la particularité de ces services réside en l'accessibilité très facile du public à un très large choix de contenus audiovisuels. Les règles ont été adoptées par le CSA sous la forme d'une délibération le 14 décembre 2010 quant à la protection du jeune public applicable aux SMAD[27].

Comme pour les services linéaires, les services de médias audiovisuels à la demande doivent respecter et mettre en œuvre eux-mêmes une signalétique, composée d'un

[23] Quelle réglementation pour les Services de médias audiovisuels à la demande ?, JP. Roux, Gazette du palais, n°113, 23 avril 2009, p 14.
[24] Rapport au gouvernement sur l'application du décret n°2010-1379, novembre 2013, CSA.
[25] Article 1 du décret n°2010-1379 du 12 novembre 2010.
[26] SMA : Services de Médias Audiovisuels
[27] Délibération du CSA concernant la protection du jeune public, la déontologie et l'accessibilité des programmes sur les services de médias audiovisuels à la demande, 14 décembre 2010.

pictogramme rond et blanc indiquant les mentions « -10 », « -12 », « -16 » ou « -18 ». Cette signalétique doit être précédée d'une mention « Déconseillée aux moins de …ans ». Elle doit également apparaître sur tout ce qui a trait au programme: image, bande annonce, messages publicitaires… Les programmes sont répartis en 5 catégories.

- Catégorie 1 : programmes tout public, aucune signalétique
- Catégorie 2 : programmes ne s'adressant pas aux mineurs de -10 ans du fait de certaines scènes susceptibles de les heurter.
- Catégorie 3 : œuvres cinématographiques interdites aux -12 ans et programmes ne s'adressant pas aux mineurs de -12 ans lorsqu'ils sont susceptibles de les troubler en recourant à la violence physique ou psychologique.
- Catégorie 4 : œuvres cinématographiques interdites aux -16 ans et programmes érotiques ou de grandes violences ne s'adressant pas à des mineurs de -16 ans. Ces programmes ne peuvent être mis à la disposition du public de manière gratuite qu'entre 22h30 et 5h.
- Catégorie 5 : œuvres cinématographiques interdites aux -18 ans et programmes pornographiques ou d'une très grande violence ne s'adressant pas à des mineurs de -18 ans. Ces programmes ne peuvent être mis à la disposition du public que de manière payante, soit par abonnement soit à l'acte.

La délibération de 2010 prévoit également un espace « tout public », dit « espace de confiance » et un « espace réservé ». L'espace de confiance doit offrir un catalogue de programmes destinés à tous les publics. Les programmes de la catégorie V et ce qui y a trait (images, bande annonce, descriptifs…) ne doivent être mis à disposition du public que dans l'espace réservé. Cet espace réservé doit être verrouillé et uniquement accessible par un code personnel spécifique.
Une délibération du CSA de 2011 a précisé les modalités de configuration du code[28]. L'utilisateur abonné doit accéder à l'espace de gestion de son abonnement via un code de gestion. L'utilisateur non abonné doit renseigner un identifiant de paiement. Tous les utilisateurs doivent déclarer sur l'honneur être majeurs. Une confirmation

[28] Délibération du CSA relative à la protection du jeune public, à la déontologie et à l'accessibilité des programmes sur les services de médias audiovisuels à la demande, 20 décembre 2011.

de leur code personnel devra leur être envoyé par tout moyen approprié (courrier, sms, appel téléphonique). Les utilisateurs ne peuvent pas désactiver ce système de verrouillage.

Les SMAD sont donc désormais soumis à un régime proche de celui des services linéaires, bien que légèrement plus souple. Cependant, ce cadre juridique ne suffit pas à protéger efficacement le jeune public sur Internet. En effet, de nombreux opérateurs échappent à la définition des SMAD. Partant, le jeune public peut facilement avoir accès à du contenu qui ne leur est pas destiné et préjudiciable, par le biais de sites Internet de partage de vidéos en ligne qui échappent à la régulation du CSA.

Section 2. Réglementation et régulation des services de communication au public en ligne

A côté de la communication audiovisuelle s'est développée la communication au public en ligne. Il faut entendre par communication au public en ligne « toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur »[29]. L'Internet est le média phare de cette forme de communication, particulièrement apprécié du jeune public. Ainsi, 77% des adolescents se rendent sur Internet au moins une fois par jour[30]. Ils sont tout aussi nombreux à être potentiellement exposés à des contenus choquants ou violents. De fait, 43% des enfants de 11 à 13 ans et 68% des 15-17 ans déclarent avoir déjà accédé à un tel contenu[31].

Ainsi, comme il a été nécessaire de restreindre la liberté de communication audiovisuelle au regard notamment de l'objectif de protection de l'enfance, il a fallu limiter la liberté de l'Internet garantie par l'article 1er de la loi de 1986.

[29] Art 1 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[30] Perception croisée enfants/parents face à l'usage d'Internet, Etude menée conjointement par l'IFOP et EMC corporation, janvier 2013.
[31] « Enfants et Internet », baromètre Calysto, 2011.

La régulation de l'Internet ne repose pas sur l'intervention d'une autorité indépendante à l'image du CSA. Il y a bien trois autorités qui exercent un contrôle sur les contenus, l'ARCEP, l'HADOPI et l'ARJEL, mais elles n'ont compétence que sur des points bien particuliers et ce de façon limitée.
La régulation de l'Internet est fondée sur une limitation de l'accès des internautes mineurs aux contenus illicites ou inappropriés (I), dont l'efficacité est assurée par la responsabilisation des opérateurs du web (II).

I. Des mesures limitant l'accès à Internet

Plusieurs mesures existent afin de prévenir les internautes mineurs du contenu préjudiciable d'un site. L'éditeur du site peut mettre en place un signal sonore ou visuel d'avertissement. Il peut également prévoir un système de vérification de l'âge des utilisateurs. Ces mesures relèvent d'une forme d'auto-régulation des opérateurs du web. La principale mesure de protection de l'enfance sur les sites pornographiques est un disclaimer[32]. Le responsable du site annonce qu'il est interdit aux mineurs d'y accéder et demande à l'utilisateur de « déclarer sur l'honneur qu'il est majeur ». Le responsable du site se dégage alors de sa responsabilité. Cependant aucun contrôle d'âge n'est possible. Partant, les enfants ont facilement accès aux contenus du site qui ne leur est pas adapté au vu de leur jeune âge.

Il a été nécessaire de prévenir la dangerosité de cette navigation libre et solitaire des mineurs sur le net. Ainsi, un logiciel de contrôle parental (logiciel de filtrage) doit être mis à disposition des parents de manière gratuite et systématique, fourni dans le kit de connexion. Ce logiciel permet de filtrer les contenus du web, grâce à une labellisation des contenus qui est fonction des différents profils internautes paramétrés[33]. Les enfants ont accès à une liste blanche de sites autorisés. Il est ainsi possible de leur interdire l'accès à des contenus liés au sexe, à la violence ou encore à la haine raciale[34]. Une liste noire permet aux adolescents d'avoir accès à tout le web à l'exception de certains sites repérés et listés en fonction de critères prédéterminés. Enfin, la navigation est libre pour l'internaute adulte.

[32] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
[33] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.
[34] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.

Un système de contrôle parental peut également être mis en place pour la télévision par câble ou par satellite, ainsi que pour les téléphones mobiles. En effet, chaque opérateur de téléphonie mobile membre de la Fédération française des télécoms s'engage à proposer un outil gratuit de contrôle parental pour toute ouverture de ligne pour un enfant[35]. La mise en place de ce contrôle parental peut être demandée à tout moment à l'opérateur, par simple appel au service clientèle. Cependant, l'efficacité de cette fonctionnalité est à nuancer. En effet, d'une part, cette fonction est encore peu connue des parents. Le contrôle parental sur les téléphones mobiles n'est ainsi activé que pour 6% des enfants de 11 à 13 ans[36]. D'autre part, cette fonction n'est pas disponible lorsque la navigation de l'enfant sur le web se fait grâce à une connexion de son téléphone mobile à la wifi.

Des inconvénients similaires atténuent la portée des logiciels de filtrage sur Internet. Les parents, confrontés à des difficultés techniques quant à l'utilisation des logiciels, sont peu nombreux à les activer. En outre, le web est un espace infini, contenant des milliards de pages Internet, des nouvelles s'en créant par milliers tous les jours. Il est donc techniquement impossible de contrôler tous les sites et d'en restreindre l'accès au jeune public[37].

Les prestataires techniques de l'Internet (fournisseurs d'accès à internet et fournisseurs d'hébergement) n'ont aucune obligation générale de surveillance et de filtrage des contenus mis en ligne sur Internet. Cependant il est possible de les astreindre à un filtrage ciblé. La Cour de justice de l'Union Européenne, fondant son appréciation sur le considérant 47 de la directive, a ainsi jugé possible la soumission des prestataires techniques à des obligations particulières de surveillance et de filtrage, de certains utilisateurs et contenus déterminés, pendant un temps limité[38]. Cette activité de surveillance ciblée et temporaire peut être demandée par l'autorité judiciaire[39].

---

[35] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.
[36] « Enfants et Internet », baromètre 2011, Calysto.
[37] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
[38] Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage, E. Derieux, RLDI, 2012/81.
[39] Article 6-I-7 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Afin de ne pas avoir à recourir aux juges, et dans le but d'accélérer la paralysie du site, le législateur a prévu la possibilité de recourir au filtrage administratif des contenus pédo-pornographiques[40].
Les autorités administratives et judiciaires peuvent également exiger la prévention de tout dommage occasionné par le contenu d'un service de communication au public en ligne, ou qu'il soit mis un terme à de tels dommages en demandant aux prestataires techniques de procéder au retrait des informations illicites ou en rendant l'accès à ces dernières impossible[41].

A défaut d'avoir l'obligation de contrôler les informations qu'ils transmettent ou stockent, les prestataires techniques doivent concourir à la lutte contre les activités illicites et rendre publics les moyens qu'ils y consacrent[42]. A cette fin, ils doivent mettre en place des dispositifs de signalement, qui permettent à toute personne de porter à leur connaissance l'existence de contenus répréhensibles. Ces dispositifs doivent être facilement accessibles et visibles. Dès lors qu'ils en ont connaissance, les prestataires doivent alors informer promptement les autorités de ces activités illicites qui leur sont signalées. Ce système est efficace. Ainsi, 100% des contenus signalés ont été retirés par les hébergeurs français en 2011[43]. Ces dispositifs ont été particulièrement encouragés au niveau européen.
Très tôt, les Etats membres ont en effet été invités à développer l'auto-régulation afin que tous les acteurs et professionnels du secteur de l'information et de l'audiovisuel aident à la lutte contre les contenus illégaux[44]. Ils ont été incités à la création de plateformes de signalement, dites hotlines[45]. En France, l'AFA a été créée en 1997. L'AFA est un acronyme pour Association des Fournisseurs d'Accès et de Services Internet. L'AFA a crée un site Internet (www.pointdecontatc.net) pour recevoir tout signalement de contenus pédopornographiques, incitant à la haine raciale ou à la violence. Sa compétence a ensuite été entendue à l'ensemble des contenus choquants accessibles aux mineurs[46]. Pareillement, une plateforme gérée par l'Office central de lutte contre la criminalité liée aux technologies de

[40] Article 4 Art 1 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[41] Article 6-I-8 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[42] Article 6-I-7 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[43] Présentation du service de signalement en ligne des contenus choquants, AFA, 2012.
[44] Recommandation 98/560/CE du 24 septembre 1998 relative à la protection des mineurs et de la dignité humaine.
[45] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.
[46] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.

l'information et de la communication, rattachée au Ministère de l'Intérieur, recueille les plaintes des internautes via le site www.internet-signalement.gouv.fr. Lorsque les contenus sont hébergés à l'étranger, il faut s'en remettre à la coopération internationale, ou signaler les contenus via le réseau de prestataires européens « inhope ».

Globalement, il semble être admis que les mesures techniques ne peuvent, à elles seules, protéger les mineurs d'un contenu préjudiciable[47]. Cependant, il faut relever que ces mesures, à défaut d'être réellement efficaces, doivent être mises en œuvre et respectées par les opérateurs au risque de voir leur responsabilité engagée au regard de l'illicéité des contenus.

II. La responsabilité des opérateurs

Différents prestataires interviennent sur Internet. Le régime de responsabilité qui leur est applicable est fonction de leurs caractéristiques et de leur action sur le web.

L'article 6-III-1 de la LCEN définit l'éditeur comme étant la personne « dont l'activité est d'éditer un service de communication au public en ligne », que ce soit à titre professionnel ou non. L'éditeur est en quelque sorte la personne responsable du site[48]. Il a un rôle actif quant à la gestion du site. C'est au regard de sa maîtrise éditoriale qu'a été développé le régime juridique qui lui est applicable. L'éditeur a une obligation d'identification et de transparence. Ainsi, il doit tenir à disposition du public ses nom, prénom domicile lorsqu'il est une personne physique, dénomination ou raison sociale et siège social lorsqu'il s'agit d'une personne morale. En sus, la loi leur impose de désigner le directeur de publication. Cette désignation va permettre de déterminer le responsable juridique. En effet, le principe est celui d'une responsabilité en cascade[49]. Le directeur de la publication est responsable de tout contenu illicite publié sur le site. A défaut d'un directeur de publication, l'auteur du contenu est désigné responsable. La responsabilité de l'éditeur est engagée in fine lorsqu'il n'est pas possible de désigner l'auteur.

---

[47] « Protéger les enfants dans le monde numérique », Rapport de la Commission au Parlement européen, au Conseil, au comité économique et social européen des régions, 2011.
[48] Contrefaçon et sites communautaires : état des lieux jurisprudentiel, C. Caron, communication commerce électronique, 2007, p143.
[49] Article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle.

Ce régime de responsabilité est justifié par la possibilité qu'a l'éditeur de contrôler les contenus. Ce régime était dès lors difficilement transposable aux prestataires intermédiaires, à savoir les fournisseurs d'accès à Internet et les fournisseurs d'hébergement, pour qui il est quasiment impossible de contrôler les contenus qu'ils transmettent ou stockent[50].

Le fournisseur d'accès à Internet (FAI) est la personne « dont l'activité est d'offrir un accès à des services de communication au public en ligne »[51]. L'article 12 de la directive de 2000 a posé le principe de l'irresponsabilité sous condition des FAI. Ainsi, l'article L 32-3-3 du code des postes et des télécommunications dispose que les FAI ne sont ni civilement ni pénalement responsables des contenus qu'ils transmettent. Cependant, ils ne peuvent pas se prévaloir de cette irresponsabilité dès lors qu'ils sont à l'origine du contenu litigieux, qu'ils ont sélectionné les destinataires de l'information ou qu'ils ont modifié les contenus ainsi transmis. Pour bénéficier de leur régime d'irresponsabilité, les FAI doivent donc être neutres.

Les prestataires de « caching » et les fournisseurs d'hébergement jouissent d'un régime d'irresponsabilité similaire. Le caching est un service de stockage automatique, intermédiaire et temporaire de l'information dans le seul but de rendre plus efficace sa transmission ultérieure[52]. Les prestataires de caching sont irresponsables dès lors qu'ils n'ont pas modifié l'information, qu'ils se sont conformés aux conditions d'accès de l'information et aux règles en concernant la mise à jour, qu'ils n'entravent pas l'utilisation licite de la technologie et qu'ils agissent promptement pour retirer le contenu illicite qui leur a été notifié.

A la différence des prestataires de caching qui fournissent un service de stockage temporaire de l'information, les fournisseurs d'hébergement assurent un stockage permanent des contenus. L'hébergeur est la personne ou la société dont l'activité est de stocker, même à titre gratuit, des signaux, écrits, images, sons ou messages de toute nature fournis par les utilisateurs[53]. L'hébergeur n'est pas responsable du contenu stocké s'il n'avait pas effectivement connaissance de l'illicéité du contenu. Il peut être déclaré responsable s'il n'a pas agi promptement pour retirer les

[50] La responsabilité en matière d'internet, M. Boizard, Droit et patroimoine, 2001.
[51] Art 6-I-1 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[52] Article 13 de la directive 2000/31/CE sur le commerce électronique.
[53] Art 6-I-2 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

informations ou en rendre impossible l'accès[54]. Certaines décisions jugent qu'une action prompte équivaut à une action le jour même de la connaissance des faits, mais cette solution ne fait pas toujours l'unanimité[55]. La connaissance des faits litigieux est présumée acquise dès lors que les prestataires en ont eu la notification[56], d'où l'obligation pour les opérateurs de mettre en place un dispositif facilement accessible et visible de signalement. La notification, pour être valable, doit mentionner les éléments listés par la loi, à savoir notamment la date de la notification, l'identité du notifiant, la description des faits litigieux et leur location précise, les motifs pour lesquels le contenu doit être retiré[57]. Les juges ont considéré que le demandeur doit signaler une nouvelle fois l'existence du contenu illicite à l'hébergeur afin que ce dernier procède, de nouveau, à son retrait. L'hébergeur n'est donc pas responsable de la remise en ligne tant que celle-ci ne lui a pas été notifiée.

La neutralité des prestataires leur permet d'échapper à leur responsabilité car le principe de neutralité du net a vocation à garantir la liberté des destinataires ou utilisateurs du réseau, et s'oppose donc à toute intervention ou contrôle des prestataires techniques[58]. Cependant, avec l'essor du réseau Internet, le web collaboratif et contributif, (web 2.0), s'est intensivement développé. Il permet aux utilisateurs de déposer des contenus sur le net et de consulter ceux déposés par d'autres internautes. Sont ainsi apparus, avec succès, des sites de partage de vidéos comme Dailymotion ou Youtube. Ces plateformes de vidéo en ligne correspondent à une activité de commerce électronique telle que définie par la LCEN. Une activité de commerce électronique est une « activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent »[59]. Cependant, elles n'ont pas été appréhendées par la loi. La qualification d'hébergeur s'est imposée en droit positif[60], les juges reconnaissant le caractère passif de l'opérateur à l'égard des

[54] Article 14 de la directive 2000/31/CE sur le commerce électronique.
[55] TGI Toulouse, réf, 13 mars 2009, krim k c/pierre g.
[56] Art 6-I-5 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[57] Art 6-I-5 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique..
[58] Neutralité et responsabilité des intermédiaires de l'Internet – Mythe ou réalité du principe de « neutralité » ?, E. Derieux, Semaine juridique Edition Générale n°13, 2012.
[59] Article 14 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[60] TGI Paris, 19 octobre 2007, zadig production et a c/ Google.

contenus mis en ligne. Dès lors, seule la méconnaissance par l'hébergeur (Youtube par exemple) d'une notification régulière est susceptible d'engager sa responsabilité à l'égard du contenu illicite. Cette solution est protectrice des hébergeurs de plateformes de vidéo. Si elle est en outre une véritable consécration de la liberté de communiquer sur Internet, ce dont il faut se réjouir, force est de constater néanmoins qu'elle est susceptible de constituer un danger pour les enfants. En effet, le visionnage de vidéos est l'une des activités que les enfants déclarent pratiquer le plus sur Internet[61]. Leur accès aux sites de partage de vidéos est totalement libre. Ils peuvent donc avoir accès à du contenu choquant, violent voire pornographique avant même qu'un internaute n'ait le temps de le signaler à l'hébergeur pour procéder à son retrait. Ainsi, la réglementation quant à la responsabilité des opérateurs de l'Internet n'est pas en parfaite adéquation avec l'intérêt de l'enfant et l'objectif de protection des mineurs.

La régulation des différents opérateurs intervenant sur Internet est nécessaire pour assurer la protection de l'enfance, mais elle ne permet pas d'appréhender avec efficacité tous les contenus inappropriés au jeune public.

[61] 57,9 % des enfants déclarent le visionnage des vidéos comme étant leur activité la plus pratiquée, « Comprendre le comportement des enfants et adolescents sur Internet pour les protéger des dangers », enquête sociologique menée par l'association Fréquence écoles, 2010.

Chapitre 2. L'insuffisance du seul encadrement des opérateurs

La protection de l'enfance à l'ère numérique ne peut pas être assurée par la seule régulation des opérateurs du net. Le législateur a donc développé des mesures complémentaires de répression et de sensibilisation (Section 1), qu'il conviendrait de faire évoluer afin de garantir leur efficacité (Section2).

Section 1. Des mesures complémentaires

En sus de la création d'infractions pénales dissuasives (I), des mesures relevant de ce qui est appelé la soft law sont développées afin d'assurer une protection efficace des mineurs sur Internet (II).

I. Des mesures de répression pénale

Le législateur a souhaité protéger les mineurs contre les contenus pornographiques, violents ou portant atteinte à la dignité humaine. Ces messages ont en effet une influence négative sur le comportement des enfants et adolescents. Tous les supports de l'image, au nombre desquels Internet, ont ainsi été accusés de susciter, notamment chez les jeunes, des formes d'agressivité[62]. De nombreux rapports ont confirmé ce phénomène. Toutes les études ont démontré que l'apparition de comportements agressifs était effectivement liée aux émissions violentes[63]. Visé à l'article 227-24 du Code pénal, le fait de fabriquer, transporter ou diffuser ces messages est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ces messages sont susceptibles d'être vus ou perçus par un mineur.

Sur le réseau Internet, les jeunes internautes sont régulièrement exposés à des contenus de nature violente, attentatoire à la dignité humaine ou les incitant à se livrer à des jeux les mettant physiquement en danger. Les enfants et adolescents sont également régulièrement exposés à des contenus sexuels via Internet. Ils le sont volontairement ou accidentellement, les sources d'exposition non sollicitée étant variées. Il peut s'agir de fenêtres « pop-up », de publicités intempestives, de mails, de

[62] « L'impact des nouveaux médias sur la jeunesse », Rapport du Sénateur M. D. Assouline, 2008.
[63] « La violence à la télévision », Rapport de Mme. B. Kriegel remis au Ministre de la Culture, 2002.

renvoi à des sites, de messages postés sur les tchats, sans oublier de mentionner les images directement accessibles à partir des moteurs de recherche[64]. L'article 227-24 du Code pénal est applicable au réseau Internet, où sont disponibles des images préalablement diffusées sur les services linéaires, mais également des images qui sont exclusivement accessibles sur le web.

Le texte ne définit pas ce qu'il faut entendre par message « pornographique », « message violent » et « message portant atteinte à la dignité humaine ». Les juges ont cependant eu l'occasion de considérer qu'un message est pornographique dès lors qu'il « représente des scènes d'actes sexuels non simulés, de manière répétitive »[65] avec l'unique vocation de « provoquer une excitation sexuelle »[66], ce qui les distingue des contenus érotiques. L'atteinte à la dignité humaine suppose de présenter une image dégradée de l'homme[67], sa figuration comme un objet dans la dépendance du pouvoir d'autrui[68]. Quant aux contenus violents, il est possible de s'en remettre à la catégorisation des programmes telle qu'assurée par le CSA[69]. La nature des messages dépendra en fin de compte de l'appréciation casuistique et subjective des juges.

Il s'agit désormais de déterminer la susceptibilité qu'a un message d'être vu ou perçu par un mineur. Il faut tout d'abord noter que le texte de loi ne vise pas les seuls messages s'adressant directement aux mineurs, comme c'est le cas dans d'autres pays. Les juges français ont fait une application stricte de cette disposition. La Cour d'appel de Paris considère qu'un message tombe sous le coup de l'article 227-24 du Code pénal dès lors qu'il est accessible par un mineur, c'est-à-dire dès lors que ce dernier peut librement le consulter[70]. Le diffuseur a l'obligation de rendre « impossible » l'accès des mineurs aux contenus. Or, du fait même de la nature du réseau Internet, il est quasi-impossible d'empêcher l'accès d'une catégorie particulière de personnes à des contenus, ce d'autant plus que les mesures de

[64] « Contre l'hypersexualisation, un nouveau combat pour l'égalité », Rapport parlementaire de Mme. C. Jouanno, Sénatrice de Paris, 5 mars 2012.
[65] Les enfants face aux images et aux messages violents diffusés par les différents supports de communication, Rapport du défenseur des enfants à Monsieur D. Perben, Ministre de la justice, décembre 2002.
[66] CA Angers, ch. civ. A, 29 oct. 2013, n° 12/00922.
[67] Les sanctions pénales et civiles de la diffusion d'un message à caractère pornographique, JY. Maréchal, La semaine juridique Edition générale, n°1, 13 janvier 2014, p 41.
[68] « Les enfants du Net », L'exposition des mineurs aux contenus préjudiciables sur l'internet, Le Forum des droits sur l'internet, 11 février 2004.
[69] La protection des mineurs face aux sites pornographiques, E. Wéry, Journal du Net.
[70] CA Paris, 13e ch. A., 2 avril 2002, n°01/03637

filtrage et de codes d'accès réservés à des majeurs ont été jugées insuffisantes à protéger les mineurs de l'accès à des contenus qui ne leur sont pas destinés, notamment pornographiques[71], à moins de bloquer l'accès au site à tous les internautes.

Cette position jurisprudentielle est problématique, contestable et contestée. Elle amène à considérer qu'une partie non négligeable des sites Internet est illégale, et ce malgré la bonne volonté des diffuseurs qui développent des systèmes pour restreindre l'accès de leurs contenus aux mineurs (constitution de guides parentaux ; avertissements visuels ; cryptage des supports visuels les plus délicats ; référencement dans les systèmes de filtrage ; paiements par carte bancaire…). De fait, les dispositions de l'article 227-24 du Code pénal sont relativement peu appliquées. Il faudrait peut-être alors, pour satisfaire la liberté de communication tout en garantissant la protection de l'enfance, prévoir des plages horaires d'accès à ces sites pornographiques, comme cela se fait sur les services audiovisuels[72].

La lutte contre la pédopornographie sur Internet est, elle, objet d'un consensus.
Sur le réseau Internet transitent de nombreux contenus, images, vidéos, textes, à caractère pédopornographique. Aux balbutiements d'Internet, les autorités n'ont pas mesuré le potentiel du réseau et n'en ont pas anticipé les éventuelles dérives. Ainsi, la Convention internationale des droits de l'enfant est-elle silencieuse quant à la pornographie enfantine[73]. Il a fallu attendre les années 2000 pour que ce phénomène soit abordé et que des mesures strictes soient adoptées. La décision du Conseil européen relative à la lutte contre la pédopornographie sur Internet du 29 mai 2000 invite les Etats à réprimer les comportements pédopornographiques sur Internet, à encourager leurs signalements, et à assurer une réaction rapide des autorités répressives. La lutte contre la pédopornographie a ensuite été régulièrement révisée et renforcée[74].

Le Code pénal sanctionne les pratiques pédopornographiques et les peines encourues sont aggravées en cas d'utilisation d'Internet. L'article 227-3 du Code

[71] Crim 12 septembre 2000, n°99-84648
[72] Toiles et filtres, C. Manara, Reccueil Dalloz 2002, p 1900.
[73] Convention International des Droits de l'Enfant du 20 novembre 1989.
[74] La Convention sur la cybercriminalité du 23 novembre 2001 ; la Recommandation du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur les droits de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne.

pénal réprime « le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique ». Ce comportement est puni de 5 ans d'emprisonnement et de 75 000 euros d'amende. Le fait de diffuser une telle image est puni des mêmes peines[75]. La consultation habituelle ou payante d'un service mettant à disposition une telle image et le fait d'acquérir ou de détenir cette image sont également réprimés[76]. Le recel d'images de pornographie enfantine[77], le fait pour un majeur de faire des propositions sexuelles à un mineur en utilisant un moyen de communication électronique[78], l'incitation à la commission d'actes pédopornographiques[79] sont autant de délits réprimés.

La loi du 17 juin 1998 a érigé en circonstance aggravante le recours à l'utilisation d'un réseau de télécommunication pour commettre des infractions au préjudice de mineurs[80]. Ainsi, les peines encourues sont aggravées lorsque les agressions sexuelles, le proxénétisme ou les viols ont été précédés d'un contact par Internet.
De même, les atteintes à la dignité humaine sont sanctionnées plus sévèrement lorsqu'elles sont commises via Internet[81].

Si ces mesures sont représentatives de la volonté des autorités publiques, gouvernementales, législatives et judiciaires, de lutter sévèrement contre la pédopornographie et de protéger efficacement le mineur contre des contenus préjudiciables, elles ne sont pas suffisantes en elles-mêmes. La protection de l'enfance doit être supportée par l'ensemble des acteurs impliqués, à savoir les pouvoirs publics et les associations ou autres organismes non gouvernementaux mais également les parents et les enseignants.

II. Des mesures non réglementaires

La réglementation des services de communication au public en ligne et des services de communication audiovisuelle et les mesures de répression pénale sont

[75] Article 227-23 alinéa 2 du Code pénal.
[76] Article 227-23 alinéa 4 du Code pénal.
[77] Article 321-1 du Code pénal.
[78] Article 227-22 du Code pénal.
[79] Article 227-28-3 du Code pénal.
[80] Loi n°98-458 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.
[81] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

nécessaires pour assurer la protection de l'enfance, mais elles ne sont pas suffisantes pour garantir cet objectif. Tous les acteurs concernés par le sujet, gouvernementaux, associatifs, particuliers, européens et nationaux, reconnaissent en effet que la mise en place d'outils techniques tels que les mesures de filtrage ou de signalement sur Internet ne suffit pas à assurer une navigation sécurisée des enfants sur le web[82].

Le Conseil de l'Union européenne a ainsi invité les Etats membres à développer un cadre national d'autorégulation des opérateurs de services en ligne afin de compléter le cadre réglementaire[83]. A cette fin, le Conseil recommandait l'élaboration de codes de conduite visant à protéger les mineurs et la dignité humaine applicables aux services en ligne. La Commission européenne a donc signé, en 2008, un accord de bonne conduite avec 20 entreprises gérant 25 sites web, dont Facebook, Google, Yahoo !. Le site Dailymotion a par exemple publié son code de bonne conduite destiné à la protection des enfants sur Internet et à l'apprentissage du bon usage de l'Internet sous format vidéo[84]. Si la nature juridique et partant la force contraignante de ces codes peut être débattue, ces codes ont été reconnus par les tribunaux comme opposables à leurs signataires et aux internautes[85].

Les fournisseurs d'accès Internet se sont, eux, engagés à contribuer aux campagnes de sensibilisation menées par les pouvoirs publics. Ils ont mission de relayer sur leurs portails respectifs les différents spots produits par les pouvoirs publics[86]. Les campagnes de sensibilisation sont commandées aussi bien par les pouvoirs publics que par les associations et les organisations non gouvernementales. Le CSA, qui produit lui-même des campagnes de sensibilisation à la télévision et sur les services de médias audiovisuels à la demande, s'associe régulièrement aux campagnes d'information visant à protéger le jeune public sur Internet[87].

De leur côté, les Etats se doivent de développer des programmes de protection des mineurs sur Internet. La protection des mineurs fait partie des objectifs de la

[82] Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009.
[83] Recommandation du Conseil 98/560/CE du 24 septembre 1998.
[84] Le code de bonne conduite de Dailymotion est accessible à l'adresse suivante : http://www.dailymotion.com/fr/legal/childprotection
[85] TC Paris, 15è ch., 11 décembre 2009, Groupement des brocanteurs de Saleya et autres c/ eBay Inc.
[86] Contrôle parental sur l'Internet : les engagements des fournisseurs d'accès Internet, 16 novembre 2005, Accord de l'AFA.
[87] « Protection de l'enfance et de l'adolescence à la télévision, à la radio et sur les services de médias audiovisuels à la demande », les brochures du CSA, novembre 2010.

stratégie numérique pour l'Europe. Au titre des principales actions figure le programme « Safer Internet »[88]. Dans ce cadre, 30 pays se mobilisent en faveur d'un Internet plus responsable et plus sûr pour les jeunes. Ce programme européen finance de nombreuses études, au titre desquelles les études EU kids online, et des projets visant à faire d'Internet un espace plus sûr. En France, ce programme est relayé par la Délégation aux usages d'Internet (DUI)[89]. La délégation développe différentes actions menées par divers acteurs. Ainsi, la société Tralalere est en charge de la campagne de sensibilisation « Internet sans crainte ». Cette campagne assure une promotion des bons usages du numérique, en menant notamment des actions de pédagogie en milieu scolaire et en s'armant d'outils de communication innovants et adaptés à son jeune public (site Internet, vidéos d'animation, jeux vidéo…). L'association E-enfance gère la ligne d'écoute et d'assistance « Net Ecoute », qui permet de répondre aux questions que les enfants et adolescents peuvent se poser quant aux jeux vidéo, à la téléphonie mobile ou à Internet. L'association des fournisseurs d'accès et de services Internet (l'AFA) gère le service de signalement en ligne des contenus choquants « Point de contact ».
Des actions complémentaires sont menées directement par la Délégation. On peut citer par exemple le site « Mineurs.fr » ouvert en décembre 2003. Il recense les différentes possibilités qui existent pour protéger les mineurs contre les contenus illicites d'Internet.

A l'image de la France, chaque Etat participant au programme Safer Internet a développé des actions de sensibilisation, menées par différents centres. Ces centres sont regroupés au sein d'un réseau européen « Insafe », qui s'occupe de coordonner leur action, et qui permet surtout l'échange des expériences entre les pays et la mise en commun des ressources entre les organismes clés d'Europe.
La sensibilisation des parents et des enfants aux enjeux et risques d'Internet ne peut être efficace sans les initiatives d'éducation aux médias. L'éducation aux médias apparaît comme une mesure essentielle pour une meilleure protection de l'enfance. Il faut donner aux enfants les moyens de se protéger eux-mêmes et sensibiliser les parents, qui sont dépassés par les nouveaux modes de communication, à des risques qu'ils sont susceptibles d'ignorer. Parents et enfants doivent apprendre à utiliser les

[88] « La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet », Rapport du CSA, mars 2012.
[89] « L'impact des nouveaux médias sur la jeunesse », rapport d'information du Sénateur M. D Assouline, 2008.

nouveaux outils de communication, en prenant connaissance des risques qu'ils comportent et des différents moyens de protection qui existent[90].

La loi n°2005-380 du 23 avril 2005 d'orientation et de programme pour l'avenir de l'école a posé le principe de l'indispensable éducation des élèves aux médias. Un an plus tard, le décret n°2006-830 du 11 juillet 2006 relatif au socle commun de connaissances et de compétences et modifiant le code de l'éducation a consacré l'éducation aux médias comme objectif fondamental du système éducatif[91]. Ainsi, l'éducation aux médias, et notamment l'apprentissage et la maîtrise d'Internet, est un enseignement inscrit dans les programmes éducatifs nationaux. Le B2i s'inscrit dans le cadre de ce programme d'éducation aux médias. Le ministère de l'Education nationale a crée en 2001 le brevet informatique et Internet, dont l'objectif est d'attester le niveau acquis par les élèves dans la maîtrise des outils multimédias et de l'Internet[92]. Cet outil permet de former les élèves à l'usage des techniques de l'information et de la communication et à la maîtrise de leurs publications, et de les familiariser avec les aides et démarches mises à leur disposition pour pouvoir les accompagner lorsqu'ils ont été confrontés à du contenu les indisposant. Depuis 2008, l'attestation du B2i est obligatoire pour l'obtention du brevet des collèges.

En outre, il est nécessaire d'aider les parents à mieux connaître et comprendre les usages de leurs enfants[93], ce qui est essentiel pour responsabiliser davantage les familles. En effet, les parents n'ont pas toujours conscience des dangers que représente Internet. Une grande majorité d'entre eux se satisfait de la familiarité des enfants avec les nouveaux outils numériques, sans en appréhender les risques[94]. Les campagnes de sensibilisation et les plateformes d'écoutes en ligne doivent donc également viser les parents. Des guides leur sont également spécialement adressés[95]. Les parents doivent assimiler et adopter les comportements qui sont primordiaux pour garantir une navigation sécurisée de leurs enfants sur le web. Ces comportements impliquent : le choix de l'emplacement de l'ordinateur (il faut

[90] Livre vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, Commission des Communautés Européennes, 16 octobre 1996.
[91] « L'impact des nouveaux médias sur la jeunesse », rapport d'information du Sénateur M. D Assouline, 2008.
[92] « Enfants et écrans : grandir dans le monde numérique », Rapport du défenseur des droits consacré aux droits de l'enfant, 2012.
[93] Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009.
[94] « Tablette tactile, la nouvelle nounou ? », sondage de l'institut CSA pour l'Observatoire Orange-Terrafemina, septembre 2012.
[95] Voir notamment « La sécurité sur internet, si on en parlait en famille ? » ; « Découvrir Internet ensemble c'est plus sûr », guides à l'usage des parents, Internet sans crainte.

privilégier une installation dans une pièce à vivre plutôt que dans la chambre du mineur) ; la présence des parents durant l'utilisation de l'ordinateur ou de la tablette ; la mobilisation des aînés pour surveiller et orienter leurs frères et sœurs plus jeunes ; la consultation récurrente des historiques ; l'encadrement de l'utilisation de l'ordinateur (tranche horaire et durée des sessions).

Bien que des mesures aient été prises pour assurer la protection de l'enfant sur Internet, des évolutions doivent être envisagées pour renforcer l'arsenal existant.

Section 2. Une nécessaire évolution ?

Il est important de souligner les efforts engagés, par l'ensemble des acteurs concernés, en matière de protection de l'enfance. Cependant, force est de constater que ces efforts ne sont pas suffisants et que leur impact doit être relativisé (I). De nombreuses mesures sont envisageables pour remédier à cette carence (II).

I. Des constats mitigés

Il faut mesurer tout d'abord l'importance de l'évolution technologique et sa célérité, qui rendent obsolètes les mécanismes de protection.
D'une part, c'est le rapport même de l'internaute avec le réseau Internet qui s'est modifié. Internet est désormais bien installé dans le paysage médiatique mondial. Est révolu le temps où l'ordinateur familial était l'unique terminal de réception de d'Internet. La technologie s'est très vite emballée après l'émergence d'Internet dans les années 1990, permettant aux « espaces Internet nomades »[96], notamment, de s'imposer sur le marché. Les smartphones (téléphones portables « intelligents » car mutlifonctions) les tablettes et les consoles de jeux portatives permettent d'avoir un accès mobile à Internet via le wifi, très prisé par les jeunes. Cette consommation individualisée et solitaire entraîne donc l'émancipation des enfants par rapport au contrôle potentiellement exercé par leurs parents. Désormais, il est fait une

[96] « Comprendre le comportement des enfants et adolescents sur Internet pour les protéger des dangers », Enquête sociologique menée par Fréquence écoles, 2010.

utilisation quotidienne et vulgarisée d'Internet, en ce sens que ce réseau est accessible en tout temps et en tout lieu.

D'autre part, les consommateurs ont modifié leur rapport aux contenus audiovisuels. Cette évolution des comportements est particulièrement notable chez les jeunes. Les smartphones et tablettes précités permettent le visionnage de contenus audiovisuels en passant par le réseau de téléphonie portable ou par un réseau sans fil, s'émancipant du réseau hertzien terrestre. Une partie des programmes télévisés sont désormais diffusés via Internet.
Les consommateurs sont donc régulièrement invités à consulter du contenu audiovisuel via Internet. 98% des internautes français consommaient de la vidéo sur Internet en septembre 2009. Au-delà des SMAD, des vidéos sont également disponibles sur les sites de journaux en ligne, les réseaux sociaux, et les plateformes de partage de vidéos (deux milliards de vidéos sont quotidiennement regardées sur Youtube[97]). Or, seuls les contenus proposés par les SMAD font actuellement l'objet d'une réglementation contraignante et d'un contrôle a priori.

La modification des rapports des internautes et plus spécifiquement des jeunes d'entre eux avec Internet et avec leur consommation de contenus audiovisuels met en exergue les lacunes et manques qui ternissent les systèmes de protection de l'enfance.
Les mécanismes de protection mis en place pour les médias traditionnels sont difficilement transposables, et de fait ne l'ont pas été, aux nouveaux supports de diffusion. Il existe ainsi une pluralité de dispositifs de régulation et de contrôle qui dépend des vecteurs de diffusion des contenus (TV, Internet), rendant le système complexe et peu lisible par les parents. Certains vecteurs sont d'ailleurs peu régulés (téléphones mobiles), voire pas du tout. L'enfant peut alors être protégé de manière différente pour un même contenu en fonction du support utilisé. Pire, il peut être protégé d'un contenu sur un site Internet régulé (SMAD), mais pouvoir y accéder sur un site échappant à tout contrôle (plateforme de vidéos)[98]. Alors même que le

[97] Philippe Bailly, Président de NPA Conseil

[98] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.

phénomène de convergence des médias s'intensifie, les normes juridiques sont encore largement segmentées par support[99].

En outre, les systèmes de protection qui existent ne sont pas performants.
Le régime de responsabilité éditoriale n'est pas convaincant face au développement des contenus générés par les utilisateurs[100]. Les sanctions pénales sont encore trop rares[101]. Les sites pornographiques, notamment gratuits, se multiplient jour après jour tandis que leur accès reste toujours très aisé. La maîtrise technologique des enfants est en décalage avec celle de leurs parents, les jeunes étant plus à l'aise avec les outils informatiques que leurs aînés et échappant à la surveillance de leurs parents. Les ressources d'éducation aux médias mises à la disposition des parents et de leurs enfants ne sont pas toujours bien connues des familles, n'étant pas assez relayées, coordonnées mais surtout trop nombreuses et donc illisibles. Les initiatives sont également parfois en retard par rapport à l'évolution des comportements des enfants sur Internet.
Les logiciels de filtrage ne sont pas parfaitement efficaces, sont souvent méconnus du public et sont inopérants lorsque l'enfant se connecte à Internet via le wifi. Cependant, généraliser le filtrage des contenus est une lourde tâche, qui apparaît à l'évidence irréaliste face au nombre de services concernés et à la dimension internationale du réseau[102]. Cet affranchissement par Internet, et plus généralement par l'ensemble des médias, des frontières territoriales est également problématique compte tenu de la proportion de contenu préjudiciable provenant de pays tiers (membres de l'UE et pays tiers). La compétence juridictionnelle des tribunaux français ne fait plus débat actuellement. La compétence est reconnue lorsque les sites sont consultables depuis le territoire français et proposent du contenu destiné au public français, alors même que leur serveur serait localisé à l'étranger. L'orientation française du site est mesurée grâce à l'analyse d'un faisceau d'indices. Elle sera retenue lorsque la langue utilisée par le site est française, lorsque l'éditeur a publié en France des publicités pour son site, lorsqu'il existe des renvois vers des sites français, lorsque la désinence correspond à « .fr »… Ce n'est donc pas tant la

[99] « La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet », Rapport du CSA, mars 2012.
[100] « La liberté de communication audiovisuelle à l'heure des nouvelles technologies de l'information et des communications », rapport de mission du groupe n°10 de la promotion « Robert Badinter » de l'ENA, février 2011.
[101] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
[102] « Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.

compétence juridictionnelle qui apparaît comme une problématique liée à l'internationalité d'Internet, mais plutôt la difficulté qu'ont les juges français à assurer l'effectivité de leurs décisions sur des opérateurs étrangers ou domiciliés à l'étranger. En outre, il n'est pas possible d'effectuer un contrôle systématique des sites Internet, ces-derniers étant en nombre infini.

En conclusion, il est indéniable que les dispositifs de protection de l'enfance, qu'ils découlent de la hard law (directives, règlements et loi) ou de la soft law (campagne de prévention, programmes d'éducation aux médias) ont été dépassés par la technologie. Si tout le monde s'accorde à reconnaître que la spécificité des supports entraîne l'adoption de règles spécifiques[103], d'aucuns considèrent indispensable de clarifier les mécanismes existants et de les renforcer.

II. Des évolutions encouragées

Les rapports sont nombreux à établir le même bilan contrasté de la politique de protection de l'enfance telle qu'elle est menée actuellement. Ils sont tout aussi nombreux à envisager les hypothèses de son amélioration.

Tout d'abord, il est proposé de renforcer les dispositifs déjà existants.
A notamment été évoquée l'idée d'étendre le filtrage administratif du réseau Internet. Pour rappel, la police administrative peut demander aux fournisseurs d'accès à Internet de bloquer l'accès des internautes aux sites pédopornographiques. Certains commentateurs réfléchissent à l'opportunité d'un filtrage administratif d'autres contenus particulièrement odieux, telle que l'incitation à la haine raciale, susceptible d'influencer les jeunes, et surtout les adolescents, en quête de repères et d'identité [104]. Cependant, cette mesure ne semble pas adéquate. Première interrogation : que recouvrerait la notion de « contenus particulièrement odieux » ? Où placer le curseur ? En tout état de cause, cette proposition est dangereuse pour la liberté de communication sur Internet. En outre, les systèmes de filtrage restent

[103] « La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet », Rapport du CSA, mars 2012.
[104] « La liberté de communication audiovisuelle à l'heure des nouvelles technologies de l'information et des communications », rapport de mission du groupe n°10 de la promotion « Robert Badinter » de l'ENA, février 2011.

toujours aussi facilement contournables (grâce à l'utilisation de serveurs proxy notamment, rapidement téléchargeable en un clic)[105].

Concernant le filtrage encore, mais parental cette fois, il est relevé que les systèmes ne sont pas les mêmes selon les supports ou services concernés. Le CSA est compétent en matière de contenus audiovisuels linéaires et délinéarisés. A cet effet, il a développé le système d'un code parental empêchant aux enfants l'accès aux programmes déconseillés aux moins de 18 ans (les programmes pornographiques et de très grande violence). Or, il n'a pas compétence pour exercer sa régulation sur Internet. Les fournisseurs d'accès à Internet délivrent des logiciels de filtrage d'Internet. Les sites filtrés dépendent donc de la programmation du logiciel, qui peut différer d'un opérateur à l'autre. Ainsi, non seulement le filtrage n'est pas le même pour les contenus audiovisuels régulés par le CSA et les autres contenus, mais en outre la protection sur Internet est propre à chaque opérateur. Il a donc été proposé de coordonner tous ces systèmes de filtrage, afin d'assurer leur efficience et leur compréhension[106]. Le CSA désirait en ce sens pouvoir labelliser les sites Internet[107]. Les sites non labellisés « site de confiance » auraient fait l'objet d'un blocage. Il n'a pas été donné suite à cette demande, et le CSA n'a pas insisté sur ce point dans son dernier rapport annuel[108].
L'idée d'une coordination du filtrage entre les différents supports est intéressante. Bien que les contenus audiovisuels et ceux circulant sur le net n'ont intrinsèquement pas la même nature, il semble possible de prévoir la définition des informations à filtrer par tous, grâce à la fixation de critères par exemple. Un coordonnateur national pourrait évaluer à chaque fin d'année la cohérence des différents systèmes de filtrage, et s'assurer que l'accès aux contenus illicites est bloqué sur tous les supports. Le cas échéant, il contacterait les opérateurs défaillants. Surtout, le coordonnateur s'assurerait que les systèmes de filtrage sont les mêmes d'un fournisseur d'accès à Internet à l'autre.

Une autre mesure consisterait à sensibiliser les hébergeurs à l'importance du signalement des contenus odieux. En effet, l'article 6-I-5 de la LCEN prévoit que la notification faite par les internautes d'un contenu odieux doit être accompagnée de

[105] « Les enfants du Net III », Forum des droits sur l'Internet, novembre 2009.
[106] « L'impact des nouveaux médias sur la jeunesse », rapport d'information du Sénateur M. D Assouline, 2008.
[107] CSA, rapport annuel, 2013.
[108] CSA, rapport annuel 2014.

mentions obligatoires[109]. La loi n'envisage pas le respect de ces éléments comme étant obligatoire pour la validité et partant l'opposabilité de la notification aux hébergeurs. Cependant, les juges ont consacré le caractère impératif de cette liste[110]. Dans le cas d'une notification insuffisamment précise, l'hébergeur continue de bénéficier du régime d'irresponsabilité consacré par la LCEN. C'est-à-dire qu'il n'est pas responsable en cas de non retrait des informations illicites. Or, le respect de cette liste peut sembler compliqué pour les internautes. En effet, ces-derniers ne sont pas toujours au courant de l'existence d'une procédure spécifique, certaines informations peuvent leur échapper ou ne pas être à leur portée (identification de la personne notifiée). Dès lors, il semble important de sensibiliser les hébergeurs et d'encourager leur bonne foi, en les incitant à retirer les contenus litigieux même lorsque la notification n'est pas complète. La protection de l'enfance n'en sera que mieux garantie.

Aux côtés du renforcement des mesures déjà existantes, il est proposé de développer des nouveaux outils de protection de l'enfance sur Internet.
La proposition qui retient le plus notre attention consiste à utiliser la technique du watermarking[111]. Le watermarking, ou tatouage numérique, permet d'insérer dans les fichiers audios ou vidéos et les images des messages. Le « tatouage » est alors intégré au fichier. Les progrès technologiques rendent possible cette insertion. Tatouer la signalétique jeunesse sur les programmes permettrait de toujours faire apparaître les avertissements quel que soit le média utilisé pour visionner le contenu et sans qu'il ne soit possible de les supprimer, ce qui est essentiel à la protection des enfants. A titre d'exemple, le film « Scary movie» a été interdit aux moins de 12 ans en France. Or, ce film est très facilement accessible sur Youtube[112], en entier et en français, sans que n'apparaisse aucune signalétique. Cette proposition permettrait en outre d'appréhender les éventuels futurs supports de visionnage des contenus audiovisuels.

Les différents rapports s'attachent également à promouvoir une action au niveau communautaire, si ce n'est au niveau mondial (la diversité des cadres juridiques nationaux rend complexe une telle action). En effet, améliorer et harmoniser la

[109] Article 6-I-5 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[110] Cass Civ. I, 17 février 2011, n° 09-13202.
[111] Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009.
[112] https://www.youtube.com/watch?v=271E78rcc2o

législation européenne est un préalable au renforcement français des mécanismes de protection de l'enfance, en permettant une application uniforme des règles européennes. Il s'agirait également de modifier la directive SMA, dont la rigidité est critiquée. Les sites de partage de vidéos échappent à la réglementation sur les services non linéaires car ils sont dénués de responsabilité éditoriale, ne faisant que fournir du contenu créé par les utilisateurs, stocker ce contenu ou le publier de façon accessoire. Or, l'exclusion de ces sites est trop radicale alors qu'ils évoluent vers une éditorialisation de leurs contenus[113]. Il faudrait ainsi repenser la directive et modifier la définition des services de médias audiovisuels afin d'intégrer ces derniers acteurs dans son champ d'application. Cependant, cette proposition s'avère compliquée. Elle requiert d'importants moyens techniques et humains. De plus, il est irréaliste de penser que le CSA serait capable de contrôler tous les contenus audiovisuels partagés sur youtube. Enfin, cela suppose de modifier le régime juridique de ces acteurs, passant du statut d'hébergeur à celui d'éditeur de contenu, et de développer un régime sui generis, le régime juridique actuel des services de médias audiovisuels ne leur étant pas adapté (il n'est ainsi pas possible de prévoir des horaires de diffusion des vidéos diffusées sur une plateforme en fonction de l'âge du public auquel elle s'adresse).

La politique d'éducation aux médias doit être améliorée. Les initiatives sont nombreuses et disparates. Les rapports sont unanimes, il faut regrouper les actions sous l'égide d'une seule et même institution[114]. La composition et les prérogatives de cette autorité diffèrent selon les rapports. Il semble que l'institution devrait être compétente en matière de protection des mineurs sur l'ensemble des supports et médias : DVD, téléphone portable, jeux vidéo, presse écrite, radio, télévision, cinéma, et Internet (et notamment les plateformes de vidéos)[115]. En effet, la convergence numérique requiert d'adopter une approche globale de la protection de l'enfance. L'institution jouirait de prérogatives lui permettant de définir et mettre en œuvre un programme national d'éducation aux médias, de financer la recherche et de vérifier le respect du programme éducatif. Elle devrait être composée d'un panel de tous les

[113] « La liberté de communication audiovisuelle à l'heure des nouvelles technologies de l'information et des communications », rapport de mission du groupe n°10 de la promotion « Robert Badinter » de l'ENA, février 2011.
[114] Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009 ; « L'impact des nouveaux médias sur la jeunesse », rapport d'information du Sénateur M. D Assouline, 2008 ; « La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet », Rapport du CSA, mars 2012.
[115] « L'impact des nouveaux médias sur la jeunesse », rapport d'information du Sénateur M. D Assouline, 2008.

acteurs concernés par la protection de l'enfance, à savoir les associations, les professionnels des médias et des réseaux, les parents, les chercheurs, les institutions publiques[116]. Un référent institutionnel permettrait en outre de développer la corégulation, à l'heure où les mécanismes de régulation et d'autorégulation ne fonctionnent pas efficacement de manière individuelle.

Développer la corégulation plutôt que d'alourdir la réglementation est une proposition supplémentaire pour améliorer le dispositif actuel de protection de l'enfance. Le recours à l'autorégulation est actuellement très limité en France. Or, si la réglementation permet de fixer rapidement un nouveau cadre juridique pour les opérateurs de l'Internet, l'autorégulation permet une adaptation plus facile des règles aux évolutions technologiques. Le droit souple ne requiert pas en effet que soit votée une nouvelle loi pour appréhender les nouvelles technologies. Ce système d'autorégulation est d'ailleurs celui qui a été retenu, et dont la performance est souvent distinguée, pour sensibiliser les professionnels de la publicité[117]. Cette approche permet en outre de responsabiliser les professionnels et de renforcer leur adhésion aux règles qu'ils élaborent eux-mêmes[118]. Ce système est également très utilisé en Allemagne, au Canada et au Royaume-Uni[119].

Le dispositif français de protection de l'enfance peut et doit être amélioré. L'objectif de protection de l'enfance ne peut en effet être assuré qu'en permettant une navigation saine sur Internet de l'enfant spectateur du numérique. Aux côtés de ce rôle de spectateur, l'enfant intervient également sur Internet en tant qu'acteur du numérique. Il s'agit alors de lui offrir une protection propre à ce statut.

---

116 Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009.
117 Du BVP à l'ARPP : nouvelle dénomination, nouvelle régulation ?, L. Arcelin-Lécuyer, Revue Lamy de la Concurrence, n°22, 2010.
118 « La liberté de communication audiovisuelle à l'heure des nouvelles technologies de l'information et des communications », rapport de mission du groupe n°10 de la promotion « Robert Badinter » de l'ENA, février 2011.
119 Médias et Sociétés, F. Balle, LGDJ, 16ème édition, 2013.

Titre II. L'enfant acteur du numérique

L'enfant a assurément les compétences lui permettant de maîtriser l'outil numérique, mais n'a pas nécessairement les capacités d'en déceler les dangers. Dangers pour lui-même, il faut notamment aider le mineur à garder privée sa vie numérique (Chapitre I). Dangers pour les autres, il faut œuvrer pour empêcher l'enfant d'adopter un quelconque comportement répréhensible (Chapitre II).

Chapitre I. La vie privée du mineur à l'épreuve du numérique

L'enfant a tendance à livrer les détails de son intimité à son public numérique et à délivrer de manière irréfléchie ou inconsciente les informations personnelles le concernant. Dès lors, il lui est offert une protection en amont (Section 1) et une suppression de ses informations en aval (Section 2).

Section 1. La protection des informations personnelles

Les informations personnelles, du mineur comme de tout internaute, doivent être protégées tant au stade de leur communication (I) qu'au stade de leur traitement (II).

I. La communication des informations personnelles

Internet peut être considéré comme une menace pour la vie privée des internautes, au rang desquels les mineurs. En effet, l'internaute, au gré de ses activités professionnelles ou de ses loisirs, est amené à se connecter sur différents sites. Chaque navigation constitue une trace numérique de l'internaute. En achetant sur un site comme Amazon un album des Beatles, acte qui aurait pu lui paraître anodin, l'internaute laisse derrière lui des données indiquant quels sont ses goûts musicaux[120]. Toutes les activités en ligne délivrent des données personnelles sur l'internaute et menacent sa vie privée.

L'article 9 du Code civil dispose que « chacun a droit au respect de sa vie privée »[121]. Si le législateur a mis en place un régime de protection de la vie privée de tout un chacun, il s'est abstenu d'en donner une définition légale. La jurisprudence et la doctrine ont alors déterminé les éléments relevant de la vie privée. De manière non exhaustive, la notion de vie privée recouvre ainsi la vie sentimentale, la vie sexuelle, les convictions politiques, philosophiques et religieuses, le domicile, le patrimoine personnel, l'état de santé d'une personne[122].

---

[120] www.amazon.com

[121] Article 9 alinéa 1 du Code civil.

[122] Voir par exemple CEDH, 29 juin 2006, req n° 11901/02 : constitue une violation de la vie privée la divulgation d'informations concernant la santé mentale d'une personne lors d'une audience publique.

Avec Internet est né le paradoxe de la vie privée, terme issu de l'expression anglaise « privacy paradox »[123]. Les internautes, de par leur pratique d'Internet, divulguent des informations les concernant et relevant de leur vie privée, tout en souhaitant que celle-ci reste protégée. Le développement des blogs et plus récemment des réseaux sociaux a accentué ce phénomène (en 2014, 68% des français étaient inscrits sur un réseau social[124]). Les mineurs, en particulier, révèlent leur quotidien via ces sites : photos, commentaires, statuts, « likes ». Les mineurs dévoilent eux-mêmes leur vie privée, mais également celle de leurs proches (parfois même les coordonnées bancaires de leurs parents). Sur les blogs et les forums de discussion, les mineurs sont susceptibles de se livrer de manière beaucoup plus intime. En établissant un lien virtuel avec un correspondant, ils peuvent penser avoir instauré une relation de confiance et délivrer des informations telles que leur numéro de téléphone, leur adresse, leur âge, le nom de l'établissement scolaire qu'ils fréquentent, ou encore envoyer des photos d'eux… Or, ils ne sont pas toujours conscients des risques auxquels ils s'exposent en partageant leur vie sur Internet. Ainsi, l'un des dangers de ces pratiques numériques est de permettre à des adultes mal intentionnés de contacter ces mineurs, voire de retrouver leur identité par le biais des informations communiquées naïvement.

Afin de lutter contre ces comportements « à risque », il a été proposé d'encourager la publication d'un message de prévention et d'alerte en première page des blogs, des forums de discussion et des réseaux sociaux[125]. Cette mesure, qui semble en effet être un prérequis à la protection des mineurs, n'est pourtant pas appliquée de manière efficace. Les mises en garde, lorsqu'elles existent, ne sont accessibles que par le biais du règlement du site[126]. Or, rien ne permet de contrôler la lecture consciencieuse de ce règlement par les mineurs. Face à ce constat, il est nécessaire d'imposer à de tels sites, dans la mesure du possible, l'affichage d'une bannière d'avertissement sur toutes les pages du site, à commencer par les pages d'accueil et d'inscription.

En outre, il peut être intéressant de missionner une association qui serait désignée par la CNIL pour effectuer un recensement des sites exclusivement dédiés aux

123 La loi Informatique et libertés est-elle dépassée ? L. Cytermann, RFDA 2015, p99.
124 Social, Digital & Mobile around the world, We are social Singapore, 2014.
125 « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
126 C'est la cas par exemple sur le site rencontre-ados.net

jeunes enfants et aux adolescents. Cette association évaluerait la fiabilité de ces sites, en indiquant notamment le nombre de harcèlements ou de comportements suspects que les utilisateurs auraient éventuellement signalés.

Une mesure pourrait consister à imposer, sur les sites principalement destinés aux enfants et adolescents, et ce quelle que soit leur nature (sites de rencontres, forums de discussions et d'entraide, forums dédiés aux jeux-vidéo…), le renseignement de l'adresse mail des parents. Cette mesure permettrait ainsi aux parents de savoir que leur enfant a rejoint une communauté d'internautes. L'objectif n'est pas d'effectuer une traçabilité des interactions de l'enfant avec d'autres internautes (si l'enfant va sur ces sites c'est notamment pour s'émanciper de ses parents et communiquer avec d'autres personnes), mais d'informer les parents, dans une moindre mesure, de l'activité numérique de leur enfant. Les parents pourraient ainsi se renseigner sur la fiabilité du site auprès de proches et de l'association susvisée désignée par la CNIL, être rassurés et laisser leur enfant échanger en toute confiance. Cette mesure permettrait également de s'assurer que l'accord des parents a bien été obtenu par le mineur, tout au moins de manière tacite[127], alors qu'actuellement les sites se contentent, dans le meilleur des cas, d'indiquer qu'il est interdit aux mineurs de s'inscrire sans l'accord d'un parent. En effet, le recueil du consentement parental n'est pas prévu par la loi, ce à quoi il conviendrait de remédier. Une alternative consisterait à créer un système de contrôle parental qui permettrait de filtrer la création de tout nouveau contact, ce qui a été mis en place par Microsoft après que des dérives aient été constatées sur la messagerie instantanée Windows Live Messenger[128].

Le G29 a précisé les règles applicables aux réseaux sociaux dans un avis du 12 juin 2009[129]. Le G29, ou groupe de travail 29, a été instauré par la directive 95/46/CE. C'est un organe consultatif européen indépendant sur la protection de la vie privée et des données, composé d'un représentant de l'instance compétente en matière de données personnelles existant dans chaque Etat (en France, la CNIL[130])[131]. Il forme

[127] Même si bien sûr l'hypothèse des enfants communiquant de fausses adresses mail n'est pas à négliger…
[128] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
[129] Avis n°5/2009 sur les réseaux sociaux en ligne, Groupe de travail « article 29 » sur la protection des données, 12 juin 2009.
[130] La loi de 1978 a créée la CNIL, autorité indépendante administrative, article 11 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[131] Article 29 de la directive 95/46/CE 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.

des avis et des recommandations et établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel[132]. Le G29 invite les réseaux sociaux à mettre en place des paramètres de confidentialité et à définir des paramètres par défaut, (les mineurs ne maîtrisant pas toujours ces outils), limitant ainsi la diffusion des données des internautes, à supprimer les comptes restés inactifs pendant une longue période, à permettre aux internautes, membres ou non du réseau, de bénéficier d'un droit à la suppression des données les concernant, à autoriser l'utilisation de pseudonymes, à développer des dispositifs permettant aux internautes de déposer des plaintes relatives à la vie privée. Les fournisseurs de services de réseautage social sont appelés à mettre en garde de façon adéquate les utilisateurs contre les risques d'atteinte à leur vie privée et à celle des autres lorsqu'ils mettent des informations en ligne. Les fournisseurs devraient également développer des logiciels de vérification de l'âge (Facebook est interdit aux mineurs de moins de 13 ans, en vertu de la loi américaine, et pourtant nombreux sont les enfants à mentir sur leur âge pour accéder au réseau, parfois même avec l'aval de leurs parents[133]). Enfin, le G29 incite les fournisseurs à modifier leurs conditions générales d'utilisation afin de les rendre plus lisibles et compréhensibles par les utilisateurs.

La CNIL constate que ces mesures, non contraignantes, ne sont pas toujours respectées[134]. Elle souligne néanmoins les initiatives entreprises par certains réseaux, et encourage les autres à adopter les mêmes démarches. Ainsi, le réseau social Famicity, ouvert depuis 2011, offre à ses membres des outils permettant de protéger leur vie privée[135]. Il est impossible de rendre les photographies publiques, il n'y a pas de liens avec les « amis d'amis », les profils des membres n'apparaissent pas dans les pages des moteurs de recherche[136].

[132] Article 30 de la directive 95/46/CE 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.
[133] L'usage des réseaux sociaux chez les 8-17 ans, Etude TNS Sofres, Juin 2011.
[134] Rapport d'activité 2012, CNIL.
[135] Des réseau sociaux plus protecteurs de la vie privée… Article de la CNIL publié sur le site www.cnil.fr, 10 septembre 2012.
[136] Avis n°5/2009 sur les réseau sociaux en ligne, Groupe de travail « article 29 » sur la protection des données, 12 juin 2009.

Il faut donc encourager les fournisseurs de service de réseautage social à s'autoréguler, en adoptant éventuellement des codes de bonne pratique[137], comme cela se fait aux Etats-Unis[138]. Ils seraient amenés également à participer à des politiques de sensibilisation. Il est indispensable en effet de développer des politiques de sensibilisation efficaces, via les écoles et les parents. Il faut donner aux enfants les moyens de comprendre la notion de donnée personnelle et les enjeux qui y sont attachés.

Aux côtés de la divulgation plus ou moins volontaire de leur vie privée par les internautes, un certain nombre de sites recueillent des renseignements personnels les concernant. Est une donnée à caractère personnel « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »[139]. Il existe des débats relatifs à ce que recouvre exactement la notion de données à caractère personnel. Dans le cadre de cette étude, il s'agit d'apprécier cette notion comme ayant un champ très étendu et évolutif, au gré notamment des développements techniques et technologiques. Ainsi, la Federal Trade Commission a modifié le Children's Online Privacy Protection Act of 1998 (COPPA) qui fixe les principes fondamentaux de la protection des données personnelles des enfants de moins de 13 ans. La Commission a pris en compte les évolutions pour modifier cet acte en considérant notamment que la géolocalisation des enfants de moins de 13 ans est une donnée personnelle, au même titre que son adresse IP ou ses photographies, les vidéos et fichiers audio qui contiennent son image ou sa voix[140].

Ces informations, qui ne semblent aux mineurs accessibles qu'à un groupe restreint de personnes, sont en vérité facilement exploitables et de fait exploitées, malgré les dispositions législatives relatives au traitement des données à caractère personnel.

---

[137] L'adoption de codes de conduite est prévue à l'article 27 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995.
[138] Internet et la collecte de données personnelles auprès des mineurs, Rapport de la CNIL présenté par C. Alvergnat, 12 juin 2001.
[139] Article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[140] Children's Online Privacy Protection Rule : Final rule Amendments to clarify the scope of the rule and strengthen its protections for children's personal information, Federal Trade Commission, 17 janvier 2013.

II. Le traitement des données à caractère personnel

Tout individu a le droit à ce que ses données personnelles soient protégées.
La Convention n°108 du Conseil de l'Europe adoptée en 1981 a consacré le droit à la protection des données personnelles au niveau international[141]. La Charte des droits fondamentaux de l'Union européenne, adoptée en 2000 et dotée d'une portée contraignante depuis 2009[142], reconnaît un caractère fondamental au droit à la protection des données personnelles, qu'elle vise de manière distincte et indépendante du droit au respect de la vie privée dans son article 8[143].
En France, le dispositif de protection est organisé par la loi « Informatique et Libertés » du 6 janvier 1978[144]. La loi de 1978 a ensuite été modifiée en 2004[145] afin de transposer en droit interne la directive de 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la lire circulation de ces données. Cette loi a fait l'objet d'une dernière modification à l'occasion de l'ordonnance du 24 août 2011[146].

La vie privée et les données personnelles de l'enfant, comme celles de toute personne physique, sont protégées de deux manières : d'une part, la loi encadre le traitement de ces informations personnelles. D'autre part, l'enfant jouit de droits lui permettant d'en assurer la protection[147].

Il faut noter de prime abord qu'il est interdit de collecter ou de traiter les données dites sensibles et relatives aux origines raciales ou ethniques de l'internaute, à ses opinions politiques, philosophiques ou religieuses, à son éventuelle appartenance syndicale, à sa santé ou à sa vie sexuelle[148]. La collecte des données personnelles autres que celles susmentionnées n'est pas illicite per se. Cependant, elle fait l'objet d'une réglementation. Le traitement des données personnelles est défini comme étant l'opération ou l'ensemble des opérations portant sur les données personnelles,

[141] Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 janvier 1981.
[142] Traité de Lisbonne modifiant le Traité sur l'Union européenne et le Traité instituant la Communauté européenne, 2007/C 306/01.
[143] Charte des droits fondamentaux de l'Union européenne, 2012/C 326/02.
[144] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[145] Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978.
[146] Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques.
[147] « Enfants et écrans : grandir dans le monde numérique », Rapport du défenseur des droits consacré aux droits de l'enfant, 2012.
[148] Article 8 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, ainsi que l'effacement ou la destruction[149]. Le traitement correspond donc, en son sens large, au fait de pouvoir disposer des données personnelles. La collecte des données personnelles peut être faite de différentes façons. Elle peut être « directe », c'est-à-dire que l'internaute délivre lui-même des informations le concernant. La collecte peut également être « indirecte », constituée par les données de connexion et de navigation de l'internaute.

A l'époque où la loi de 1978 a été adoptée, le traitement des données était essentiellement assuré par les administrations, les entreprises et les associations[150]. Le développement d'Internet a ensuite donné naissance à la collecte massive et automatisée des données par une pluralité d'acteurs privés. La loi de 1978 distingue ainsi les traitements faits par le secteur public de ceux orchestrés par le secteur privé[151]. Les premiers doivent faire l'objet d'une autorisation préalable tandis que les seconds doivent être déclarés à la CNIL[152].
Pour être licite, le traitement des données personnelles doit répondre à des exigences légales[153]. Les données doivent être collectées et traitées de manière loyale. Elles doivent être collectées pour des finalités déterminées. Elles doivent être proportionnées à ces finalités et être uniquement conservées pendant la durée nécessaire aux finalités déclarées. En outre, l'intéressé doit avoir consenti au traitement de ses données, à moins que le traitement soit réalisé, entre autres exceptions, au regard d'une obligation légale ou d'un intérêt légitime[154]. Le dispositif de protection n'établit aucune différenciation entre l'adulte et l'enfant, qui ne jouit pas d'une protection renforcée de ses données personnelles. Ainsi, la collecte de données auprès de mineurs est-elle possible. Pour procéder à la collecte, le fournisseur doit recueillir le consentement préalable des parents, et fournir une information claire aux mineurs. A la lecture de la directive, il apparaît que ce

[149] Article 2 § 3 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[150] La loi Informatique et libertés est-elle dépassée ? L. Cytermann, RFDA 2015, p99.
[151] Protection de la vie privée et des données personnelles, N. Mallet-Poujol, Legamedia, février 2004.
[152] Articles 22 et 25 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[153] Article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[154] Article 7 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

consentement doit être explicite[155]. Cette condition semble faire défaut dans le cadre de la collecte directe des données personnelles[156]. Cependant, une partie de la doctrine considère que les utilisateurs consentent néanmoins à la collecte de leurs données en les mettant volontairement en ligne[157].

Le responsable du traitement doit également garantir au mineur (comme à tout intéressé) le respect de ses droits. Il s'agit du droit à l'information (comprenant notamment le droit d'être informé de l'utilisation qui va être faite de ses données)[158], du droit de s'opposer à la collecte de ses données[159], du droit d'accès[160] et de rectification de ses données[161].

Dès lors que le responsable du traitement a reçu le récépissé de la CNIL attestant de sa déclaration, il peut commencer à procéder au traitement des données. Il n'est cependant pas exonéré de ses responsabilités et doit encore se soumettre à certaines obligations. Le responsable de la collecte et du traitement des données doit assurer la sécurité des informations[162]. Il doit prendre toutes les précautions nécessaires pour prévenir une violation des données. Une violation des données s'entend comme une « violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques »[163]. En cas de violation des données, le fournisseur doit en informer l'intéressé. A défaut de notification, il encourt une peine de 5 ans d'emprisonnement et 300 000 euros d'amende [164] . Cependant, cette disposition est uniquement applicable aux fournisseurs de services de communications électroniques accessibles au public. Elle ne concerne donc pas les fournisseurs de service de réseautage social, qui sont considérés comme étant des services de la société de l'information[165]. L'extension de

[155] « La personne concernée a indubitablement donné son consentement », article 7 a) de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995.
[156] La protection du mineur dans le cyber espace, C. Nlend, Thèse, 2007.
[157] Les réseaux sociaux face à de nouvelles contraintes – Impacts de la recommandation de la Commission des clauses abusives, A.L. Falkman, La Semaine Juridique édition Entreprises et Affaires, n°12, 19 mars 2015, p 1136.
[158] Article 32 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[159] Article 38 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[160] Article 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[161] Article 40 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[162] Article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[163] Article 34 bis de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[164] Article 226-17-1 du Code pénal.
[165] Avis n°5/2009 sur les réseaux sociaux en ligne, Groupe de travail « article 29 » sur la protection des données, 12 juin 2009.

la procédure de notification est ainsi fortement plébiscitée et pourrait être décidée prochainement[166]. En effet, les réseaux sociaux collectent des milliards de données personnelles, et ce notamment et surtout à des fins commerciales, qu'il conviendrait de protéger d'une éventuelle violation.

Les responsables de réseaux sociaux participent au traitement des données des utilisateurs et sont donc visés par la directive de 1995. A cet effet, ils devraient informer les utilisateurs de l'utilisation qu'ils font de leurs données, et notamment celle faite à des fins de marketing. En effet, l'inscription à ces sites est – généralement – gratuite. Ces sites se rémunèrent par la publicité qu'ils diffusent sur leurs pages. Ainsi, afin de vendre les espaces publicitaires, le responsable du site transmet aux publicitaires les informations que l'internaute lui aura communiquées.

Le dispositif de protection des données personnelles tel qu'il existe actuellement est fréquemment critiqué. Les modalités du recueil du consentement et d'information ne sont pas satisfaisantes. Les conditions générales d'utilisation des sites sont inaccessibles à l'utilisateur, en ce sens qu'elles lui sont incompréhensibles et qu'elles ne peuvent, de toute façon, être négociées. Le droit est parfois silencieux, notamment en ce qui concerne le devenir des données personnelles en cas de désabonnement d'un site communautaire[167]. Le droit ne permet finalement pas une maîtrise effective par l'individu de ses données.

Les remèdes proposés sont nombreux. Il s'agirait notamment d'encourager l'autorégulation, ce qui permettrait d'instaurer in fine un système reposant sur la corégulation, la complémentarité entre réglementation publique et responsabilisation des acteurs ayant déjà porté ses fruits dans d'autres domaines[168]. Dans cette optique, il serait demandé aux responsables de traitement de pratiquer la transparence dans leur activité de gestion des données personnelles. Ils devront également simplifier leurs politiques d'utilisation, voire adopter des standards en matière de conditions générales d'utilisation[169]. Enfin, il est indispensable de soutenir des actions de sensibilisation des internautes, et surtout des jeunes, qui sont les plus vulnérables, aux risques liés au traitement de données à caractère

[166] La responsabilité des réseaux sociaux en cas de violation des données personnelles, J.P. Arroyo et C. Prault, RLDI, 2014, p109.
[167] « L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
[168] Le numérique et les droits fondamentaux, Etude annuelle 2014, Conseil d'Etat.
[169] La loi Informatique et libertés est-elle dépassée ? L. Cytermann, RFDA 2015, p99.

personnel. Ces actions devraient être relayées par tous les médias, et notamment publiées sur les différents sites web, en décrivant exactement les droits des utilisateurs[170].

Un projet de règlement européen visant à se substituer à la directive de 1995 a été présenté en 2012. Les discussions sur le texte définitif du règlement devraient reprendre au second semestre 2015[171]. La modernisation du cadre juridique se jouera donc dans un avenir proche.

Si le traitement des données personnelles fait l'objet de critiques, le législateur européen a consacré aux internautes le droit d'en demander la suppression.

Section 2. La « suppression » des données personnelles

Les informations accessibles sur Internet ont un caractère indélébile. Si certains considèrent ce caractère comme vertueux, les informations délivrées par l'enfant durant son jeune âge peuvent ne plus être en adéquation avec la personnalité de l'adulte qu'il est devenu, et lui porter préjudice notamment à l'heure de son entrée dans la vie professionnelle. Le législateur a alors reconnu un droit au déréférencement à tous les internautes (I). Cependant, droit au déréférencement ne signifie pas suppression des données. La protection de la vie privée sur Internet ne peut être totale sans consacrer un droit à l'oubli numérique (II).

I. Le droit au déréférencement

Une identité numérique est attachée à tout internaute, voire au-delà à toute personne dont certaines informations circuleraient sur Internet, avec ou sans son consentement. L'identité numérique peut être définie comme « la collection des traces (écrits, contenus audios ou vidéos, messages sur des forums, identifiants de

[170] « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 4 novembre 2010.
[171] Projet de Règlement Européen sur la protection des données personnelles : ce qui va changer, T. Dor, D. Rimsevica, Le Monde du Droit, 7 avril 2015.

connexion, etc.) que nous laissons derrière nous, consciemment ou inconsciemment, au fil de nos navigations sur le réseau et le reflet de cet ensemble de traces, tel qu'il apparaît « remixé » par les moteurs de recherche »[172]. L'identité numérique se compose donc des noms, prénoms, pseudos, coordonnées, photos, articles, commentaires, liés à un individu. Elle lui est propre. Dès lors, il serait logique que chaque personne ait la maîtrise de son identité numérique, et plus généralement de sa vie numérique. Cependant, cette maîtrise n'est pas effectivement acquise. Bien trop souvent, des informations concernant une personne circulent sur Internet à ses dépens, et sont susceptibles de lui porter préjudice. Un tel constat est établi notamment lorsqu'une recherche Internet exécutée par le biais d'un moteur de recherche et composée du nom patronymique d'une personne fait apparaître des liens menant vers des sites dont le contenu est relatif à l'intéressée. Cette pratique numérique a fait l'objet d'un contentieux largement commenté[173].

Un particulier espagnol reprochait à Google de faire apparaître, au titre des résultats d'une recherche, des informations le concernant et vieilles d'une dizaine d'années. Sa plainte contre Google n'ayant pas aboutie, il s'est adressé à l'Agence espagnole de protection des données personnelles qui a obligé Google à retirer les informations litigieuses de la liste des résultats. Google a saisi la Audencia Nacional[174], qui s'est adressée à la Cour de Justice de l'Union Européenne. Au titre d'une question préjudicielle, la CJUE s'est prononcée sur l'activité d'indexation des résultats pratiquée par les moteurs de recherche.

En premier lieu, la Cour européenne a qualifié les moteurs de recherche de responsables de traitement de données au sens de la directive de 1995.
Le responsable de traitement de données est « la personne physique ou morale, l'autorité publique, le service ou l'organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[175]. Le groupe 29 a explicité cette définition légale[176]. Il estime que la capacité de « déterminer » les finalités et les moyens du traitement s'apprécie selon

[172] Qu'est-ce que l'identité numérique ?, O. Ertzscheid, Encyclopédie numérique, 2013.
[173] CJUE, gr. Ch., 13 mai 2014, Google Spain SL et Google Inc. c/ Agencia Espanola de Proteccion de Datos (AEDP), n° C-131/12.
[174] Haut tribunal espagnol
[175] Article 2 d) de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995.
[176] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», 16 février 2010, Groupe de travail « article 29 » sur la protection des données.

une approche factuelle. Le responsable du traitement est celui qui exerce une véritable influence quant aux activités de traitement. Les « finalités » d'un traitement sont les buts, les raisons de ce traitement. Les « moyens » du traitement sont les aspects techniques et d'organisation qui doivent permettre d'atteindre la ou les finalités du traitement.

La juridiction européenne relève que les moteurs de recherche exercent une activité autonome de celle effectuée par les éditeurs de site, qui consiste à indexer les informations publiées sur Internet et à les mettre à disposition des internautes. Elle met en exergue le rôle décisif tenu par le moteur de recherche en ce qu'il rend accessible les données à tout internaute procédant à un simple requête alors que la majorité d'entre eux n'y aurait pas eu accès sans son intermédiaire[177]. Pour la Cour, cette activité autonome est caractéristique d'un traitement de données personnelles alors même que les liens sont présentés de « de manière automatisée, constante et systématique à partir d'informations publiées sur Internet »[178]. A cet effet, les juges européens consacrent la possibilité pour les internautes de faire valoir les droits qui leur sont reconnus par la directive auprès des moteurs de recherche. Pour la Cour, l'exercice effectif de ces droits implique corollairement l'obligation pour Google de supprimer de la liste des résultats des informations relatives à une personne. Elle reconnaît par là aux internautes un droit au déréférencement (également appelé droit à la désindexation) opposable aux moteurs de recherche, qui serait une déclinaison des droits d'accès, de rectification et d'effacement[179].

Le déréférencement s'entend comme « le fait de supprimer certains résultats figurant dans la liste de ceux affichés par un moteur de recherche après une requête effectuée sur la base de données relative à une personne »[180]. Le droit à la désindexation tel que consacré par la CJUE est un droit autonome, qui s'exerce par les particuliers indépendamment de tout effacement des informations litigieuses sur le site auquel mènent les liens présentés comme résultats d'une requête. Le plaignant n'a pas à justifier d'un quelconque préjudice pour qu'il soit fait droit à sa demande. En outre, il faut relever que les liens doivent être déréférencés alors

[177] « La consécration d'un droit à l'oubli… principalement pour les anonymes », A. Casanova, RLDI n°106, 2014.
[178] « L'automaticité du moteur de recherche sur internet : opposition absolue entre les jurisprudences européenne et française », J. Huet, RLDI n°106, 2014.
[179] « La Cour de justice, les moteurs de recherche et le droit « à l'oubli numérique » : une fausse innovation, de vraies questions », R. Perray et P. Salen, RLDI n°109, 2014.
[180] Guidelines on the implementation of the Court of Justice of the European Union judgment on"Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González », G29, 26 novembre 2014.

même que l'information à laquelle ils ont trait serait licite. Le moteur de recherche doit également indiquer les raisons pour lesquelles le contenu a été supprimé des résultats.

Cependant, le déréférencement n'est pas accordé de plein droit. Le déréférencement est ordonné lorsque les données sont « inadéquates, non pertinentes ou excessives au regard des finalités du traitement ». Il s'agit d'apprécier les autres droits en présence afin de juger de la pertinence de l'information, l'intérêt du demandeur devant prévaloir sur celui que pourrait avoir le responsable du traitement dans l'exercice de son activité ou celui des tiers. Il faut articuler les intérêts en présence en fonction de la nature de l'information, de sa sensibilité pour la vie privée, de l'intérêt du public à disposer de cette information[181]. Le lien ne doit pas être déréférencé lorsque l'intérêt du public prévaut. C'est le cas par exemple d'informations relatives à une personne jouant un rôle dans la vie publique[182]. La CJUE ajoute néanmoins que le droit à la protection des données personnelles et le droit au respect de la vie privée « prévalent, en règle générale, sur l'intérêt des internautes ». Les cas de conservation des liens doivent donc être isolés[183].

Dans cette affaire, le Cour européenne applique le droit européen issu de la directive de 1995 au moteur de recherche américain Google, ce qui peut être surprenant au premier abord. En effet, la demande de déréférencement était faite auprès de Google Spain. Or, la filiale espagnole de Google Inc.ne traite pas directement les données collectées sur Internet. Ce traitement est effectué par la société mère, dont le siège est établi en Californie. Cependant, malgré cet élément d'extranéité, la CJUE considère que la législation européenne est applicable dès lors que le traitement est effectué dans le cadre des activités de l'entité espagnole[184]. Or, la Cour conclut que « le traitement de données à caractère personnel est effectué dans le cadre de l'activité publicitaire et commerciale de [Google Spain] ».

La CJUE consacre ainsi un droit au déréférencement à tout internaute.

---

181 « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? », V.L. Benabou et J. Rochfeld, Recueil Dalloz 2014, p 1476.
182 « Google Inc. condamné en référé à déréférencer un lien renvoyant vers un contenu qui n'est pas illicite en soi », O. Pignariti, RLDI N°113, 2014.
183 « CJUE : le droit à l'oubli n'est pas inconditionnel », J. Le Clainche, RLDI, n°107, 2014.
184 Article 4 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995.

Les autorités européennes de protection des données personnelles insistent notamment sur le fait que les demandes de déréférencement formulées par les mineurs doivent toujours être satisfaites, conformément à « l'intérêt supérieur de l'enfant »[185].

Le droit au déréférencement permet aux internautes d'avoir une maîtrise un peu plus importante de leurs données sur le web. Cependant, la désindexation permet uniquement à l'internaute de demander la suppression des liens dirigeant les utilisateurs vers le site qui a publié l'information litigieuse. Bien qu'elle n'apparaisse plus au titre des résultats d'une recherche, cette information continuera d'apparaître sur le site sur lequel elle a été diffusée en premier lieu, et sur les sites qui l'auraient éventuellement reprise. Ainsi, ce droit au déréférencement est improprement qualifié de droit à l'oubli, qui n'existe pas encore mais qui est essentiel pour assurer une effectivité de la protection des données personnelles.

II. Vers un droit à l'oubli ?

Le « droit à l'oubli » permettrait de renforcer la protection de la vie privée et des données personnelles sur Internet. Ce droit a vocation à permettre aux internautes de ne laisser aucune trace de leur passage lors de la suppression de leurs comptes, sur les réseaux sociaux notamment. Les données seraient définitivement supprimées. Un tel droit est particulièrement important pour les mineurs. Exposés très jeunes aux espaces numériques, ils n'ont pas les capacités suffisantes pour appréhender les risques qu'Internet fait courir à leur vie privée. Ils n'ont pas toujours conscience de la portée d'une photographie ou d'un commentaire, susceptibles de leur causer un préjudice immédiat et futur, au moment de leur entrée dans la vie professionnelle. Il faut permettre à l'internaute d'adapter sa vie numérique d'enfant à sa vie d'adulte.

Mesurant la gravité des conséquences des légèretés de l'adolescence, le gouverneur de l'Etat de Californie a approuvé une loi sur le droit des mineurs à l'oubli numérique[186]. Cette loi, dite « eraser law », consacre la protection de la vie privée

[185] Guidelines on the implementation of the Court of Justice of the European Union judgment on"Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González », G29, 26 novembre 2014.
[186] Senate Bill No. 568, Privacy: Internet: minors, approved by Governor on September 23, 2013.

des mineurs dans le monde numérique. Elle est entrée en vigueur le 1er janvier 2015[187]. La section 22581 de la loi permet aux mineurs d'effacer toute trace numérique (commentaire irréfléchi, photographie compromettante) dont il ne mesurait pas la portée au moment de sa publication sur Internet. Ce droit à l'oubli numérique, également appelé droit à l'effacement, qui a essentiellement vocation à s'appliquer aux réseaux sociaux, vise également tous les sites Internet et les applications pour mobile. La loi californienne impose aux opérateurs de garantir aux mineurs la possibilité d'enlever les informations sans qu'ils aient besoin de justifier leur demande[188].

La loi californienne constitue une innovation juridique en droit américain. Cependant, sa portée doit être relativisée. En effet, la demande de suppression ne peut porter que sur des informations publiées par le mineur intéressé lui-même. Les commentaires et photographies postés par des tiers, voire les informations diffusées par lui et reprises par les tiers, ne peuvent être retirés à sa demande. En outre, le législateur américain a prévu de nombreuses exceptions à l'exercice du droit à l'oubli[189]. La loi prévoit également une alternative à l'effacement de l'information. Elle permet à l'opérateur de procéder à l'anonymisation des données afin que le mineur ne puisse plus être identifié.
Enfin, le défaut majeur de la loi vise les bénéficiaires du droit à l'oubli. Seuls les mineurs ressortissant de l'Etat californien jouissent de ce droit, dont ils ne peuvent plus se prévaloir une fois soufflées leurs 18 bougies, ce qui restreint drastiquement l'utilité et l'efficacité du droit à l'effacement[190].

En France, le droit à l'oubli a été évoqué pour la première fois par l'autorité judiciaire en 2009. Un particulier avait demandé à un éditeur de supprimer les informations le concernant et faisant état d'une procédure ouverte à son encontre par la Commission des opérations de bourse, alors même qu'il avait ultérieurement été blanchi[191]. Le tribunal a alors considéré qu'à l'heure de la mémoire numérique, le droit à l'oubli doit être revendiqué comme « un droit élémentaire ».

---

187 Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, N. Martial-Braz et E. Gattone, Recueil Dalloz, p2788, 2013.
188 Section 1, Chapter 22.1. Privacy Rights for California Minors in the Digital World, 22581, (a).
189 Section 1, Chapter 22.1. Privacy Rights for California Minors in the Digital World, 22581, (b).
190 Section 1, Chapter 22.1. Privacy Rights for California Minors in the Digital World, 22580, (d).
191 TGI de Paris, 25 juin 2009, C. Vernes c/SAS les Echos, légipresse N°266, III p. 215, novembre 2009.

Ce contentieux a été suivi d'un dépôt de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique »[192]. Adoptée par le Sénat le 23 mars 2010, cette loi n'a cependant pas été promulguée.

La protection de la vie privée a été inscrite, par l'adoption de la « Charte sur le droit à l'oubli numérique » le 13 octobre 2010, au titre des objectifs que doivent poursuivre les éditeurs de site, principalement les représentants des sites collaboratifs[193]. Les signataires se sont engagés à expliquer aux utilisateurs les précautions à prendre avant de publier leurs données, leur permettre d'y avoir accès pour apprécier l'étendue des données communiquées, et leur assurer un droit à la rectification et à la suppression. Cependant, si la Charte a été signée par une douzaine d'entreprises (Copainsdavant, Skyblog, Viadeo etc.), les gros acteurs du net dont Facebook et Twitter ne s'y sont pas pliés. Il est regrettable également que le texte ne soit pas contraignant.

L'évolution des règles devrait finalement être actée par la révision de la directive de 1995. Une proposition de Règlement relatif au « droit à l'oubli numérique et à l'effacement » a été rendue publique par la Commission européenne en janvier 2012[194]. Le règlement, dont la nature a vocation à unifier les règles sur l'ensemble du territoire européen, consacre un droit à l'effacement des données[195]. Le projet de règlement a été adopté par le Parlement européen le 12 mars 2014. Sa promulgation devrait intervenir au second semestre 2015 s'il est voté par le Conseil européen. Le texte arroge à toute personne intéressée le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant et la cessation de la diffusion de ces données lorsque la conservation des données est inadéquate à la finalité du traitement, lorsque le traitement n'est pas conforme au règlement, lorsque la personne demanderesse retire son consentement au traitement, ou lorsqu'elle s'y oppose[196]. A la différence de la loi californienne, le droit à l'effacement serait invocable par tous les internautes, mineurs comme majeurs. Afin d'appréhender l'hypothèse des publications multiples des données dont est

[192] Proposition de loi n°331 visant à mieux garantir le droit à la vie privée à l'heure du numérique, déposée par Y. Détraigne et A.M. Escoffier, 24 février 2010.
[193] "Une charte sur le droit à l'oubli sur internet, sans Google ni Facebook", La tribune.fr du 13 octobre 2010
[194] Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.
[195] Le « droit à l'oubli numérique » en Europe et en Californie, C. Castets-Renard et G. Voss, RLDI, n°100, 2014.
[196] Article 17 I de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.

demandé l'effacement, le projet de règlement impose aux responsables du traitement qui auraient rendues publiques les données d'informer les tiers de la demande d'effacement, afin que ceux-ci puissent prendre la mesure de la demande et puissent procéder eux-mêmes à l'effacement de ces données sur leurs sites[197].

Si le projet de règlement ne prévoit pas de protection spécifique pour les enfants, l'article 8 est néanmoins consacré aux conditions dans lesquelles le traitement de données à caractère personnel relatives aux enfants peut être licite. Lorsque l'enfant a moins de 13 ans, le consentement doit être donné ou le traitement autorisé par le parent ou la personne qui a la garde de l'enfant. Le responsable du traitement doit s'efforcer « raisonnablement d'obtenir un consentement vérifiable, compte tenu des moyens techniques disponibles »[198].

Ce texte, censé améliorer la protection de la vie privée et des données des internautes, est pourtant accusé de ne pas être à la hauteur des attentes. Il proclamerait des droits qui se déduisent déjà de la directive de 1995 telle qu'elle est actuellement rédigée. En outre, il prévoit un certain nombre d'exceptions au droit à l'effacement[199]. Le responsable n'est pas tenu de faire droit à la demande d'effacement lorsque la conservation des données personnelles est nécessaire à l'exercice du droit à la liberté d'expression, pour des motifs d'intérêt général dans le domaine de la santé publique, à des fins de recherche historique, statistique et scientifique, ou encore au respect d'une obligation légale. Les responsables du traitement peuvent également se prévaloir d'une alternative à l'effacement des données, susceptible d'atténuer la portée du droit à l'effacement, leur permettant de conserver les données en en limitant le traitement. Une partie de la doctrine relève que le projet de règlement n'assure pas une suppression totale des données. Les informations publiées ou copiées par des tiers ne sont pas couvertes par le droit à l'effacement. Or, à l'heure des réseaux sociaux, les informations personnelles concernant un individu, et notamment un mineur, sont tout autant publiées par lui

[197] Article 17 II de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.
[198] Article 8 de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.
[199] Article 17 III de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, 25 janvier 2012.

que par les autres, ce qui aurait pour conséquence de réduire le droit à l'effacement à un droit symbolique[200].

Le droit à l'oubli tel qu'il est envisagé par le projet de règlement européen ne fait pas l'unanimité. Des auteurs craignent notamment les effets pervers qui peuvent en être la conséquence[201]. Le droit à l'oubli peut en effet représenter un danger vis-à-vis des adolescents, qui assoiront éventuellement leur confiance sur l'existence d'un tel droit et ne se sentiront plus concernés par le contrôle des publications d'informations les concernant.

Face à un droit à l'oubli qui n'existe pas mais qui présente déjà des défauts, l'action la plus efficace semble être, une fois de plus, l'éducation et la sensibilisation des enfants et adolescents à la problématique des données personnelles, doctrine partagée par le gouvernement. Interpellé par des députés, le Gouvernement a souligné l'importance cruciale de la vie privée et plus particulièrement de celle des mineurs[202]. Dans sa réponse, il évoque l'impératif d'un volet éducatif sur les nouveaux usages numériques et dresse les mesures adoptées en ce sens. Ainsi, « dans le plan gouvernemental « Faire entrer l'école dans l'ère numérique », des programmes spéciaux sont prévus afin de renforcer la sensibilisation et la vigilance des adolescents vis-à-vis des médias numériques ». Il semble nécessaire de poursuivre ces actions, voire de les renforcer. Une campagne de sensibilisation s'avère également essentielle pour informer les citoyens des droits qui leur sont reconnus. Un sondage Eurobaromètre a en effet dénoncé la méconnaissance des internautes de la loi Informatique et Libertés et des droits qu'elle consacre[203].

L'enfant ne maîtrise pas la portée d'Internet. Il est indispensable de lui offrir les droits lui permettant de protéger sa vie privée d'adulte en devenir et d'adulte qu'il sera devenu. Une protection pleine et entière de l'enfant implique également sa connaissance de l'existence des comportements répréhensibles sur Internet. L'enfant doit être en mesure d'identifier ces comportements afin de ne pas les adopter.

---

[200] Le « droit à l'oubli numérique » en Europe et en Californie, C. Castets-Renard et G. Voss, RLDI, n°100, 2014.
[201] « Le droit à l'oubli sur internet : une idée dangereuse », S. Tisseron, Libération, 6 décembre 2012.
[202] « Question écrite n°49646 de M. G. Bui », questions.assemblee-nationale.fr, publié le 11.02.2014.
[203] La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information, Rapport d'information n°441 déposé au Sénat, Y. Détraigne et A.M. Escoffier.

Chapitre 2. Les comportements cybercriminels de l'enfant sur Internet

Internet n'est pas un lieu de totale liberté. Les enfants doivent mesurer leurs comportements. Les infractions qu'ils peuvent commettre sont « classiques », en ce sens qu'elles s'appliquent à tous les internautes (Section 1). Une infraction est néanmoins particulièrement fréquente chez les mineurs : le cyber-harcèlement (Section 2).

Section 1. Les infractions classiques commises sur Internet

L'enfant ne doit ni porter atteinte aux droits d'autrui (II), ni abuser de la liberté d'expression au cours de son activité numérique (I).

I. Une limite à l'expression : l'abus de droit

« Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières »[204]. Fondamentale à toute société démocratique, l'expression libre doit être garantie à tous les ressortissants français[205]. Cependant, elle peut également faire l'objet de restrictions. Les limites à la liberté d'expression doivent être prévues par la loi et constituer des mesures nécessaires, dans une société démocratique, pour atteindre des objectifs d'intérêt général, tel que le maintien de l'ordre public, de la sécurité nationale, de la santé publique ou encore de la sûreté publique[206].
En outre, la liberté d'expression est un droit qui n'est pas protégé lorsqu'il fait l'objet d'abus. L'abus de droit est évoqué à l'article 17 de la CEDH : « aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un Etat, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention ».

[204] Article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950.
[205] Article 11 de la Déclaration des droits de l'homme et du citoyen, 26 août 1789.
[206] Article 10 alinéa 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950.

En application de cet article 17 et de l'alinéa second de l'article 10, la CEDH exclut de la protection de l'article 10 de la Convention certains propos[207]. La diffamation et l'injure, délits prévus par la loi sur la liberté de la presse, sont au nombre des ces exclusions.

La diffamation consiste en « une allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé »[208]. L'allégation est le fait de reprendre des propos attribués à des tiers. Pour être diffamatoire, l'allégation doit se présenter sous la forme d'une articulation précise de faits de nature à être, sans difficulté, l'objet d'une preuve ou d'un débat contradictoire[209]. Il faut un « fait précis », de façon à distinguer la diffamation de la simple expression d'une opinion. L'imputation est l'affirmation personnelle qu'un fait, acte ou parole, est attaché à une personne.

La différence entre l'injure et la diffamation est ténue. L'injure est « un propos qui, sans contenir l'imputation d'aucun fait, porte atteinte à l'honneur ou à la dignité de la personne visée et renvoie d'elle une image dégradante »[210]. Cette définition recouvre toute expression outrageante, mépris ou invective.

La diffamation et l'injure sont pénalement réprimées. Elles sont constitutives de délits lorsqu'elles sont publiques, de contraventions lorsqu'elles ne le sont pas[211]. La publicité du propos s'entend de sa communication au public par l'un des moyens prévus à l'article 23 de la loi sur la liberté de la presse, soit notamment par « tout support de l'écrit, de la parole, de l'image », ainsi que « tout moyen de communication au public par voie électronique ». Il est privé lorsqu'il est adressé à un groupe de personnes déterminé, non accessible aux personnes étrangères à ce groupe.

La sanction pénale de la diffamation et de l'injure est fonction de la qualité de la victime, du mobile et du support. Ainsi, la diffamation et l'injure publique commises

[207] Convention européenne des droits de l'homme, P. Dourneau-Josette, juin 2013.
[208] Article 29 de la loi du 29 juillet 1881 sur la liberté de la presse.
[209] Ass plén, 25 juin 2010, n°08-86.891, note V. Vigneau, Chronique de jurisprudence de la Cour de cassation, D. 2010, p 2090.
[210] Cass crim, 20 juin 1946, gaz pal 1946, n°2, p 178.
[211] Droit de la presse, E Dreyer, D. 2015, p 342.

envers les personnes physiques sont punies d'une amende de 12 000 euros[212]. La diffamation et l'injure non publiques envers une personne sont punies de l'amende prévue pour les contraventions de la 1ère classe[213], le montant de l'amende pour cette classe de contraventions étant fixé à 38 euros[214].

La diffamation a pris une forme nouvelle avec le développement d'Internet et l'apparition des blogs et réseaux sociaux[215]. En effet, toutes les publications sur Internet, même adressées à un public restreint, sont soumises à la loi sur la presse. La difficulté propre à cet outil relève de l'appréciation du caractère public du propos litigieux. Dans une décision du 9 juin 2006, le Tribunal d'instance de Strasbourg a ainsi considéré qu'une diffamation sur Internet n'est pas nécessairement publique. Il s'agit alors de déterminer les destinataires d'un propos diffamatoire. En effet, le caractère public des messages nécessite la réunion de deux éléments. Il faut qu'il y ait une multiplicité de destinataires, et que ces destinataires ne soient pas liés entre eux par une communauté d'intérêts[216].

Les forums de discussion sont considérés comme étant des lieux privés dès lors que leur accessibilité suppose une sélection des internautes. Cette sélection permet en effet de garantir un nombre restreint d'intervenants sur le forum, et une communauté d'intérêts entre eux[217]. Cependant, dès lors que les messages sont librement consultables ou que tout visiteur peut y poster un message sans condition d'inscription sur le forum, le forum revêt la qualité de lieu public[218].

Les blogs et les pages personnelles sur Internet sont publiques lorsque le « site est accessible à tous les internautes désireux de le visiter ou au hasard d'une recherche, quel que soit le centre d'intérêts qui les y conduit »[219].

De même, il n'existe pas de régime juridique propre pour les messages publiés sur les réseaux sociaux. Leur caractère public ou privé dépend d'une appréciation casuistique. La Cour de cassation a eu à connaître des propos injurieux publiés sur

[212] Articles 32 et 33 de la loi du 29 juillet 1881 sur la liberté de la presse.
[213] Articles R 621-1 et R 621-2 du Code pénal.
[214] Article 131-13 du Code pénal.
[215] « La cybercriminalité », F. Chopin, Rubrique du Répertoire Pénal Dalloz, juillet 2013.
[216] Crim, 19 février 1863, Bull Crim n°56.
[217] CA Paris, 1re ch., 5 juin 2003, Comm. com. électr. 2004, comm. 35.
[218] Tribunal d'instance de Strasbourg, 9 juin 2006.
[219] CA Paris, 11è ch., 6 juin 2007, Mairie de Puteaux / Christophe G.

Facebook et MSN[220]. Après avoir constaté que le compte Facebook de l'auteur des propos litigieux n'était accessible qu'aux personnes dûment agréées par lui, les juges en ont déduit qu'il existait une communauté d'intérêts entre ces personnes, de telle sorte que les propos ne pouvaient être constitutifs d'une diffamation publique. Le caractère public ou privé du réseau est donc affaire de paramétrages[221].

Il faut noter néanmoins la précision qui a été faite par la Cour quant aux destinataires du message. Elle relève leur « nombre très restreint ». Dès lors, plusieurs questions peuvent être soulevées. Le nombre de destinataires était-il déterminant dans la solution présentée par la Cour ? Le cas échéant, quel est le nombre de destinataires au-delà duquel le compte Facebook est considéré comme étant un lieu public ? Ces questions restent ouvertes actuellement, l'autorité judiciaire n'ayant pas eu l'occasion d'y répondre.

Le réseau social Twitter a quant à lui été jugé comme étant un lieu public. En effet, les tweets postés depuis un compte, étant librement accessibles par tous les utilisateurs du site, sont considérés comme relevant de l'espace public, malgré la possibilité de sélectionner les personnes pouvant les lire, insuffisante à les rendre privés.

Les jeunes internautes sont très présents sur Internet, et notamment sur les pages susvisées : forums de discussion, blogs et réseaux sociaux. Ils sont nés avec ces outils interactifs, qu'ils utilisent quotidiennement. Cette navigation peut leur apparaître comme un prolongement des discussions entamées dans la cour de récréation. Or, ils n'ont pas toujours conscience que les propos qu'ils tiennent sur Internet ne relèvent plus de la sphère de leur intimité. L'injure prononcée sur Internet reste un délit (ou le cas échéant une contravention) pénalement répréhensible en dépit de la minorité de son auteur, la loi française s'imposant à tous.

Le régime de responsabilité pénale du mineur est prévu à l'article 122-8 du Code pénal. Le législateur accorde une importance au discernement de l'enfant quant au prononcé de la sanction. Seuls les mineurs capables de discernement sont pénalement responsables. L'absence de discernement est présumée, de manière irréfragable, comme étant totale chez le mineur de dix ans ou moins. Les mineurs de dix à treize ans ne peuvent voir prononcer à leur encontre que des mesures

[220] Cass, 1ère Civ, 10 avril 2013, n°11-19.530, note, A. Lepage, com com électr., n°81, 2013.
[221] Chronique de jurisprudence de droit de la presse, P. Piot, Gazette du Palais, juin 2013, p 14.

éducatives. A partir de treize ans, un mineur peut être condamné à une peine. Il bénéficie alors d'une excuse de minorité, qui constitue une atténuation de sa responsabilité pénale et une diminution de la peine qu'il encourt[222].

Les mineurs peuvent donc être pénalement coupables de diffamation ou d'injure, et plus généralement de toutes les infractions de presse qu'ils commettent, pour des propos publiés sur Internet. De manière non exhaustive, les mineurs peuvent ainsi être jugés responsables d'apologie (de crimes de guerre ; de crimes contre l'humanité ; des actes terroristes[223], etc.)[224], de provocation (à la discrimination, à la haine ou à la violence en raison de l'origine, de l'appartenance ou de la non-appartenance à une ethnie, une nation, une race ou une religion déterminée ; à atteindre à la vie ; à commettre une agression sexuelle ; à la commission d'actes terroristes ; etc.)[225], de contestation des crimes contre l'humanité[226]. Or, les jeunes internautes tiennent régulièrement de tels propos condamnables. Un malheureux constat en a ainsi été dressé à la suite des attentats terroristes du 7 janvier 2015 dirigé contre le journal Charlie Hebdo. De nombreux mineurs ont prononcé leur soutien aux frères Kouachi sur les réseaux sociaux. Dans pareilles circonstances, il semble nécessaire de promouvoir, au-delà de la justice éducative, de véritables mesures d'éducation. Dans leur apprentissage d'Internet, il faut informer les enfants de leurs droits, leur apprendre que ces droits ne sont pas sans limite, et les avertir des sanctions attachées à ces limitations.

Le même travail d'éducation doit prévenir les enfants d'attenter aux droits d'autrui.

II. Les atteintes au droit d'autrui

Le droit à la vie privée est consacré tant en droit interne qu'en droit international[227]. En droit français, le droit à la vie privée est visé à l'article 9 du Code civil. Les contours de la notion ont été définis par la jurisprudence. Relèvent ainsi de la vie privée, à titre d'exemple, la vie sentimentale, la religion, les opinions politiques, le patrimoine d'une personne. Le droit à l'image est un attribut de la personnalité,

[222] Article 20-2 de l'ordonnance n°45-174 du 2 février 1945 relative à l'enfance délinquante.
[223] La loi du 14 novembre 2014 sur « la lutte contre le terrorisme » a intégré le délit d'apologie dans le Code pénal.
[224] Article 24 de la loi du 29 juillet 1881 sur la liberté de la presse.
[225] Articles 23 et 24 de la loi du 29 juillet 1881 sur la liberté de la presse.
[226] Article 24 bis de la loi du 29 juillet 1881 sur la liberté de la presse.
[227] Article 8 CEDH, Article 7 de la Charte européenne des droits fondamentaux.

distinct du droit à la vie privée, qui se déduit de l'article 9 susvisé[228]. Le droit à l'image est un droit absolu. Toute personne peut s'opposer à sa reproduction sans son autorisation expresse et spéciale, (en ce qu'elle doit être obtenue pour chaque mode de diffusion)[229], même si le protagoniste a consenti à être photographié, et indépendamment de l'existence de tout lien familial ou amical. En sus de l'autorisation personnelle du mineur, la publication de son image requiert l'obtention de l'accord du ou le cas échéant des titulaires de l'autorité parentale. A défaut, et dès lors que la personne est identifiable[230], la publication de sa photographie constituera une atteinte à son droit à l'image, de nature à engager la responsabilité civile de l'auteur de la publication[231], quand bien même serait-il mineur.

Le développement d'Internet multiplie les risques d'atteinte à la vie privée d'autrui, notamment par les mineurs. En effet, les jeunes internautes partagent un grand nombre de photographies les mettant en scène, seuls ou avec des amis, ou mettant en avant ces derniers, sur les blogs et autres réseaux sociaux[232].
Une étude locale révèle ainsi que 22% de lycéens ont déjà posté des photographies de leurs amis sans leurs accords. Ce faible pourcentage peut sembler surprenant. Basé sur les déclarations personnelles des internautes interrogés, il est possible de suspecter le nombre de publications irrégulières plus élevé. Quoi qu'il en soit, ces jeunes internautes qui publient des photographies sans en obtenir l'autorisation ne sont pas toujours conscients d'atteindre à l'image d'autrui et d'engager leur responsabilité ce faisant. Bien que les contentieux soient rares et qu'ils se résolvent essentiellement à l'amiable, il peut être intéressant, dans le cadre de l'éducation des enfants aux médias, de leur expliquer les règles de droit applicables et les risques encourus lorsqu'elles sont méconnues.

De même, il est nécessaire de familiariser les jeunes internautes avec le délit d'usurpation d'identité, qui constitue une atteinte à la vie privée, à l'honneur et à la réputation de la personne dont l'identité a été usurpée. Ce délit a été crée par la loi n°2011-267 du 14 mars 2011 dite LOPPSI 2. Ainsi, le fait d'usurper l'identité d'un

[228] Civ. 1ère, 10 mai 2005, A. Lepage, Dalloz 2005, p 2643.
[229] CA Paris, 1ère Ch., 23 mai 1995, Hassier, Dalloz 1996, p75.
[230] 1ère Civ, 21 mars 2006, obs A. Lepage, Dalloz 2006, p 2702.
[231] Article 1382 du Code civil.
[232] Facebook et ses pratiques en collège et lycée, Enquête dans les collèges et lycées de l'académie de Dijon, avril 2012.

tiers est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne[233]. 64% des jeunes reconnaissent qu'il existe un grand risque d'usurpation d'identité sur Facebook[234]. Il n'est pas certain qu'ils soient aussi nombreux à connaître le caractère illicite de cette pratique et ses conséquences juridiques.

Enfin, l'une des plus grosses atteintes au droit d'autrui qui a accompagné le développement d'Internet est relative au droit d'auteur. Rapidement, le législateur a souhaité appréhender le numérique pour offrir une protection aux œuvres, principalement radiophoniques, audiovisuelles et littéraires. Les fournisseurs doivent ainsi développer des moyens techniques permettant de prévenir les atteintes au droit d'auteur et en informer leurs abonnés[235]. Ils doivent rappeler que le piratage nuit à la création artistique lorsqu'ils offrent aux utilisateurs la possibilité de télécharger des fichiers dont ils ne sont pas les fournisseurs[236]. L'exploitation numérique des œuvres a ensuite fait l'objet d'une réglementation européenne[237], transposée en 2006 par la loi dite DADVSI relative au droit d'auteur et aux droits voisins dans la société de l'information[238]. Cette loi appréhende la problématique du téléchargement illégal, renforcée par la lutte contre le piratage issue des lois Hadopi I et II[239]. Le téléchargement est un processus de transfert, à partir d'un ou plusieurs ordinateurs d'uploaders [qui envoient les données], aboutissant à l'enregistrement, sur le disque dur de l'ordinateur du downloader [qui reçoit les données], d'une copie d'une œuvre ou d'autres données protégées par un droit de propriété intellectuelle »[240]. Le téléchargement d'œuvres est illicite « lorsqu'il porte sur des œuvres protégées dont la diffusion numérique n'a pas été autorisée par les ayants-

[233] Article 226-4-1 du Code pénal.
[234] Facebook et ses pratiques en collège et lycée, Enquête dans les collèges et lycées de l'académie de Dijon, avril 2012.
[235] Article 6 I. 1 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[236] Article 7 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[237] Directive européenne n°2001/29 du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[238] Loi n°2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.
[239] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet et loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.
[240] Avis n°2005-2 du Conseil supérieur de la propriété littéraire et artistique relatif à la distribution des œuvres en ligne, Code de la propriété intellectuelle, dispositions communes, Dalloz, 7ème édition, 2007, p 906-907.

droit »[241]. De la même façon, la pratique du peer-to-peer (pair-à-pair) est une forme de téléchargement illégale. Elle implique l'échange de fichiers par l'internaute en contrepartie de la reproduction sur son disque dur de fichiers mis à disposition par d'autres utilisateurs[242].

D'une part, la mise à disposition d'un logiciel permettant le téléchargement est réprimée par la loi[243]. D'autre part, le téléchargement d'une oeuvre, quelle que soit sa forme (direct download ou peer-to-peer), est qualifié d'acte de contrefaçon lorsqu'il est rendu possible sans l'autorisation de son auteur[244]. Les actes de contrefaçon sont punis de trois ans d'emprisonnement et 300 000 euros d'amende[245]. L'internaute qui met à disposition l'œuvre est coupable de contrefaçon, aussi bien que l'internaute qui télécharge, ce-dernier effectuant ainsi une reproduction non autorisée de l'œuvre. Cependant, le législateur a prévu une procédure spécifique contre les délits de contrefaçon d'œuvres via Internet. La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet est une autorité administrative indépendante créée afin d'appliquer une réponse graduée au téléchargement illicite. Cette réponse comporte trois étapes[246]. En premier lieu, l'abonné reçoit de la Commission de protection des droits de l'Hadopi un mail d'avertissement. En cas de réitération de son comportement illicite dans les six mois suivants cet avertissement, il est envoyé un second avertissement à l'abonné, par message électronique et lettre remise contre signature. La troisième étape consiste à informer l'abonné contre lequel aura été constaté de nouveaux faits de téléchargement commis dans un délai d'un an suivant la date de présentation de la seconde recommandation que ces faits sont susceptibles de poursuites pénales. L'internaute encourt alors des sanctions pécuniaires. Il peut être condamné pour négligence[247] et être attaqué pour contrefaçon par l'auteur qui aura subit un préjudice.

Il existe une forme de téléchargement qui présente une certaine originalité. Le streaming est la diffusion et l'accès en flux continu d'une œuvre qui implique son

[241] Loi DADVSI : mesures pénales, civiles et de prévention, Etude n°271-30, Lamy Droit des médias et de la communication, novembre 2000.
[242] « Peer to peer » exception de copie privée et droit d'auteur, Lamy Droit du numérique, 2014.
[243] Article L 335-2-1 du Code de la propriété intellectuelle.
[244] Article L 335-4 du Code de la propriété intellectuelle.
[245] Article L 335-2 du Code de la propriété intellectuelle.
[246] Article L 331-25 du Code de la propriété intellectuelle.
[247] Article R 335-5 du Code de la propriété intellectuelle.

téléchargement provisoire chez l'internaute[248]. Par exemple, les contenus visionnés sur Youtube le sont en streaming. Si le diffuseur est considéré comme un contrefacteur au même titre que pour le téléchargement direct ou le peer-to-peer, la qualification juridique du spectateur est actuellement incertaine en France. En effet, la loi n'interdit pas la simple consultation d'une œuvre, quand bien même serait-elle contrefaite. Une partie de la doctrine a proposé de condamner les utilisateurs de streaming pour recel de contrefaçon[249]. « Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, […], 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, du produit d'un crime ou d'un délit »[250]. Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende. Toutefois, le recel étant un délit, il est exigé que soit rapportée la preuve et d'un élément matériel, et d'un élément moral pour le caractériser. Or, cet élément moral n'existe pas nécessairement dans la pratique du streaming. En effet, les internautes peuvent avoir accès aussi bien à du streaming légal qu'à du streaming illégal (preuve en est sur Youtube où le contenu proposé aux internautes peut avoir été volontairement déposé par l'auteur d'une œuvre). La distinction de ces différentes formes de streaming n'étant pas aisée, l'intention de visionner du contenu illégal peut faire défaut chez les utilisateurs[251]. Ce fondement devra donc être clarifié par les juges.

Une étude de l'association de lutte contre la piraterie audiovisuelle révèle que près de 13 millions de Français ont consulté des sites dédiés au téléchargement en 2014[252]. Les jeunes internautes sont des consommateurs importants de contenus accessibles au téléchargement ou au streaming. 64,2% des enfants tous âges confondus avouaient faire un usage régulier du téléchargement en 2010, quelle que soit la forme qu'il emprunte[253]. Si les 15-18 ans semblent plus concernés par le droit d'auteur que leurs aînés, le visionnage en streaming a tendance à être considéré « a priori » comme licite[254], ce qui expliquerait son augmentation récente[255]. Les plus

[248] Le droit de reproduction de l'auteur d'une œuvre musicale, Etude n°477-22, Lamy Droit des médias et de la communication, novembre 2000.
[249] Le streaming, légal ou illégal ?, A. Dimeglio et M-D. Gleize, revue électronique Le Journal du Net, 3 juin 2008.
[250] Article 321-1 du Code pénal.
[251] La propriété intellectuelle à l'ère du streaming : quelle répression ?, A. Jaber, RLDI, 2011, n°77.
[252] La consommation illégale de vidéos sur Internet en France, Période 2009/2014, Etude de l'ALPA, 1er avril 2015.
[253] Comprendre le comportement des enfants et adolescents sur Internet pour les protéger des dangers, enquête sociologique menée par l'association Fréquence écoles, 2010.
[254] Perceptions et pratiques de consommation des « Digital Natives » en matière de biens culturels dématérialisés, Etude qualitative, Hadopi, Janvier 2013.

gros consommateurs sont les 25-34 ans. Il est trop tôt pour expliquer cette différence de consommation entre les deux générations, et l'accès de conscience de la plus jeune quant au droit d'auteur.
La Haute Autorité se demande néanmoins s'il ne faut pas accueillir ces résultats comme les bienfaits des politiques de prévention menées par les médias, l'école et les parents. Il semble alors que ces politiques doivent être conservées et renforcées. Il faut notamment orienter les campagnes sur le téléchargement en streaming, dont l'illicéité n'est pas suffisamment connue des jeunes internautes.

Aux-côtés des infractions classiques que les enfants peuvent commettre sur Internet, il est un comportement répréhensible qui leur est quasi-propre, étant particulièrement répandu chez ces jeunes internautes.

Section 2. Une infraction répandue chez les mineurs : le cyber-harcèlement

Véritable sujet, le cyber-harcèlement est la prolongation sur Internet du harcèlement traditionnel. Alors qu'il s'est rapidement imposé comme l'un des dangers les plus importants auquel un enfant peut être confronté, il a longtemps été méconnu de l'opinion publique et sa portée minimisée (I). L'heure est désormais à la prévention de ce fléau et la responsabilisation aussi bien des enfants, des parents, des enseignants que de l'ensemble de la communauté web (II).

I. Un fléau mésestimé

Le harcèlement est un comportement répété se manifestant par des propos ou des actes physiques dont la conséquence se traduit par une pression psychologique chez la victime.
Le harcèlement est protéiforme. Le harcèlement sexuel est connu et régulièrement dénoncé. Le harcèlement moral est souvent associé aux milieux professionnel et scolaire. Le harcèlement sur Internet, (le cyber-harcèlement), silencieusement délaissé jusqu'à récemment, a fait l'objet d'une récente mobilisation.

[255] La consommation illégale de vidéos sur Internet en France, Période 2009/2014, Etude de l'ALPA, 1er avril 2015.

Le cyber-harcèlement ne se confond pas avec le harcèlement traditionnel, qui existait bien avant la naissance d'Internet. Le cyber-harcèlement, francisation du terme anglais « cyberbullying », est un « acte agressif, intentionnel perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule »[256]. Le cyber-harcèlement se pratique donc majoritairement via Internet, sur les forums, les tchats, les jeux en ligne, les courriers électroniques et surtout les réseaux sociaux et les sites de partage de photographies et de vidéos. Il se pratique également par le biais des téléphones portables[257]. La CNIL relève néanmoins que le cyber-harcèlement a principalement lieu sur Facebook, par des messages adressés à la victime, la publication de photos ou vidéos compromettantes d'elle, voire la création d'une page la visant pour mieux la tourner en ridicule.
Le harcèlement virtuel peut emprunter plusieurs formes. Il peut s'agir d'intimidations, d'insultes, de moqueries, menaces en ligne, propagation de fausses rumeurs, piratage de comptes, publication de photos et/ou vidéos, création d'un sujet de discussion à l'encontre de la victime, et plus généralement tout ce qui est susceptible de porter atteinte à l'identité numérique d'une personne[258].

Le cyber-harcèlement implique la répétition d'actes, avec l'intention de blesser de la part de leur auteur, qui s'inscrivent dans un rapport de force déséquilibré – ce déséquilibre pouvant résulter de l'âge, du physique, du pouvoir de supériorité ou du nombre de harceleurs face à la victime[259]. Le lynchage peut également venir de la communauté web. Dans ce cas, les harceleurs et la victime ne se connaissent pas nécessairement. La victime aura le plus souvent posté une vidéo la représentant en train de réaliser une quelconque prestation (chant, vidéo humoristique à l'image des célèbres youtubers Cyprien, Norman fait des vidéos et autres). Sa prestation sera alors jugée, sans filtre, par les internautes l'ayant visionnée.

Le cyber-harcèlement est considéré comme étant le risque le plus important auquel un enfant est exposé sur Internet, peut-être parce que les harceleurs ont le sentiment de pouvoir agir impunément dès lors qu'un écran les sépare de leur

[256] Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russel, S., & Tippett, N. (2008).Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child, Psychology and Psychiatry, 49,p 376
[257] Les ados dans le cyberespace, prises de risque et cyberviolence. C. Blaya, 2013. De Boeck
[258] Le harcèlement sur internet en questions, CNIL, 02 novembre 2010.
[259] Avis n°6 de l'Observatoire des Droits de l'Internet concernant le Cyberharcèlement, février 2009.

victime, ou que cette distance leur donne le courage de l'agresser lâchement. 40% des collégiens et lycéens déclarent ainsi avoir été victimes de cyber-violence au moins une fois pendant l'année scolaire, les filles étant les cibles privilégiées[260]. Ce problème est souvent méconnu des parents, voire des enseignants, alors que son issue peut être tragique. En effet, s'il en est souvent la prolongation, le cyber-harcèlement est accusé d'être plus radical que le harcèlement traditionnel. De par ses caractéristiques propres, les conséquences du harcèlement sur Internet sont psychologiquement plus lourdes pour la victime. Alors que le harcèlement traditionnel s'arrête aux portes de l'établissement scolaire, Internet permet aux harceleurs de traquer leur victime au cœur même de son intimité, sans la supervision qu'il peut y avoir dans la cour de récréation. Sous couvert d'anonymat, la victime ne connaît pas toujours l'identité des harceleurs. Elle n'est pas non plus en mesure de déterminer le public qui a pu avoir connaissance des messages, leur diffusion étant massive sur ce réseau. Constamment exposée à cette violence, la victime étouffe, se sent isolée et en insécurité permanente.

Phénomène méconnu des parents, des enseignants et de l'opinion publique, le législateur n'en a que récemment mesuré l'importance.

Le cyber-harcèlement pouvait jusqu'alors être dénoncé au titre du harcèlement moral. Consacré à l'article 222-33-2 du Code pénal, le harcèlement moral est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Il était possible également de réprimer ces comportements en s'attachant aux effets qu'il produisait, comme la diffamation ou l'injure.

Ce délit a finalement été consacré par la loi pour l'égalité entre les femmes et les hommes, en tant que circonstance aggravante du harcèlement[261]. L'article 222-33-2-2 du Code pénal a une portée large et ne vise pas expressément le harcèlement virtuel. Il punit d'un an d'emprisonnement et de 15 000 euros d'amende le fait de harceler une personne qui se traduit par une altération physique ou mentale de la santé de la victime. Lorsque ce fait a été commis par l'utilisation d'un service de communication au public en ligne, la peine est aggravée, l'auteur encourant alors deux ans d'emprisonnement et 30 000 euros d'amende. Elle sera de trois ans d'emprisonnement et 45 000 euros d'amende lorsque ces faits commis par Internet ont, en outre, visé un mineur de quinze ans.

[260] Guide pratique pour lutter contre le cyber-harcèlement entre élèves.
[261] Loi n°2014-873 du 4 août 2014 pour l'égalité entre les femmes et les hommes.

Le cas échéant, le harceleur peut engager sa responsabilité pénale pour provocation au suicide lorsque ses propos tendent en ce sens. La provocation au suicide est punie de 3 ans d'emprisonnement et de 45 000 euros d'amende lorsqu'elle a été suivie du suicide ou d'une tentative de suicide, et de
5 ans d'emprisonnement et de 75 000 euros d'amende lorsque la
victime a moins de 15 ans[262].

La loi pour l'égalité entre les femmes et les hommes est également venue appréhender la pratique du « happy slapping », qui s'est répandue en 2014[263]. Le happy slapping consiste à filmer ou photographier l'agression d'une personne et à la diffuser sur Internet. Cette pratique est désormais punie de 5 ans d'emprisonnement et de 75 000 euros d'amende[264].

Les peines nouvellement créées par le législateur ne peuvent être prononcées qu'après plainte, ouverture d'une enquête et décision de justice.
Avant que n'aboutisse cette longue procédure, la CNIL recommande aux victimes du harcèlement virtuel d'utiliser les outils proposés par les sites pour dénoncer les propos et comportements répréhensibles. Lorsque les messages arrivent par SMS ou courriers électroniques, la victime doit enregistrer l'auteur comme contact « indésirable » afin de bloquer tous les messages en sa provenance.
La CNIL est compétente pour connaître des cas de harcèlement sur Internet. Saisie par les victimes, elle les aide à obtenir la suppression des propos et photographies qui leur portent préjudice.
Une ligne d'écoute adressée aux victimes est ouverte du lundi au vendredi de 9h à 19h, l'appel étant gratuit, anonyme et confidentiel.

Si, malgré la reconnaissance juridique du cyber-harcèlement, les sanctions ne tombent pas toujours, surtout lorsque les harceleurs sont mineurs, Catherine Blaya, présidente de l'Observatoire international de la violence à l'école, regrette la criminalisation du harcèlement virtuel, à laquelle elle préfère une politique fondée sur la prévention et l'éducation[265].

[262] Article 223-13 du Code pénal.
[263] « Un groupe d'adolescentes violentes en garde à vue à Nice », Nice-Matin, 21 février 2014.
[264] Article 222-33-3 du Code pénal.
[265] Comment combattre la cyber-violence à l'école ?, M. Maillard, Le Monde, 2 décembre 2014.

II. Une nécessaire responsabilisation

Le cyber-harcèlement était à l'honneur à l'occasion des premières Assises Nationales sur le harcèlement à l'Ecole des 2 et 3 mai 2011.

L'école est le lieu privilégié pour sensibiliser les enfants à la thématique du cyber-harcèlement. Au même titre que l'éducation sexuelle, la prévention relative au sida, aux dangers de la drogue et de l'alcool, l'école se doit de démocratiser le harcèlement et son équivalent virtuel. L'enseignement peut donc se faire à part entière, avec l'intervention de tiers pour ouvrir le dialogue et débat, ou être prévu dans le cadre du B2i. A cette fin, la CNIL propose un espace Internet dédié aux enseignants pour les accompagner dans le développement d'une éducation numérique. Il est fondamental que l'enfant assimile la notion et ses enjeux. Les éducateurs doivent apprendre aux enfants et adolescents à protéger leurs données et informations personnelles sur Internet. Ces-derniers doivent être en mesure de maîtriser les paramètres de confidentialité. Ils ne doivent pas communiquer leurs mots de passe. L'enfant doit faire attention à la nature de ses publications, qui peuvent être utilisées à son encontre. Il ne doit pas envoyer de photographies de lui a quiconque lui en fait la demande[266].

L'association e-enfance a réalisé un film « Derrière la porte », disponible sur le site netecoute.fr. La vidéo interactive confronte les jeunes internautes à différentes situations en les laissant choisir le déroulement de l'action. Chaque alternative est suivie d'un commentaire expliquant les conséquences du choix retenu et le régime juridique qui peut y être attaché. Tous les dangers du numérique y sont abordés : happy slapping, addictions aux jeux, cyber-harcèlement. Il peut sembler intéressant d'initier les jeunes enfants à cette forme d'apprentissage au cours, par exemple, d'une heure « de vie de classe ».

Plus généralement, il est indispensable que les collèges et lycées soient fournis en affiches préventives et soient plus nombreux à leur trouver une place sur les murs, notamment à l'infirmerie. En outre, les écoles doivent prévoir un règlement intérieur précisant les règles et les sanctions relatives à l'utilisation des nouvelles technologies.

[266] Chantages sexuels, harcèlement… Les ados pris au piège du net, A. Logeart, Le nouvel obs, 28 mars 2013.

L'objectif est de faire connaître ce problème, d'alarmer les potentiels jeunes harceleurs sur les graves conséquences qui peuvent en découler, de réfréner les comportements répréhensibles par la prise de conscience individuelle et d'encourager les victimes et les témoins à dénoncer ce phénomène.

Au-delà de son rôle à jouer quant à la prévention du cyber-harcèlement, l'éducation nationale doit apporter son soutien aux victimes. Les enseignants, en contact direct avec les enfants, doivent être attentifs aux signes qui peuvent résulter du cyber-harcèlement[267]. La victime peut ainsi devenir anxieuse, craintive, isolée, fatiguée, en prise avec des troubles du sommeil. Bien souvent, ses résultats scolaires chutent et l'intérêt de l'élève pour les activités diminue. Un comportement agressif et provocant peut également être perceptible chez l'auteur d'un harcèlement.
Bien sûr, ces signes ne sont peut-être pas liés à un quelconque harcèlement. Ils peuvent être le corollaire classique du passage de l'enfance à l'adolescence. Néanmoins, et dans la mesure du possible, les enseignants doivent être invités à s'expliquer le changement dans l'attitude d'un élève, afin d'identifier au plus vite, le cas échéant, un éventuel problème sous-jacent.
Lorsque des cas de harcèlement et de cyber-harcèlement sont identifiés, l'école doit prévenir les parents (et réciproquement) et prendre les mesures adéquates pour y mettre fin. Si ce n'est par obligation juridique, c'est par devoir moral que l'école, les enseignants et les proviseurs doivent prendre leur responsabilité. France 2 a récemment consacré un documentaire au harcèlement scolaire[268]. Edifiant, ce reportage révèle que les victimes sont bien souvent délaissées, leurs parents confrontés à une équipe éducative qui n'agit et ne réagit pas. Pire, un proviseur a prié la mère d'une victime de changer son fils d'établissement plutôt que de s'attaquer au problème qui sévissait dans son collège.
Il est impératif que ce genre de témoignage n'ait plus lieu d'être. Les sanctions disciplinaires doivent être exemplaires, exclusion provisoire voire définitive de l'auteur, obligatoirement suivies d'un rappel à l'ordre général de tous les élèves.

La lutte contre le harcèlement virtuel doit également passer par la responsabilisation de l'ensemble de la communauté du web.

[267] Guide pratique pour lutter contre le cyber-harcèlement entre élèves.
[268] Documentaire « Souffre-douleurs, ils se manifestent », réalisé par Andrea Rawlins Gaston et Laurent Follea, diffusé le 10 février 2015 sur France 2.

A cet effet Facebook a développé des outils de signalement du harcèlement sur sa plateforme[269]. Les signalements de harcèlement sont ainsi traités en 24h, les messages injurieux pouvant aussi bien être signalés par la victime que par les témoins du harcèlement.

Lancé par cette dynamique, Twitter avait alors annoncé vouloir lutter contre le harcèlement en ligne[270]. Si une procédure de signalement existait déjà, il lui était reprochait d'être complexe. En mars dernier, le réseau social a rendu public et disponible un filtre contre le harcèlement, permettant de bloquer les tweets offensants ou injurieux afin qu'ils ne soient pas visibles de leurs destinataires[271].

Plus récemment a été crée un label Respect Zone, aux origines duquel se trouve l'association sans but lucratif « Initiative de Prévention de la Haine »[272]. Le label est un outil qui permet de signaler un espace en ligne comme étant une zone de respect. Il permet de protéger les internautes de propos haineux. Pour pouvoir bénéficier du label Respect Zone, les éditeurs de site doivent adhérer à la charte Respect Zone. Ce faisant, ils s'engagent, dans la mesure du possible, à retirer de leur site les contenus cyberviolents, cyberdiscriminants ou cyberharcelants.

[269] Portail anti-harcèlement de Facebook : nous avons testé la version française, L. Provost, Le Huffington Post, 21 mai 2014.
[270] Twitter veut lutter contre le harcèlement en ligne, RLDI, 2013, n°96.
[271] Twitter expérimente un filtre contre le harcèlement, Le Monde, 24 mars 2015.
[272] Respect Zone, le label à suivre…, JP. Viart, Les Affiches parisiennes, 31 octobre 2014.

CONCLUSION

Le numérique est un véritable défi pour la protection de l'enfance. En effet, il est difficile de protéger efficacement l'enfant en raison de la nature même d'Internet. A l'inverse des médias traditionnels, presse, radio et télévision, il n'est pas possible d'envisager une règle unique pour prévenir l'accès de l'enfant à du contenu indésirable, du fait de la diversité des contenus, de la variété des dangers et de la pluralité des activités que le jeune internaute peut exercer sur Internet. En outre, un contrôle systématique ou renforcé des contenus n'est pas souhaitable et serait assurément inconstitutionnel, portant une atteinte démesurée à la liberté de communication.

Plusieurs hypothèses sont envisageables pour améliorer la protection de l'enfance. Il semble important, entre autres, que les prérogatives soient regroupées sous l'égide d'une autorité unique, qui serait compétente pour l'ensemble des médias et des supports. Cela permettrait en outre de centraliser l'ensemble des actions actuellement éclatées pour la mise en place d'un dispositif de protection des enfants global et structuré et adapté aux particularités de chaque média. Cette autorité serait également l'homologue qui interviendrait auprès des acteurs du net. En effet, il serait souhaitable de promouvoir l'autorégulation. Cette forme de régulation permettrait probablement aux professionnels des médias de se sentir directement concernés par l'objectif de protection de l'enfance, et aux règles d'être fixées en adéquation avec les possibilités techniques dont ils disposent. Plus largement, il s'agirait de renforcer la coopération de tous les toutes les personnes intervenant sur Internet, les FAI, les opérateurs de services de médias audiovisuels, les opérateurs de services de communication au public en ligne, et également les internautes eux-mêmes.

Enfin, il s'agit d'appréhender la nature évolutive d'Internet et des technologies numériques, au regard de laquelle la réglementation peut sembler caduque avant même son entrée en vigueur. Dès lors, l'éducation aux médias reste la meilleure des réponses.

BIBLIOGRAPHIE

I. Codes

Code du cinéma et de l'image animée.

Code civil.

Code pénal.

Code des postes et des télécommunications.

Code de la propriété intellectuelle.

II. Conventions, règlements, directives, lois, décrets, chartes et recommandations (par nature et ordre chronologique)

Déclaration des droits de l'homme et du citoyen.

Traité de Lisbonne modifiant le Traité sur l'Union européenne et le Traité instituant la Communauté européenne, 2007/C 306/01.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 janvier 1981.

Convention International des Droits de l'Enfant du 20 novembre 1989.

Convention sur la cybercriminalité du 23 novembre 2001.

Charte des droits fondamentaux de l'Union européenne, 2012/C 326/02.

Directive du 5 mai 1989 relative à la protection de l'enfance et de l'adolescence dans la programmation des émissions diffuées par les services de télévision publics et privés.

Directive n°89/552/CEE du 3 octobre 1989 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à l'exercice d'activités de radiodiffusion télévisuelle.

Directive 95/46/CE 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.

Directive 97/36/CE du 30 juin 1997 modifiant la directive 89/552/CEE.

Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

Directive européenne n°2001/29 du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

Directive 2007/65/CE modifiant la directive 89/552/CE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à l'exercice d'activités de radiodiffusion télévisuelle.
Directive 2010/13/UE visant à la coordination de certaines dispositions législatives, règlementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels.
Loi du 29 juillet 1881 sur la liberté de la presse.
Loi n°49-956 du 16 juillet 1949 sur les publications destinées à la jeunesse.
Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle.
Loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication (loi Léotard).
Loi n°89-25 du 17 janvier 1989 modifiant la loi du 30 septembre 1986 relative à la liberté de communication.
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.
Loi n°2000-719 du 1er août 2000 modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.
Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978.
Loi n°2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.
Loi n°2007-293 du 5 mars 2007 réformant la protection de l'enfance.
Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.
Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.
Loi n°2014-873 du 4 août 2014 pour l'égalité entre les femmes et les hommes.
Senate Bill No. 568, Privacy: Internet: minors, approved by Governor on September 23, 2013.
Ordonnance n°45-174 du 2 février 1945 relative à l'enfance délinquante.
Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques.

Décret n°2010-1379 du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande.
Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique
Charte des prestataires de services d'hébergement en ligne et d'accès à internet en matière de lutte contre certains contenus spécifiques, 14 juin 2004.
Recommandation 98/560/CE du 24 septembre 1998 relative à la protection des mineurs et de la dignité humaine.
Recommandation du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur les droits de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne.
Décision-cadre n°2004/68/JAI du Conseil européen relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie du 22 décembre 2003.
Constitution de la Cinquième République Française, 1958.
Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.

III. Rapports, discours, recommandations et décisions (par nature et ordre chronologique)

Les dix ans du CSA 1989-1999, CSA.
Internet et la collecte de données personnelles auprès des mineurs, Rapport de la CNIL présenté par C. Alvergnat, 12 juin 2001.
Les enfants face aux images et aux messages violents diffusés par les différents supports de communication, Rapport du défenseur des enfants à Monsieur D. Perben, Ministre de la justice, décembre 2002.
« La violence à la télévision », Rapport de Mme. B. Kriegel remis au Ministre de la Culture, 2002.
« Les enfants du Net », L'exposition des mineurs aux contenus préjudiciables sur l'internet, Le Forum des droits sur l'internet, 11 février 2004.
La révision de la directive « télévision sans frontières » : une adaptation du cadre réglementaire européen aux évolutions du paysage audiovisuel, C. Bonenfant-Jeanneney, S. Fautrelle, 2008, Observatoire européen de l'audiovisuel.
La culture de service public de radiodiffusion, Observatoire Européen de l'Audiovisuel, 2007, p65.

« L'impact des nouveaux médias sur la jeunesse », Rapport d'information du Sénateur D. Assouline, 2008.
Rapport de la « Commission Famille, éducation aux médias », à l'attention de Madame Nadine Morano, Secrétaire d'Etat chargée de la Famille et de la Solidarité, juin 2009.
« Les enfants du Net III », Forum des droits sur l'Internet, novembre 2009.
« Protection de l'enfance et de l'adolescence à la télévision, à la radio et sur les services de médias audiovisuels à la demande », les brochures du CSA, novembre 2010.
Le harcèlement sur internet en questions, CNIL, 02 novembre 2010.
« Protéger les enfants dans le monde numérique », Rapport de la Commission au Parlement européen, au Conseil, au comité économique et social européen des régions, 2011.
« Aménagement numérique des territoires : passer des paroles aux actes », Rapport d'information du sénateur H. Maurey, 2011.
« La liberté de communication audiovisuelle à l'heure des nouvelles technologies de l'information et des communications », rapport de mission du groupe n°10 de la promotion « Robert Badinter » de l'ENA, février 2011.
« Enfants et écrans : grandir dans le monde numérique », rapport 2012 consacré aux droits de l'enfant, Défenseur des droits.
« Contre l'hypersexualisation, un nouveau combat pour l'égalité », Rapport parlementaire de Mme. C. Jouanno, Sénatrice de Paris, 5 mars 2012.
« La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet », Rapport du CSA, mars 2012.
Présentation du service de signalement en ligne des contenus choquants, AFA, 2012.
Rapport annuel 2012/2013, Safer Internet France.
Rapport d'activité 2012, CNIL.
Children's Online Privacy Protection Rule : Final rule Amendments to clarify the scope of the rule and strengthen its protections for children's personal information, Federal Trade Commission, 17 janvier 2013.
Rapport au gouvernement sur l'application du décret n°2010-1379, novembre 2013, CSA.
Rapport annuel du CSA, 2013.
Rapport annuel du CSA, 2014.
La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information, Rapport d'information n°441 déposé au Sénat, Y. Détraigne et A.M. Escoffier.
Recommandation CSA du 7 juin 2005 aux éditeurs de services de télévision concernant la signalétique jeunesse et la classification des programmes.

Décision du CSA, Le CSA adopte une nouvelle signalétique, 17/09/2002.
Décision n°2004-496 du 10 juin 2004 du conseil Constitutionnel.
Décision du CSA, « Publicité pour un jeu vidéo déconseillé aux moins de 16 ans : intervention auprès de MyTF1 », Assemblée plénière du 16 octobre 2012.
Délibération relative à l'intervention de mineurs dans le cadre d'émissions de télévision diffusées en métropole et dans les départements d'outre-mer, CSA, 17 avril 2007.
Délibération du CSA concernant la protection du jeune public, la déontologie et l'accessibilité des programmes sur les services de médias audiovisuels à la demande, 14 décembre 2010.
Délibération du CSA relative à la protection du jeune public, à la déontologie et à l'accessibilité des programmes sur les services de médias audiovisuels à la demande, 20 décembre 2011.
Contrôle parental sur l'Internet : les engagements des fournisseurs d'accès Internet, 16 novembre 2005, Accord de l'AFA.
Livre vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, Commission des Communautés Européennes, 16 octobre 1996.
Avis n°5/2009 sur les réseaux sociaux en ligne, Groupe de travail « article 29 » sur la protection des données, 12 juin 2009.
Avis n°6 de l'Observatoire des Droits de l'Internet concernant le Cyberharcèlement, février 2009.
Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», 16 février 2010, Groupe de travail « article 29 » sur la protection des données.
« Une approche globale de la protection des données à caractère personnel dans l'Union européenne », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 4 novembre 2010.
Guidelines on the implementation of the Court of Justice of the European Union judgment on"Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González », G29, 26 novembre 2014.

IV. Doctrine (par ordre alphabétique d'auteurs)

Du BVP à l'ARPP : nouvelle dénomination, nouvelle régulation ?, L. Arcelin-Lécuyer, Revue Lamy de la Concurrence, n°22, 2010.
La responsabilité des réseaux sociaux en cas de violation des données personnelles, J.P. Arroyo et C. Prault, RLDI, 2014, p109.
Médias et Sociétés, F. Balle, LGDJ, 16ème édition, 2013.

« Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? », V.L. Benabou et J. Rochfeld, Recueil Dalloz 2014, p 1476.
Les ados dans le cyberespace, prises de risque et cyberviolence. C. Blaya, 2013. De Boeck
La responsabilité en matière d'internet, M. Boizard, Droit et patroimoine, 2001.
La pornographie dans les forums, M. Cahen, http://www.murielle-cahen.com
La confiance dans l'économie numérique, E. Caprioli, P. Agosti, Petites affiches, 03 juin 2005, n°110, p 4
Contrefaçon et sites communautaires : état des lieux jurisprudentiel, C. Caron, communication commerce électronique, 2007, p143.
« La consécration d'un droit à l'oubli… principalement pour les anonymes », A. Casanova, RLDI n°106, 2014.
Le « droit à l'oubli numérique » en Europe et en Californie, C. Castets-Renard et G. Voss, RLDI, n°100, 2014.
« La cybercriminalité », F. Chopin, Rubrique du Répertoire Pénal Dalloz, juillet 2013.
Le pouvoir de sanction du Conseil supérieur de l'audiovisuel, S. Clément-Cuzin, AJDA 2001, p 111.
La loi Informatique et libertés est-elle dépassée ? L. Cytermann, RFDA 2015, p99.
Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage, E. Derieux, RLDI, 2012, p 81.
Neutralité et responsabilité des intermédiaires de l'Internet – Mythe ou réalité du principe de « neutralité » ?, E. Derieux, Semaine juridique Edition Générale n°13, 2012.
« Google Spain : Droit à l'oubli ou oubli du droit ? », A. Debet, Comm. Com. Electronique, n°7, 2014.
Le streaming, légal ou illégal ?, A. Dimeglio et M-D. Gleize, revue électronique Le Journal du Net, 3 juin 2008.
Projet de Règlement Européen sur la protection des données personnelles : ce qui va changer, T. Dor, D. Rimsevica, Le Monde du Droit, 7 avril 2015.
Convention européenne des droits de l'homme, P. Dourneau-Josette, juin 2013.
Droit de la presse, E Dreyer, D. 2015, p 342.
Qu'est-ce que l'identité numérique ?, O. Ertzscheid, Encyclopédie numérique, 2013.
Les réseaux sociaux face à de nouvelles contraintes – Impacts de la recommandation de la Commission des clauses abusives, A.L. Falkman, La Semaine Juridique édition Entreprises et Affaires, n°12, 19 mars 2015, p 1136.
« L'automaticité du moteur de recherche sur internet : opposition absolue entre les jurisprudences européenne et française », J. Huet, RLDI n°106, 2014.
La propriété intellectuelle à l'ère du streaming : quelle répression ?, A. Jaber, RLDI, 2011, n°77.

« CJUE : le droit à l'oubli n'est pas inconditionnel », J. Le Clainche, RLDI, n°107, 2014.
Protection de la vie privée et des données personnelles, N. Mallet-Poujol, Legamedia, février 2004.
Toiles et filtres, C. Manara, Reccueil Dalloz 2002, p 1900.
Les sanctions pénales et civiles de la diffusion d'un message à caractère pornographique, JY. Maréchal, La semaine juridique Edition générale, n°1, 13 janvier 2014, p 41.
Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, N. Martial-Braz et E. Gattone, Recueil Dalloz, p2788, 2013.
La réforme de la communication audiovisuelle, J. Morange, RFDA 1994, p 1170.
La protection du mineur dans le cyber espace, C. Nlend, Thèse, 2007.
« La Cour de justice, les moteurs de recherche et le droit « à l'oubli numérique » : une fausse innovation, de vraies questions », R. Perray et P. Salen, RLDI n°109, 2014.
« Google Inc. condamné en référé à déréférencer un lien renvoyant vers un contenu qui n'est pas illicite en soi », O. Pignariti, RLDI N°113, 2014.
Chronique de jurisprudence de droit de la presse, P. Piot, Gazette du Palais, juin 2013, p 14.
Quelle réglementation pour les Services de médias audiovisuels à la demande ?, JP. Roux, Gazette du palais, n°113, 23 avril 2009, p 14.
Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russel, S., & Tippett, N. (2008).Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child, Psychology and Psychiatry, 49,p 376.
La directive dite Services de médias audiovisuels sans frontières modifiant la directive dite Télévision sans frontières, Y. Thiec, Communication Commerce électronique n°6, Juin 2008.
L'évolution récente du régime des sanctions du Conseil supérieur de l'audiovisuel, JP Thiellay, AJDA 2003, p 475.
La protection des mineurs face aux sites pornographiques, E. Wéry, Journal du Net.
Loi DADVSI : mesures pénales, civiles et de prévention, Etude n°271-30, Lamy Droit des médias et de la communication, novembre 2000.
Le droit de reproduction de l'auteur d'une œuvre musicale, Etude n°477-22, Lamy Droit des médias et de la communication, novembre 2000.
Twitter veut lutter contre le harcèlement en ligne, RLDI, 2013, n°96.
« Peer to peer » exception de copie privée et droit d'auteur, Lamy Droit du numérique, 2014.

V. Jurisprudences (par ordre chronologique)

Crim, 19 février 1863, Bull Crim n°56.

Cass crim, 20 juin 1946, gaz pal 1946, n°2, p 178.

Cass. Ass. Plén., 9 mai 1984, Fullenwarth, obs. J. Huet, RTD Civ. 1984, p 508.

CA Paris, 1ère Ch., 23 mai 1995, Hassier, Dalloz 1996, p75.

TGI Paris, UNADIF c/ Faurisson, 13 novembre 1998.

TGI Paris, réf, UEJF et licra c/yahoo Inc et Yahoo France, 22 mai 2000.

Crim 12 septembre 2000, n°99-84648

CA Paris, 13e ch. A., 2 avril 2002, n°01/03637

CA Paris, 1re ch., 5 juin 2003, Comm. com. électr. 2004, comm. 35.

Civ. 1ère, 10 mai 2005, A. Lepage, Dalloz 2005, p 2643.

1ère Civ, 21 mars 2006, obs A. Lepage, Dalloz 2006, p 2702.

Tribunal d'instance de Strasbourg, 9 juin 2006.

CEDH, 29 juin 2006, req n° 11901/02

CA Paris, 11è ch., 6 juin 2007, Mairie de Puteaux / Christophe G.

TGI Paris, 19 octobre 2007, Zadig production et al c/ Google inc., n° 06/11874

TGI Toulouse, réf, 13 mars 2009, krim k c/pierre g.

TGI de Paris, 25 juin 2009, C. Vernes c/SAS les Echos, légipresse N°266, III p. 215, novembre 2009.

TC Paris, 15è ch., 11 décembre 2009, Groupement des brocanteurs de Saleya et autres c/ eBay Inc.

Ass plén, 25 juin 2010, n°08-86.891, note V. Vigneau, Chronique de jurisprudence de la Cour de cassation, D. 2010, p 2090.

Cass Civ. I, 17 février 2011, n° 09-13202.

CA Paris, 21 juin 2013, SPPF c/ Youtube, n°11/09195.

CA Paris, 11 déc 2013, rldi févr 2013, n°3362.

Cass, 1ère Civ, 10 avril 2013, n°11-19.530, note, A. Lepage, com com électr., n°81, 2013.

CA Angers, ch. civ. A, 29 oct. 2013, n° 12/00922.

CA Paris, 9 avril 2014, rldi mai 2014, n°3475.

CJUE, gr. Ch., 13 mai 2014, Google Spain SL et Google Inc. c/ Agencia Espanola de Proteccion de Datos (AEDP), n° C-131/12.

VI. Etudes, enquêtes et sondages (par ordre chronologique)

« Comprendre le comportement des enfants et adolescents sur Internet pour les protéger des dangers », enquête sociologique menée par l'association Fréquence écoles, 2010.
« Enfants et Internet », baromètre Calysto, 2011.
L'usage des réseaux sociaux chez les 8-17 ans, Etude TNS Sofres, Juin 2011.
Facebook et ses pratiques en collège et lycée, Enquête dans les collèges et lycées de l'académie de Dijon, avril 2012.
« Tablette tactile, la nouvelle nounou ? », sondage de l'institut CSA pour l'Observatoire Orange-Terrafemina, septembre 2012.
Perception croisée enfants/parents face à l'usage d'Internet, Etude menée conjointement par l'IFOP et EMC corporation, janvier 2013.
Perceptions et pratiques de consommation des « Digital Natives » en matière de biens culturels dématérialisés, Etude qualitative, Hadopi, Janvier 2013.
Le numérique et les droits fondamentaux, Etude annuelle 2014, Conseil d'Etat.
Social, Digital & Mobile around the world, We are social Singapore, 2014.
La consommation illégale de vidéos sur Internet en France, Période 2009/2014, Etude de l'ALPA, 1er avril 2015.

VII. Journaux

« Le droit à l'oubli sur internet : une idée dangereuse », S. Tisseron, Libération, 6 décembre 2012.
Chantages sexuels, harcèlement… Les ados pris au piège du net, A. Logeart, Le nouvel obs, 28 mars 2013.
« Un groupe d'adolescentes violentes en garde à vue à Nice », Nice-Matin, 21 février 2014.
Portail anti-harcèlement de Facebook : nous avons testé la version française, L. Provost, Le Huffington Post, 21 mai 2014.
Respect Zone, le label à suivre…, JP. Viart, Les Affiches parisiennes, 31 octobre 2014.
Comment combattre la cyber-violence à l'école ?, M. Maillard, Le Monde, 2 décembre 2014.
Twitter expérimente un filtre contre le harcèlement, Le Monde, 24 mars 2015.

VIII. Autres

Documentaire « Souffre-douleurs, ils se manifestent », réalisé par Andrea Rawlins Gaston et Laurent Follea, diffusé le 10 février 2015 sur France 2.

Table des matières