HAL
open science

La protection du mineur à l'aune des réseaux sociaux

Célia Scaultz

To cite this version:

Célia Scaultz. La protection du mineur à l'aune des réseaux sociaux. Droit. 2020. dumas-02960116

HAL Id: dumas-02960116

https://dumas.ccsd.cnrs.fr/dumas-02960116v1

Submitted on 7 Oct 2020

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

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

Mémoire
La protection du mineur à l'aune des réseaux sociaux

Sous la direction du Professeur Anne-Sophie Brun-Wauthier
Université de Grenoble Alpes – Faculté de droit

Master 2 – Droit privé - Droit des personnes et de la famille

SCAULTZ Célia

<u>Membres du jury :</u> **Madame le Professeur Anne-Sophie BRUN-WAUTHIER**
Madame le Professeur Gaëlle RUFFIEUX

Soutenance le 11 septembre 2020 à 9h30

REMERCIEMENTS :

Avant de présenter le contenu de cette étude, je tiens à exprimer ma reconnaissance et mes remerciements envers les personnes qui m'ont permis d'élaborer ce travail de recherche.

Ainsi, je tiens à remercier Madame le Professeur Anne-Sophie Brun-Wauthier, ma directrice de recherche et directrice du Master 2 droit des personnes et de la famille, qui m'a accordé sa confiance en acceptant de superviser ce travail. Je lui suis reconnaissante de son investissement à mes côtés ainsi que du temps et de l'aide qu'elle m'a consacré.

Je voudrais également remercier Monsieur Michael Stora, psychologue - psychanalyste et cofondateur de l'Observatoire des Mondes Numériques en Sciences Humaines ainsi que Monsieur Jacques Henno, journaliste, auteur et conférencier spécialisé dans les nouvelles technologies et l'association e-Enfance pour leur disponibilité et leur collaboration.

Enfin, je tiens à remercier Madame le Professeur Gaëlle Ruffieux d'avoir accepté de faire partie des membres du jury de ma soutenance de mémoire.

TABLES DES ABREVIATIONS :

C.Civ	Code Civil
C.Pén	Code pénal
CA	Cour d'appel
CCass	Cour de cassation
CE	Conseil d'Etat
CEDH	Cour Européenne des Droits de l'Homme
CIDE	Convention internationale des droits de l'enfant
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
DDHC	Déclaration des droits de l'homme et du citoyen
EMI	Education aux médias et à l'information
G29	Groupe de travail de l'article 29
HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet
RGPD	Règlement général sur la protection des données
UNESCO	United Nations Educational, Scientific and Cultural Organization (Organisation des Nations unies pour l'éducation, la science et la culture)

SOMMAIRE :

Chapitre I : La protection avérée du mineur sur les réseaux sociaux

Chapitre II : La protection limitée du mineur sur les réseaux sociaux

INTRODUCTION :

« On se sert des réseaux sociaux en sachant qu'ils se servent de nous. Etre prudent dans l'usage, c'est être sage dans les conséquences. »

Cette analyse de Daniel Confland illustre parfaitement l'effet pervers de la relation que l'Homme peut entretenir avec les réseaux sociaux. Si depuis une quinzaine d'années, ils font partie intégrante de sa vie, ils s'avèrent parfois dangereux pour lui. Aujourd'hui, plus populaires que jamais avec 3,8 milliards d'utilisateurs, soit 49% de la population mondiale, les réseaux sociaux sont considérés comme le moyen de communication le plus rapide et le plus utilisé. Toutefois, les menaces liées ne cessent pas, elles aussi, d'augmenter. Ces dangers sont appréhendés différemment selon les utilisateurs. D'un côté, ceux qui ont grandi sans et appris à les utiliser montre une certaine méfiance et prudence dans leur utilisation. De l'autre côté, ceux n'ayant connu qu'un monde avec pensent savoir les maîtriser et présentent une grande confiance, parfois trompeuse, dans leur utilisation. Natif de l'ère numérique, le mineur a une utilisation naïve des réseaux sociaux. Ainsi, sa vulnérabilité et son manque de prudence peut engendrer des conséquences à ne pas sous estimer, mais également le mettre dans une position d'insécurité et lui porter préjudice.

Le mineur est un individu de moins de 18 ans[1], communément appelé « enfant » dans le langage courant. En raison de son âge, ce dernier est considéré comme vulnérable, nécessitant une protection particulière. S'il dispose de la jouissance de la totalité de ses droits, il ne peut pas les exercer puisqu'il est juridiquement incapable. De ce fait, jusqu' à l'âge de 18 ans, le mineur devra être assisté par ses représentants légaux, titulaires de l'autorité parentale, pour mettre en œuvre ses droits. Au delà de la mise en œuvre des droits du mineur, l'autorité parentale a pour principale mission de protéger le mineur. Cette protection particulière du mineur signifie qu'il doit être préservé de tout danger ou risque de danger. En effet, les titulaires de l'autorité parentale ont le devoir de protéger le mineur dans sa santé, sa sécurité, sa moralité et d'assurer son éducation et son développement. [2] Ces premières obligations impliquent un devoir de surveillance lié au droit de garde. Les responsables légaux doivent veiller à la sécurité du mineur et au bon comportement de ce dernier tout en contrôlant les relations et les correspondances que l'enfant peut entretenir avec les tiers. Ainsi, ils peuvent interdire au mineur certaines activités s'ils estiment qu'elles ne

[1] Article 388 alinéa 1 C.civ : « Le mineur est l'individu de l'un ou l'autre sexe qui n'a point encore l'âge de dix-huit ans accomplis. »

[2] Article 375 alinéa 1 C.civ : « Si la santé, la sécurité ou la moralité d'un mineur non émancipé sont en danger, ou si les conditions de son éducation ou de son développement physique, affectif, intellectuel et social sont gravement compromises, des mesures d'assistance éducative peuvent être ordonnées par justice à la requête des père et mère conjointement, ou de l'un d'eux, de la personne ou du service à qui l'enfant a été confié ou du tuteur, du mineur lui-même ou du ministère public.

sont pas conformes à son intérêt. Ce devoir de surveillance s'applique aussi bien au monde réel qu'au monde virtuel avec l'utilisation des réseaux sociaux.

Le réseau social se définit comme une « plateforme de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs»[3]. Cette plateforme invite le futur usager à fournir un certain nombre de données personnelles pour qu'il puisse bénéficier du statut d'utilisateur. Une fois intégré la communauté, ce dernier pourra interagir avec les autres utilisateurs en partageant divers contenus et utilisant une messagerie en ligne. Auparavant, sous le web 1.0, l'internaute avait un rôle « passif » puisqu'il s'agissait avant tout d'un web statique centré sur la distribution de l'information sollicitant peu les utilisateurs. Aujourd'hui, avec l'émergence de ce type de plateformes, l'internaute a désormais un rôle « actif» puisqu'il est lui-même éditeur de contenus et d'information.[4] Cette ère du web 2.0 est donc venue renforcer les liens entre les utilisateurs afin de faire naître une intelligence collective. [5]

Aujourd'hui, il existe plusieurs catégories de réseaux sociaux. D'une part sont apparus ceux qui permettent de constituer ou reconstituer virtuellement des liens en faisant partie d'une communauté. D'autre part, sont apparus ceux qui ont une vocation plus professionnelle. Enfin, une dernière catégorie a vu le jour : celle des réseaux sociaux à vocation matrimoniale. Au fur et à mesure du temps et de leur succès, les réseaux sociaux se sont donc déclinés en fonction des besoins de chacun. Par nature de la relation, l'intérêt des mineurs se porte principalement sur la première catégorie de réseau. Afin de répondre au mieux à cette problématique de la protection des mineurs sur les réseaux sociaux et de comprendre les enjeux, il est essentiel de revenir sur les principales plateformes utilisées par ces derniers en France.

Crée en 2004 par Mark Zuckerberg, Facebook est le réseau social le plus célèbre. Avec plus de deux milliards d'utilisateurs, il est devenu le réseau social le plus utilisé dans le monde et un moyen de communication à part entière. Cette plateforme permet de partager des statuts, photos, vidéos ou articles avec ses « amis », mais également de discuter de manière instantanée avec une ou plusieurs personnes en créant des groupes. Même si l'outil est très utilisé à tous les âges, pour la génération Z, il semble être considéré comme réseau social de « vieux ». Selon une étude, 41% des 13-16 ans déclarent utiliser la plateforme sociale Facebook[6]. Ce taux s'explique par la présence des parents sur ce réseau social les empêchant de s'exprimer en toute liberté. Ainsi, parallèlement, d'autres réseaux sociaux ont suscité l'attention de ces derniers. C'est notamment le cas d'Instagram, appartenant à l'entreprise Facebook, qui est en tête avec 74% de 13-16 ans déclarant utiliser ce réseau social.[7] Cette plateforme a pour fonction principale de partager des photos et vidéos avec ses abonnés. Les utilisateurs y suivent les comptes qui les intéressent, qu'il

[3] Avis 5/2009 sur les réseaux sociaux en ligne, Groupe de travail « Article 29 » sur la protection des données, adopté le 12 juin 2009. p. 4
[4] R.Fassi-Fihri, « Quel droit pour les réseaux sociaux ? », Revue de droit public 2018, n°3, 1er mai 2018, p.685
[5] V.Fauchoux, J-M. Bruguière et P.Deprez, *Le droit de l'internet, lois, contrats et usages* , 2e édition 2013, LexisNexis p. 7.
[6] Etude faite en 2019 par Morning Consult auprès de 2000 américains de 13 à 38 ans afin de chercher à mesurer les usages des plus jeunes sur les réseaux sociaux
[7] *Ibid*

s'agisse de leurs amis ou de célébrités ou de communication commerciale. Sur chaque publication, il est possible d'y laisser des commentaires ou des « like ». Twitter, crée en 2006, intéresse moins les jeunes mais est tout de même présent dans leur quotidien. Ce réseau social a pour fonction de poster des messages brefs appelés « tweets » agrémentés de photos ou de vidéos, nécessairement publics et pouvant être repartagés par les utilisateurs. Les collégiens et lycéens se servent de cette plateforme pour commenter leur quotidien et réagir aux actualité qui les touchent. De son côté, YouTube est une plateforme de partage de vidéos. Si elle n'est pas considérée comme un réseau social à proprement parlé, elle compote certaines fonctionnalités de réseau social. En effet, il est possible d'y regarder des vidéos déjà présentes sur la plateforme, mais également d'en produire et d'en partager. Ce service regroupe des vidéos variées recueillant plus ou moins de vus. Enfin, Snapchat est l'un des réseaux les plus récents et les plus utilisés par les mineurs car 62% des 13-16 ans déclarent l'utiliser quotidiennement.[8] Crée en 2011, le principe de ce réseau social est d'envoyer des photos ou des vidéos à durée très limitée de visionnage à ses contacts (10 secondes maximum). Ainsi que de partager des conversations dont l'historique est effacé au bout de 24 heures. Les utilisateurs considèrent que sur ce réseau social le ton peut y être plus léger sans crainte que les propos ou photos ne soient ressortis à d'autres moments. Ces différentes plateformes telles que présentées ci-dessus ont certaines caractéristiques communes. Elles vont permettre le partage de contenus : qu'il s'agisse de contenus de tiers, c'est-à-dire provenant de différents médias et d'autres personnes ou bien de contenus personnels, c'est-à-dire des images, vidéos, textes, humeur ou planification d'évènements. Elles vont également donner la possibilité d'interagir par le biais de commentaires ou de mécanismes montrant l'appréciation appelés des « like ». Puis, elles mettent à disposition des messageries en ligne afin d'y échanger en « privé » avec ses contacts mais pouvant également avoir la fonctionnalité de messagerie de groupe de sorte à faciliter les échanges à plusieurs par groupe affinitaire. Enfin, ces réseaux sociaux sont une façon pour l'utilisateur de se représenter vis-à-vis des autres, plus ou moins publiquement, par le biais de son profil, « mur » ou de la page qui se construit à chaque ajout dans le profil ou à chaque nouvelle publication. Pour accéder à ces réseaux sociaux, une grande partie des mineurs utilisent une application sur leur smartphone. Ils sont donc fréquentés tout au long de la journée, en tout lieu et prennent une part conséquente dans la vie quotidienne des adolescents.

Depuis ces vingt dernières années, le monde numérique a grandement évolué. Des ordinateurs aux smartphones, des blogs aux réseaux sociaux, les nombreux progrès technologiques et numériques sont venus révolutionner les moyens de communication. Toutefois, jusqu'à récemment, la société a bénéficié de ces évolutions technologiques sans pour autant se soucier des dangers que cela pouvait engendrer. La prise de conscience de cette problématique est récente et

[8] *Ibid*

a influé sur des dispositifs de normalisation et d'encadrement. Ainsi, le RGPD[9] du 26 avril 2016, directement applicable depuis le 25 mai 2018, est venu normaliser l'utilisation du numérique et notamment des réseaux sociaux. L'objectif principal est d'amorcer la construction de la protection des données personnelles. Pour une grande partie, les réseaux sociaux ont comme principe économique la gratuité contre l'abandon de données à caractère personnel. Tous les utilisateurs, qu'ils soient majeurs ou mineurs, sont touchés par le traitement de ces données : c'est pour cette raison que ce texte est venu l'encadrer. Ce règlement vient également responsabiliser les acteurs du traitement de données privées et renforcer les pouvoirs de la CNIL. Crée par la loi Informatique et Libertés du 6 janvier 1978[10], la CNIL est une autorité administrative indépendante française chargée de veiller à ce que l'informatique soit au service du citoyen et ne porte pas atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Par leur traitement de données à caractère personnel, les réseaux sociaux ont été sources de nouveaux enjeux pour la protection de la vie privée. De ce fait, la CNIL est également chargée de veiller à la protection de ces données personnelles traitées par les services de traitement d'informations. En plus de son rôle d'alerte, de conseil et d'information, elle dispose également d'un pouvoir de contrôle et de sanction. Cette normalisation est donc en pleine construction. Elle est amenée à évoluer et se renforcer. Récemment, la loi du 24 juin 2020, dite « loi Avia », visant à lutter contre le contenu haineux sur internet[11], avait pour objectif de venir mettre fin à l'impunité des comportements haineux sur internet et montrer l'urgence ainsi que la nécessité de réguler les réseaux sociaux. Cependant, malgré qu'elle soit fondée sur une grande partie des préoccupations des dangers d'Internet, le contenu de ce texte est, quasiment intégralement, censuré par le Conseil constitutionnel dans une décision du 18 juin 2020[12]. Cette loi ne produit donc pas les effets souhaités. Toutefois, dans un contexte où la lutte contre les dangers en ligne, et notamment contre les contenus haineux, constitue une préoccupation sociale et sociétale de premier ordre, le législateur a la volonté de retravailler ce dispositif afin d'apporter une protection convenable et certaine sur le web[13]. Ce nouveau texte et cette volonté de le faire évoluer, malgré la censure, montre bien l'inquiétude de la société envers les dangers du cyberespace et le travail de normalisation qui est en cours pour répondre à ce problème.

De plus, à l'heure où la préoccupation des dangers liés aux nouvelles technologies est d'actualité, des organes consultatifs ont été chargés par la Commission Européenne de produire des recommandations. Ainsi, le G29 instauré par la directive 95/46/CE[14] produit des recommandations à la Commission Européenne sur la protection des données personnelles et de

[9] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
[10] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[11] Loi n°2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet
[12] Décision n°2020-801DC du 18 juin 2020 du Conseil constitutionnel
[13] M. Untersinger et A. Piquard, « La loi Avia contre la haine en ligne largement rétoquée par le Conseil constitutionnel », LeMonde, 18 juin 2020
[14] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée le 25 mai 2018

la vie privée. Ces avis traitent notamment des problématiques qui visent les réseaux sociaux. Le contrôleur européen de la protection des données est un autre organe consultatif qui vient mettre en garde des risques liés à une utilisation imprudente des réseaux sociaux.

En complément du droit, les réseaux sociaux développent une autorégulation permettant d'imposer aux utilisateurs des règles de bonne conduite et de bonne pratique mais également contrôler leur bon respect. Par exemple, lors d'une journée pour un internet plus sûr organisée par la Commission européenne, Facebook a signé un accord pour améliorer la sécurité des mineurs qui utilisent ce réseau social. [15] Ainsi, Facebook a instauré un paramétrage spécifique pour les utilisateurs mineurs, âgés de 13 à 17 ans, en réglant par défaut la visibilité de leur publication en « privé », c'est-à-dire visible uniquement par leurs « amis », les personnes qu'ils ont autorisé à voir le contenu de leur profil. Par ailleurs, si le mineur choisi de diffuser le message en mode « public », le réseau social attirera son attention sur les éventuelles conséquences de son action. De plus, la plateforme fait attention à la diffusion de données sensibles du mineur, puisque même si le mineur à renseigné ses coordonnées, sa date de naissance ou le nom de son école, ces informations n'apparaissent pas dans une recherche publique. Enfin, le réseau social modifie aussi le paramétrage de la géolocalisation en la désactivant par défaut. Toutefois, aux 18 ans de l'enfant, ces paramétrages de protection seront désactivés automatiquement.

Compte tenu de sa capacité juridique « partielle » et sa maturité en devenir, le mineur est une personne particulièrement vulnérable aux impacts des processus de réseaux sociaux. Sa protection est difficile à cerner et à étudier car elle confronte de nombreux domaines. D'une part, dans la multitude de répercussions que les réseaux sociaux peuvent avoir sur sa vie, trop volumineux à développer dans leur totalité, l'étude a dû être orientée sur une sélection d'impacts et de dangers. D'autre part, l'utilisation par le mineur des réseaux sociaux et la protection qui en découle relève d'un traitement hybride pluridisciplinaire. La problématique se traite à travers les droits et libertés fondamentaux et plus spécifiquement à travers le droit pénal, le droit civil ainsi que le droit numérique. L'analyse pourrait s'ouvrir sur une discipline en particulier, toutefois cette étude aborde le sujet de manière plus générale et pluridisciplinaire afin d'avoir un aperçu de la problématique dans sa globalité.

[15] Communiqué de presse de la Commission européenne, « Socialisation sur internet: accord entre les grands sites par l'entremise de la Commission», IP/09/232, 10 février 2009.

Aujourd'hui, la question de l'enfance et de la jeunesse dans le paysage numérique actuel nécessite de faire l'objet de nombreuses réflexions car l'utilisation des réseaux sociaux par les mineurs est devenu un sujet majeur de préoccupation. Les réseaux sociaux ont un rôle crucial dans la socialisation des mineurs puisqu'ils occupent une place prépondérante dans leur relation avec la société. Face à l'utilisation de ces nouveaux moyens de communication qui requière un comportement de prudence et des connaissances techniques, les mineurs peuvent paraître particulièrement vulnérables. Si les natifs de l'ère numérique sont fortement incités à utiliser ces outils au quotidien, pour autant, ils ne maitrisent pas forcément les enjeux d'une telle utilisation et ne savent pas la remettre en question. A l'aune des réseaux sociaux, la protection du mineur est donc une préoccupation qui a vocation à se développer et occuper une place croissante dans la société. Compte tenue de l'avancée technologique fulgurante et la facilitation d'accès à ces services pour les mineurs, cette problématique est d'autant plus pertinente. Un équilibre doit donc être trouvé entre l'utilisation de ces nouveaux services par les mineur et leur protection.

Pour traiter le sujet de la protection du mineur à l'aune des réseaux sociaux, il a fallu, dans un premier temps, avoir une approche théorique. Toutefois, s'agissant d'une problématique extrêmement récente et d'un sujet très large aucun ouvrage n'a été écrit à ce sujet à ce jour. En parallèle, la doctrine s'est, pour l'instant, rarement penchée sur la question. Il est possible de trouver des écrits de professeurs ou de professionnels portant en partie sur cette thématique. Néanmoins, le sujet y est uniquement traité à travers certains domaines particuliers et ceux-ci n'analysent pas ce problème de manière transversale. Les quelques articles existants s'interrogeaient uniquement : soit sur l'aspect pénal, à travers la cybercriminalité, soit sur l'aspect numérique, à travers le droit à l'oubli et à la protection des données personnelles. Ainsi les approches sont toujours spécialisées sans avoir un regard global de la problématique. Puis, s'agissant d'une problématique très récente, la jurisprudence est encore très pauvre car les affaires n'ont pas encore été portées en juridiction. Quelques arrêts ont été rendus par les cours d'appel et très peu par la cour de cassation. De plus, pour pouvoir répondre à ce sujet, l'analyse des textes et des lois fut indispensable. Cependant, s'agissant d'un problème contemporain, l'arsenal législatif a dû se moderniser. Or, le droit nécessite toujours une certaine inertie pour pouvoir s'adapter aux faits. Ce retard apparaît d'autant plus face à la rapidité d'évolution des nouvelles technologies et plus spécialement du développement des réseaux sociaux. En effet, les usages, pratiques et outils évoluent très vite en matière de réseaux sociaux. Cette vitesse d'évolution est renforcée par la volonté pour les plus jeunes d'expérimenter le plus rapidement possible les nouveautés. Il est donc compliqué pour le législateur d'adapter le droit au même rythme que ces évolutions et ces utilisations laissant, ainsi, place à un vide juridique et posant des difficultés pour le développement de cette étude.

Dans un second temps, afin d'avoir une vue globale sur cette problématique, il était essentiel de compléter cette réflexion théorique avec une approche pratique du sujet. Au delà du cadre juridique, il est important d'avoir conscience des conséquences de l'utilisation des réseaux sociaux sur le développement et la sécurité des plus jeunes. Puis, si la protection s'effectue en posant un cadre pour le mineur ou les acteurs qui l'entourent, elle se fait également en l'armant d'outils pour qu'il puisse réagir et se défendre face au danger. Afin de s'appuyer sur des cas concrets, le témoignage de personnes impliquées dans cette problématique semble incontournable. D'une part, il était nécessaire de faire appel à l'expertise des professionnels œuvrant sur les problématiques liées aux réseaux sociaux : journalistes, psychologue-psychanalyste, professionnels du milieu associatif. D'autre part, pour enrichir et illustrer le sujet, il semblait utile d'avoir recours à des acteurs directs en la personne de jeunes influenceurs, de parents d'enfants influenceurs et d'agences spécialisées dans le domaine. Etonnamment, ces derniers, surfant constamment sur le principe de communication et de l'accessibilité, n'ont pas répondu présents aux requêtes et laissant aux sollicitations qu'une réponse totalement silencieuse. A contrario, les experts se sont avérés très disponibles et coopératifs.

S'il n'est pas question de restreindre le mineur dans ses droits liés aux réseaux sociaux, une obligation de protection s'impose tout de même pour le préserver de bon nombre de dangers. Il est donc intéressant de s'interroger : Où en est-il de la protection du mineur sur les réseaux sociaux ? Est-elle suffisamment assurée ou nécessite-t-elle d'être renforcée ?

Dans un premier temps, un état des lieux de la protection du mineur, telle qu'elle est déjà assurée par les différents dispositifs peut être fait. (Chapitre 1) Mais, même si l'ère des réseaux sociaux est déjà bien avancée dans le monde numérique que nous vivons actuellement, il reste encore beaucoup à faire s'agissant de l'encadrement de ses pratiques et en matière de prévention. Alors, dans un second temps, le vide juridique et la difficulté de mise en place de cette protection doivent être soulignés. (Chapitre 2)

CHAPITRE I : La protection avérée du mineur sur les réseaux sociaux

Les réseaux sociaux ne sont pas seulement un espace de communication, de culture ou de consommation, ce sont également un lieu d'exercice de certaines libertés fondamentales. Il est donc essentiel de concilier cette innovation apportée par l'ère du numérique à la protection des droits fondamentaux des utilisateurs, peu importe leur âge. Au vu de leur place importante dans la société, cette conciliation est donc une condition *sine qua non* pour un usage numérique de confiance. (Section 1) Aujourd'hui, la « jeunesse 2.0 » fait passer une grande partie de sa vie sociale par les réseaux sociaux. Cette nouvelle réalité ouvre les portes à de nombreux enjeux et oblige le droit à s'adapter aux évolutions technologiques et virtuelles. L'explosion du numérique et la simplification de l'accès à Internet, ainsi qu'aux réseaux sociaux, ont donné naissance à une toute nouvelle forme de délinquance : la cybercriminalité. Cette nouvelle forme de délinquance concerne les situations dans lesquelles les systèmes informatiques constituent l'objet même du délit et celle dans lesquelles les systèmes ou réseaux informatiques constituent le moyen de commettre l'infraction. Autrement dit, tous les outils numériques deviennent des moyens de commettre des actes de cybercriminalité ou d'en être des victimes. Le législateur a dû s'adapter et réagir face à cette nouvelle forme de criminalité afin d'assurer la protection des mineurs. (Section 2)

Section 1 : Le respect des droits fondamentaux du mineur dans l'utilisation des réseaux sociaux

L'Internet et ses outils sont de puissants facilitateurs des droits de l'Homme. En tant que moyen de communication, les réseaux sociaux ont favorisé la liberté d'expression et, aujourd'hui, représentent clairement l'outil privilégié des mineurs internautes pour l'exercice de droit. (Paragraphe 1) De plus, les réseaux sociaux sont également utilisés par les mineurs internautes pour dévoiler une partie, voire toute leur vie privée. Ainsi, les enjeux juridiques en termes de protection de la vie privée et du droit à l'image se sont retrouvés démultipliés. (Paragraphe 2)

Paragraphe 1 : L'exercice du droit à la liberté d'expression par l'accès aux réseaux sociaux

Les réseaux sociaux sont devenus un terrain d'expression propice à l'exercice de certains droits fondamentaux. En outre, l'interdiction ou la restriction à leur accès pourraient porter atteinte à certaines libertés. A ce titre, une nouvelle interrogation est apparue : la reconnaissance d'un droit d'accès aux réseaux sociaux, comme il l'a été fait pour l'accès à Internet. (A) Cet accès aux réseaux sociaux est d'autant plus primordial suite à leur croissance dans un environnement numérique, les mineurs d'aujourd'hui ont investis ces nouveaux espaces de libertés afin d'exercer leur droit à la liberté d'expression. (B)

A) Du droit d'accès à Internet au droit d'accès aux réseaux sociaux

Au regard de l'évolution de l'usage d'Internet, il est de plus en plus évident qu'il s'avère être un outil essentiel à divers égards. Au plan pratique, il est souvent incontournable dans une multitude de démarches administratives essentielles à un bon déroulement du service public dont les usagers français peuvent avoir besoin pour faire valoir leurs droits. L'accès à Internet est donc une nécessité fondamentale. Au plan de la communication, Internet s'est imposé comme le moteur principal des réseaux sociaux au travers desquels la liberté d'expression peut s'exercer. L'accès aux réseaux sociaux est devenu un vecteur d'expression pour l'Homme. Or, l'adoption de la loi du 12 juin 2009 dite « Hadopi 1 »[16] ou « loi création et Internet » favorisant la diffusion et la protection de la création sur Internet est venue impacter l'accès à Internet. Le texte instaure la création d'une Haute autorité pour la diffusion des œuvres et la protection des droits sur l'Internet chargée de veiller à la prévention et à la sanction du piratage des œuvres. Autrement dit, l'objectif du législateur est de dissuader les internautes de télécharger illégalement des œuvres. En cas de non respect des dispositions et de piratage, la loi prévoyait la mise en œuvre d'une « riposte graduée » par l'HADOPI allant de l'envoi d'un message d'avertissement jusqu'à la possibilité de prononcer une coupure de la connexion des abonnés en cas de récidive. Face à l'adoption de cette loi, le Conseil constitutionnel est saisi au motif qu'un tel pouvoir donné à une autorité administrative indépendante portait atteinte au droit à la liberté d'expression et instituait des sanctions manifestement disproportionnées rendant ce pouvoir répressif inconstitutionnel. Dans une décision en date du 10 juin 2009[17], les gardiens de la Constitution ont censuré le volet répressif de cette loi en estimant que seules les instances judiciaires étaient compétentes pour décider de couper un abonnement internet et non une simple autorité administrative. Cette décision du

[16] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet
[17] Décision n°2009-580 DC 10 juin 2009 du Conseil Constitutionnel

Conseil constitutionnel apparait comme fondamentale et emblématique puisqu'elle proclame que l'accès à Internet est une composante de la liberté d'expression. A travers cette décision, le Conseil laisse entendre un signal fort sur la place consacrée à la liberté d'expression sur Internet et précise que la liberté d'expression, c'est-à-dire la libre communication des pensées et des opinions, implique la liberté d'accès à Internet. De ce fait, les juges reconnaissent donc un nouveau droit-liberté : le droit d'accès à internet. Ce droit d'accès à Internet est nécessairement rattaché à la liberté d'expression, mais également à l'évolution technologique puisque le Conseil des Sages précise que cette décision a été prise « en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions ». Si pour certains auteurs, cette décision ne consacre pas, en lui-même, un droit fondamental d'accès à Internet ou encore un droit de l'homme puisqu'il doit uniquement être reconnu comme : « un moyen de concrétisation de la liberté d'expression et de communication »[18], pour d'autres, elle protège le droit d'accès à Internet au même titre qu'un droit fondamental et en en faisant un droit constitutionnel au motif que l'accès à internet constitue l'une des modalités d'exercice de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789.[19] Dans son étude annuelle de 2014, le Conseil d'Etat allait dans le sens de la seconde position.[20] De plus, le Conseil souligne qu'il s'agit « [d'] un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ». Afin de stopper la divergence d'opinions, la loi du 7 octobre 2016 pour une République numérique[21] est venue reconnaître l'accès à Internet comme un droit fondamental en France puisqu'elle oblige les fournisseurs à maintenir la connexion de leurs abonnés en cas de factures impayés. Désormais, l'article L115-3 du code de l'action sociale et des familles[22] considère que l'accès à Internet est un service essentiel au même titre que l'eau, le gaz et l'électricité. Au niveau européen, le Parlement européen a adopté le 26 mars 2009 une recommandation relative aux libertés fondamentales sur Internet rappelant au Conseil de l'Union Européenne qu'il doit garantir l'accès à internet[23]. Si cette recommandation n'a pas d'impact sur le droit interne, la Cour de justice de l'Union européenne a rappelé dans un arrêt du 13 décembre 1989 dit Salvatore Grimaldi c/ Fonds des maladies professionnelles[24] que les juges nationaux doivent prendre en compte ces recommandations lorsqu'elles leur permettent d'avoir une

[18] M. Bardin, « Le droit d'accès à internet : entre « choix de société » et protection des droits existants » , RLDI 2013, n°91
[19] L. Marino, *Le droit d'accès à internet, nouveau droit fondamental* , Recueil Dalloz 2009, p.2045
[20] Etude annuelle 2014 du CE – Le numérique et les droits fondamentaux
[21] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
[22] Article L115-3 al.1 du Code de l'action sociale et des famille : « Dans les conditions fixées par la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement, toute personne ou famille éprouvant des difficultés particulières, au regard notamment de son patrimoine, de l'insuffisance de ses ressources ou de ses conditions d'existence, a droit à une aide de la collectivité pour disposer de la fourniture d'eau, d'énergie, d'un service de téléphonie fixe et d'un service d'accès à internet. »
[23] Recommandation n°2008/2160 du Parlement européen du 26 mars 2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet
[24] CJUE, 2e chambre, Salvatore Grimaldi c/ Fonds des maladies professionnelles, 13 décembre 1989, n°322/88, Recueil de jurisprudence 1989, p.04407

meilleure interprétation des dispositions nationales. A l'échelle internationale, le conseil des droits de l'homme de l'Organisation des nations unies reconnaît, dans une résolution votée le 5 juillet 2012, que l'accès à Internet est un droit fondamental au même titre que d'autres droits de l'Homme. Malgré le fait que cette résolution ne soit pas contraignante d'un point de vue juridique, elle envoie un message international. Ce respect à l'accès à Internet est pris en compte lors des bilans annuels des Etats en matière de respect des droits fondamentaux. De plus, l'article 19 de la Déclaration universelle des droits de l'homme[25] et l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[26] définissent la liberté d'opinion et d'expression, et donc entre autre la liberté d'accès à Internet, comme celle d'émettre et de recevoir des idées ou informations de toute nature. Or, la liberté de réception suppose un accès le plus large possible à tous les moyens de communication et par conséquent, incluant la communication en ligne. [27] D'ailleurs, dans un arrêt du 18 décembre 2012 dit Ahmet Yildirim c/ Turquie[28], la CEDH a souligné l'importance des sites internet en précisant que : « l'Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit de liberté d'expression et d'information ». Ainsi, le droit d'accès à Internet nécessite l'accès aux moyens de communication de toute nature qu'ils soient. Les réseaux sociaux sont des services web correspondant à un moyen de communication puisqu'ils permettent de diffuser et de recevoir du contenu. Ces derniers disposent de spécificités propres, par exemple la capacité de personnalisation à travers les profils ou bien la diversité des contenus. En outre, même si le contenu peut être obtenu par un autre moyen de communication, les réseaux sociaux constituent un type de services à part entière et leur accès doit rester libre afin que l'internaute puisse choisir le moyen de communication le plus adapté à ses besoins.[29] Par conséquent, de ce droit général d'accès à Internet peut découler un droit plus spécifique qu'est celui du droit d'accès aux réseaux sociaux.

A l'heure de la fulgurance des réseaux sociaux, ce type de service constitue un élément quasi-incontournable du lien social, voir même, le lieu d'exercice de droits fondamentaux tels que la liberté d'expression. L'accès au service Internet et la possibilité d'y exprimer ses idées, notamment à travers les réseaux sociaux sont donc des corollaires de la liberté d'expression. [30] Le Conseil constitutionnel l'a rappelé dans une décision du 18 juin 2020[31] venue censurer une grande partie des dispositions de la loi dite « Avia »[32] adoptée le 13 mai 2020 visant à lutter contre les contenus

[25] Article 19 de la Déclaration universelle des droits de l'homme de 1948 : « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit. »
[26] Article 10 de la CEDH : « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. »
[27] P. Mouron, « L'accès aux réseaux sociaux est un droit constitutionnel selon la Cour suprême des Etats-Unis », Revue européenne des médias et du numérique, IREC, 2017, pp.62-64.
[28] CEDH, 2e section, Ahmet Yildirim c/ Turquie, 18 décembre 2012, n°311/10
[29] P. Mouron, *Op.cit*
[30] J-S Mariez et L. Godfrin, « Censure de la « loi Avia » par le Conseil constitutionnel : un fil rouge pour les législateurs français et européen ?, Dalloz actualité, 29 juin 2020
[31] Décision n°2020-801DC du 18 juin 2020 du Conseil Constitutionnel
[32] Loi n°2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

haineux sur Internet. En substance, cette loi imposait aux réseaux sociaux de retirer sous une heure les contenus à caractère terroristes ou pédopornographiques et sous vingt-quatre heures les contenus haineux, dès lors qu'ils ont été signalés par des internautes, sous la menace d'une importante amende en cas de non respect. Avant même son adoption, ce projet de loi a suscité de nombreuses critiques estimant qu'il portait atteinte à la liberté d'expression et de communication. Pour prononcer l'inconstitutionnalité de cette loi, les Sages reprennent les multiples critiques soulevées par les opposants en pointant la technicité juridique des délits en cause, la nécessaire appréciation du contexte, le risque de signalements nombreux et infondés à traiter dans un court délai ou encore la sévérité de la peine, incitant les plateformes à retirer systématiquement les contenus signalés.[33] Le Conseil censure la loi dite « Avia » au motif que son adoption est « une atteinte à l'exercice de la liberté d'expression et de communication qui n'est pas nécessaire, adaptée et proportionnée ». Dans cette décision, les juges ont repris, en premier lieu, une formule similaire à celle rendue le 10 juin 2009 censurant la loi Hadopi I en précisant qu'« en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, [la liberté de communication] implique la liberté d'accéder à ces services ». En second lieu, ils sont venus ajouter un droit, tout aussi fondamental, celui de « s'y exprimer ». Par conséquent, cette décision introduit, dans le champ de la liberté d'expression qui est constitutionnellement protégée, le droit de chaque citoyen à s'exprimer sur les réseaux sociaux. [34]

Au vu de la motivation du Conseil des Sages, cette censure peut être perçue, indirectement, comme les prémices de la création d'un nouveau droit à valeur constitutionnelle en France pouvant être qualifié de droit d'accès aux réseaux sociaux. Dès lors, la France prendrait une position dans le sillon de celle prise par la Cour suprême des Etats-Unis qui, dans un arrêt du 19 juin 2017, considère que l'accès aux réseaux sociaux est un droit constitutionnel relevant du droit à l'information et de la liberté d'expression garantis par le premier amendement de la Constitution. Dans cette affaire, un homme s'était vu interdire l'ouverture d'un compte sur le réseau social Facebook, en vertu de la loi de l'Etat de Caroline du Nord, à la suite d'une condamnation pour un délit sexuel. Ce dernier décida de se créer un compte sous une fausse identité sur le réseau social et fut condamné pour fraude. Après avoir contesté la loi de l'Etat de Caroline du Nord au motif qu'elle violerait la liberté d'expression, l'affaire fut portée devant la Cour suprême des Etats-Unis. La Cour reconnaît alors que les réseaux sociaux constituent des vecteurs de la liberté d'expression car elle peut être exercée dans des lieux virtuels qui relèvent du cyberespace et qui permettent des

[33] C. Bigot, « Régulation des contenus de haine sur internet : retour sur le désaveu infligé par le Conseil constitutionnel à l'encontre de la loi dite « Avia », Recueil Dalloz 2020, p.1448
[34] *Ibid*

échanges illimités mais aussi peu coûteux. [35] De plus, malgré la volonté de protéger les mineurs des prédateurs sexuels, la loi de Caroline du Nord interdisant totalement l'accès aux réseaux sociaux aux délinquants est une atteinte disproportionnée à la liberté d'expression. Les réseaux sociaux sont des services qui permettent de s'informer librement et communiquer facilement. Donc pour la Cour, ils permettent l'exercice de nombreuses activités relevant de la liberté d'expression et facilitent la réinsertion des délinquants dans la société après avoir purgés leur peine. Ainsi, la loi de Caroline du Nord prive ces personnes visées des moyens d'exercice de l'une des plus importantes libertés : la liberté d'expression.

L'accès aux réseaux sociaux est donc une modalité essentielle à l'exercice d'autres droits fondamentaux tel que la liberté d'expression. Or, en limitant l'accès aux réseaux sociaux, le législateur doit avoir conscience des répercussions que cette barrière peut avoir sur les autres droits fondamentaux. En cette ère 2.0, le droit à la liberté d'expression, essentiel à l'épanouissement personnel des mineurs, est principalement exercé par ces derniers à travers les réseaux sociaux. Cependant, le législateur est venu restreindre leur accès aux réseaux sociaux avec la mise en place d'une majorité numérique afin de les protéger des dangers et des dérives de ces plateformes. Il est donc complexe de trouver un juste équilibre entre restriction de l'espace du mineur sur le net pour le protéger et respect de son droit à la liberté d'expression. (B)

B) L'exercice du droit à la liberté d'expression sur les réseaux sociaux

Le droit à la liberté d'expression est reconnu à l'article 10 de la DDHC de 1789 qui pose que : « Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi. », mais aussi par l'article 11 qui prévoit que : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. ». Ces deux articles ont une valeur constitutionnelle puisque le préambule de la Constitution du 4 octobre 1958 renvoie à la DDHC de 1789 et ce droit est également reconnu par de nombreux textes internationaux. Le droit à la liberté d'expression appartient aussi bien au citoyen majeur qu'au mineur comme le souligne l'article 13 de la Convention internationale des droits de l'enfance qui prévoit une protection spécifique de la liberté d'expression pour le mineur.[36] C'est un droit universel permettant à chacun d'avoir son opinion, ses idées et de l'exprimer par n'importe quel moyen. La liberté d'expression peut prendre plusieurs

[35] P. Mouron, *Op.cit*

[36] Article 13 de la CIDE : « L'enfant a droit à la liberté d'expression. Ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen du choix de l'enfant. »

formes : elle peut être orale ou écrite et peut se retrouver aussi bien dans les journaux que sur les réseaux sociaux. La liberté d'expression est aujourd'hui analysée comme la plus représentative des libertés mais elle est également soumise à des limites : même si elle est considérée comme un droit fondamental à valeur constitutionnel, il ne s'agit pas d'un droit absolu. Si les textes viennent la protéger, ils lui fixent certaines limites en renvoyant aux cas prévus par la loi. Ainsi, la loi sanctionne l'incitation à la haine et la diffusion de propos injurieux, raciales, antisémites, homophobes ou bien diffamatoires tenus sur Internet et en particulier sur les réseaux sociaux.

Les réseaux sociaux sont une zone d'expression libre qui permettent aux citoyens d'exercer l'un des droits les plus fondamentaux : la liberté d'expression. La durabilité illimitée et la diffusion mondiale des informations diffusés sur ces plateformes donnent à cette liberté d'expression une forme universelle.[37] Par conséquent, quid du droit permettant d'encadrer l'utilisation des réseaux sociaux pour limiter les abus et permettre un bon exercice de la liberté d'expression ? Il ressort que les actes répréhensibles réalisés sur les réseaux sociaux sont soumis aux mêmes dispositions que ceux réalisés par voie presse écrite ou tout autre support. En effet, la loi du 29 juillet 1881 sur la liberté de la presse a été conçue pour appréhender toutes les formes de communication. De ce fait, le droit de la presse pourra s'appliquer dès que la qualification de média pourra être retenue. Le fait de conférer aux réseaux sociaux la qualité de média rend applicable cette législation envers tous les propos diffamatoire ou injurieux exprimés sur ce support. En effet, dès que l'utilisateur d'un réseau social publie un message, ce dernier devient éditeur d'information et par conséquent responsable de ce qu'il publie. Toutefois, cette loi vise uniquement les propos publics. Or, lorsque les propos tenus sont accessibles qu'à un nombre restreint de personnes, ils sont considérés comme étant des propos privés et ne relevant pas de ladite loi. En ce qui concerne la tenue de propos d'incitation à la haine raciale raciale, dans son rapport « Internet et les réseaux numérique » de 1998, le Conseil d'Etat souligne que le champ d'application de la loi nationale peut être étendu le plus largement possible lorsque l'auteur des propos est français et que le message est accessible en France. [38] De ce fait, même si les propos sont tenus sur une plateforme étrangère, la majorité sont américains, la loi française a vocation à s'appliquer.

A l'instar du grand nombre de mineurs connectés quotidiennement sur Internet et possédant un compte sur les réseaux sociaux, ces derniers s'avèrent être le support d'expression favoris des jeunes où ils s'expriment parfois sans filtre ni pudeur sans avoir conscience à quel point il s'agit d'une véritable vitrine exposant leurs propos à d'innombrables internautes. Or, il est important que le mineur garde à l'esprit qu'il est responsable de ce qu'il écrit sur les réseaux sociaux. De ce fait, quel que soit son âge, si le mineur tient de tels propos sur les réseaux sociaux, comme le prévoit

[37] R. Fassi-Fihri, « Quel droit pour les réseaux sociaux ? », Revue de droit public, n°3, 1er mai 2018 p.685
[38] Rapport du CE , « Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'Etat3, p.171

l'article 121-1 du Code pénal[39], sa responsabilité pénale pourra être engagée. Toutefois, seul l'enfant de 13 ans et plus qui commet une infraction pourra encourir une peine d'amende et d'emprisonnement devant des juridictions spécialisées et selon des modalités adaptées. De plus, le mineur doit être conscient qu'il est important de rester maître de son identité numérique et de ne pas la compromettre car la durabilité de tout ce qui est publié et archivé sur le web est quasi illimité. Des propos tenus dans le passé peuvent s'avérer être de véritables « bombes à retardement » et devenir préjudiciables lorsqu'ils réapparaissent. C'est l'expérience qu'a vécu un candidat représentant la France au concours Eurovision de la chanson, évènement annuel organisé par l'Union européenne de radio-télévisions, qui a vu sa participation remise en cause à la suite de la résurgence de tweets antisémites postés à l'âge de 14 ans et relayés sur les réseaux sociaux. Cette résurgence peut être faite à l'initiative de personnes malveillantes ou qui ont un intérêt à créer un préjudice à la personne visée.

Toutefois, malgré la volonté du législateur d'encadrer de plus en plus la parole en ligne, l'arbitrage de la liberté d'expression a été abandonné aux réseaux sociaux eux-mêmes. [40] En pratique, ce sont les modérateurs des plateformes qui définissent les limites de la liberté d'expression. Autrement dit, ce sont les plateformes elles-mêmes qui définissent ce qui peut être écrit ou non en ligne. De plus, une grande partie de la modération est faite par des algorithmes. Par conséquent, parfois, un message peut être considéré comme dépassant les limites de la liberté d'expression et donc être supprimé avant même qu'il ne soit lu par un humain. Or, comme l'a souligné Mark Zuckerberg, cette compétence est celle du système judiciaire et non celle d'une entreprise privée. Les règles créées par les réseaux eux-mêmes ne peuvent pas se substituer au droit.

Par conséquent, les réseaux sociaux sont des plateformes sans limite de temps et de frontières, mais ils ne sont pas un espace de non-droit. Dès lors, les propos émis ne sont pas toujours maîtrisés et peuvent tomber sous la qualification d'infraction pénale. Les réseaux sociaux sont donc un moyen pour le mineur d'exercer de façon encadrée son droit à la liberté d'expression. Si, en parallèle, ils peuvent être un terrain propice à l'atteinte du droit à la vie privée et du droit à l'image, ils bénéficient d'une protection indiscutable. (Paragraphe 2)

[39] Article 121-1 du C.pén. : « Nul n'est responsable pénalement que de son propre fait »
[40] D.Leloup, « Malgré les lois, l'Etat a abandonné aux réseaux sociaux l'arbitrage de la liberté d'expression », Le Monde, 19 février 2020

Paragraphe 2 : La protection du droit à la vie privée et du droit à l'image sur les réseaux sociaux

Le développement d'Internet et des réseaux sociaux est venu perturber la vision de la vie privée. L'interprétation du droit au respect de la vie privée évolue au rythme des nouvelles technologies. Au cours du XIXe siècle, les premières questions sur l'atteinte à la vie privée sont apparues avec les journaux. Depuis la fin du XXe et le début XXIe siècle, Internet est venu remodeler l'idée du respect de la vie privée en intégrant à ce principe la protection des données personnelles. De part sa vulnérabilité et son hyperconnexion, le mineur doit faire l'objet d'une protection spécifique pour ses données personnelles. (A) En parallèle, le droit à l'image est également touché par ce nouvel intérêt à divulguer des éléments de la vie privée à travers des publications de photos sur les réseaux sociaux. Toutefois, l'image du mineur est protégée par la nécessité du double consentement des titulaires de l'autorité parentale pour la publication de photos sur un réseau social. (B)

A) La protection du droit à la vie privée par la protection des données à caractère personnel

A l'ère des réseaux sociaux, la protection de la vie privée et des données personnelles devient un défi pour les utilisateurs ainsi que pour les organismes chargés d'encadrer leur utilisation. Dans les conditions générales d'utilisation de Facebook, Snapchat ou encore Instagram, le respect à la vie privée est lié à la collecte de données à caractère personnel. La protection de la vie privée est plus ancienne que la protection des données personnelles. En effet, le droit à la vie privée a été introduit dans le droit français par la loi n°70-643 du 17 juillet 1970. Ce droit est reconnu par de nombreux textes : l'article 9 du Code Civil[41] ou bien l'article 8 de la Convention Européenne des Droits de l'Homme[42] ou encore l'article 2 de la Déclaration des Droits de l'Homme et du Citoyens de 1789. Toutefois, le droit au respect de la vie privée est un droit difficile à délimiter car aucun texte ne donne sa définition. C'est pour cette raison que la jurisprudence est intervenue pour préciser que pouvaient rentrer dans le domaine de la vie privée : l'image[43], la vie familiale et les origines familiales[44] ainsi que de nombreux autres éléments. Donc, le droit au respect de la vie privée permet de protéger une personne contre l'atteinte à l'intimité de sa vie privée et instaure un devoir de non-immixtion aux tiers. Cependant, lorsque la personne a consenti à l'immixtion, il n'y a pas d'atteinte à sa vie privée.

[41] Article 9 c.civ : « Chacun a droit au respect de sa vie privée. »
[42] Article 8 alinéa 1 CEDH : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »
[43] CCass, Civ.2e, 5 mars 1997, n°95-14.503
[44] CCass, Civ.1re, 16 octobre 1984, n°83-11.786, Bull. civ. I, n°268

Récemment, le RGPD[45] a fait entrer dans le domaine du respect de la vie privée les données ayant un impact particulier sur la vie privée. Désormais, une protection particulière est prévue pour ces données à caractère personnel. Ce règlement européen définit la notion de données à caractère personnel comme étant : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[46]. Derrière les données à caractère personnel se cachent les informations qui permettent d'identifier une personne physique tel que le nom ou une photo. [47] Ces éléments sont exigés pour ouvrir un compte sur un réseau social. Au regard de la législation européenne, la protection des données personnelles est reconnue comme un droit fondamental par le traité de Lisbonne et de la Charte des droits fondamentaux de l'Union européenne.

Lors de l'adoption de la loi Informatique et Libertés du 6 janvier 1978[48], aucune disposition relative aux données personnelles des mineurs n'était prévue : les majeurs et les mineurs étaient protégés de la même façon. Il n'y avait aucune distinction d'âge. L'article 38 de la loi Informatique et Libertés a instauré un droit d'opposition. Une personne peut donc s'opposer pour des motifs légitimes à la diffusion, la transmission ou la conservation de données la concernant. En complément du droit d'opposition, il y a le droit à l'oubli numérique qui permet à tout citoyen français d'exiger, sous certaines conditions, l'effacement de textes, images, commentaires contenant des données à caractère personnel le concernant. Ces contenus peuvent être effacés dès leur publication. Néanmoins, afin de protéger au maximum les données personnelles, le droit à l'oubli ne fait pas l'objet d'un délai de prescription et de limite de date. De ce fait, les contenus très anciens peuvent également être effacés. Le droit à l'oubli numérique peut s'appliquer par deux types de suppression des données à caractère personnel. D'une part, il y a le droit à l'effacement consacré à l'article 40 de la loi Informatique et Libertés. Ici, il s'agit d'une suppression des données personnelles dès lors que ces dernières sont inexactes, incomplètes, équivoques, périmées ou si leur collecte, utilisation, communication ou conservation sont interdites. D'autre part, la jurisprudence Google Spain c/ Agencia Española de Protección de Datos de la Cour de justice de

[45] Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[46] Article 4 -1 du règlement (UE) n°2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

[47] O. Tambou, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déférencement », RTD Eur. 2016, p.249

[48] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

l'Union européenne[49] est venue consacrer un nouveau droit : le droit au déréférencement. Ici, l'oubli est partiel car il ne s'agit pas de demander la suppression des informations mais de demander au propriétaire du moteur de recherche d'interdire d'afficher certains résultats de recherche ayant l'identité de la personne comme mots clés. Les outils permettant d'obtenir la suppression d'informations et d'assurer une protection des données personnelles face à l'utilisation des réseaux sont nombreux. Cependant, cette protection initialement prévue n'était pas spécifique aux mineurs.

Pendant longtemps, les risques de traces laissées par les mineurs sur Internet ou les réseaux sociaux ont été négligés. Or, face à l'inconscience des adolescents à « partager » sur les réseaux sociaux toutes sortes d'informations les concernant ou concernant leur entourage, le législateur français a décidé d'apporter une protection spécifique au mineur par la loi pour une République numérique du 7 octobre 2016[50]. Ainsi, l'article 63 de la loi pour une République numérique modifie l'article 40 de la loi Informatique et Libertés en consacrant un véritable droit d'oubli au bénéfice des mineurs. [51] Désormais, les mineurs bénéficient d'une procédure accélérée pour l'effacement de leurs données à caractère personnel collectées. Tout d'abord, la personne concernée devait être mineure au moment de la collecte des données. Ensuite, la loi couvre toute donnée « collectée » c'est-à-dire peu importe que ce soit le mineur, un tiers mineur ou un majeur qui l'ait publiée. Enfin, il n'y a pas de délai de prescription pour demander l'effacement des données au responsable de traitement. Selon la directive n°95/46/CE[52], le responsable de traitement est : « l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.». De ce fait, les réseaux sociaux gratuits ou payants sont considérés comme responsables de traitement. [53] Afin d'avoir une protection maximale, lorsque le responsable de traitement a transmis les données collectées à un autre responsable de traitement, le premier devra signaler le second de l'effacement des données.

Par la suite, le droit européen est également venu apporté une protection par l'adoption du RGPD, applicable à partir du 25 mai 2018, en soulignant au considérant 38 du préambule[54] la nécessité d'une protection spécifique pour les données à caractère personnel des enfants utilisées

[49] CJUE, 13 mai 2014, « Google Spain SL, Google Inc./ Agencia Española de Protección de Datos, Mario Costeja González », C-131/12
[50] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
[51] Article 40-II alinéa 1er loi Informatique et Libertés : « Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. ».
[52] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données
[53] M. Péron, « Libre propos sur le droir à l'oubli numérique », RDLF2017, chron. n°15
[54] Considérant 38 du RGPD (Préambule): « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. »

lors de l'utilisation de services proposés directement à un enfant, à des fins marketing ainsi que pour la création de profils de personnalité ou d'utilisateur. De plus, le règlement prévoit à l'article 17 un droit à l'oubli. Ce dispositif permet à tout citoyen résidant dans un pays membre de l'Union européenne de demander l'effacement les données personnelles qui le concernent. Le point f du paragraphe 1 de ce dit article précise que les enfants bénéficient de ce même droit à l'oubli. Ainsi, pour les mineurs, ce droit est relativement identique à celui déjà introduit en droit interne. La seule différence est que le règlement vise les données collectées auprès « d'enfants » alors que la loi française vise les données collectées auprès « de personnes mineures ». Cette différence de formulation a interpellé les praticiens : tous les mineurs doivent-ils être considérés comme des enfants ? La notion d'enfant ne vise-t-elle que les mineurs les plus jeunes ? Le droit à l'oubli européen serait-il plus restrictif que notre droit interne actuel ? [55] L'article 8 du RGPD relatif au consentement des enfants précise qu'un enfant peut être âgé d'au moins seize ans. De ce fait, le RGPD protège les enfants âgés de seize ans et plus alors que la législation française protège les enfants de moins de dix-huit ans. De plus, le RGPD apporte une protection spécifique pour le traitement des données à caractère personnel des mineurs. En effet, l'article 6 du règlement énumère les différentes bases légales rendant licite le traitement d'une donnée à caractère personnel et prévoit des aménagements spécifiques lorsque les données traitées concernent un mineur. Ainsi, le point f de l'article 6-1 du RGPD prévoit que le traitement des données est licite s'il : « est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ». De ce fait, dès lors qu'il y a une mise en balance entre les intérêts du mineur et les intérêts du responsable de traitement, ce sont toujours les intérêts du mineur qui priment.

Le RGPD n'a donc pas révolutionné le droit à l'oubli des mineurs en France puisque le droit interne l'avait anticipé avec la loi pour une République numérique. Il a uniquement permis une harmonisation des législations et la protection de tous les enfants européens en leur garantissant ce droit.[56] Cependant, en permettant au mineur d'effacer les données à caractère personnel collectées, le législateur lui a redonné un pouvoir de contrôle sur ses informations. [57] Si le mineur est acteur dans la protection de sa vie privée, en revanche, en ce qui concerne le droit à l'image, le processus de protection est différent. En effet, celui-ci est délégué aux titulaires de l'autorité parentale. (B)

[55] O. Foret, « Le droit à l'oubli des mineurs », Dalloz IP/IT 2018, p.350
[56] *Ibid*
[57] A. Bensoussan, « Le « droit à l'oubli » sur internet », Gaz. Pal. 6 février 2010, n°37, P.3

B) La protection du droit à l'image par le double consentement des titulaires de l'autorité parentale

Selon Michael Stora, psychologue – psychanalyste et co-fondateur de l'Observatoire des mondes numériques en sciences humaines : « *Dans la bulle Internet, c'est avec des cas de jurisprudence que l'on commence à instaurer des lois, car il n'existe actuellement aucune loi concernant le droit à l'image spécifique à l'exposition sur les réseaux sociaux. Concrètement, les parents ont le droit de poster des photos de leurs enfants sur les réseaux sociaux car les mineurs partagent leur droit à l'image avec leurs parents jusqu'à leur majorité.* ». La publication, plus ou moins massive, sur les réseaux sociaux de photos de ses enfants est devenue une pratique courante. Pourtant, elle n'est pas anodine puisqu'elle touche le droit à l'image de l'enfant. D'après une étude de 2018[58], 24% des parents publient une photo ou une vidéo de leurs enfants sur les réseaux sociaux au moins une fois par jour. Ce phénomène est appelé le « sharenting ». Cette expression anglosaxone est un néologisme tiré de la contraction de « share », qui signifie partager, et « parenting » qui renvoie à l'adjectif parental. Ce terme fait référence à l'exhibition quotidienne, par certains parents, de leurs enfants sur les réseaux sociaux.

Le droit à l'image est le droit de chacun sur son image. Autrement dit, pour toute diffusion de l'image d'une personne, cette dernière doit y avoir consenti, quel qu'en soit le support. La Cour de cassation a précisé que, pour qu'il y ait une atteinte au droit à l'image, il est nécessaire qu'une identification de la personne représentée soit possible. [59] Le droit à l'image se décompose en droit à la captation de l'image et en droit à la diffusion de l'image. La captation de l'image de la personne est le fait de la prendre en photo, la filmer, la dessiner ou la peindre[60]. Dès lors, cet acte doit faire l'objet d'un consentement de la personne. Toutefois, le consentement est présumé lorsque le droit à l'image est envisagé dans un lieu public. Une fois la captation de l'image faite, il faut à nouveau le consentement de la personne pour qu'elle soit diffusée et exploitée. Le fait qu'une personne consente à être photographiée ne signifie pas qu'elle consent à ce qu'elle soit diffusée. Le droit à l'image s'applique également sur Internet. Avant la publication en ligne, il est essentiel de s'assurer que les personnes représentées et reconnaissables sur l'image soient d'accord avec sa diffusion. Au quel cas, le droit à l'image peut être invoqué afin d'enlever les photos du net. Lorsque la personne qui apparaît sur l'image est une personne mineure, il faut recueillir l'autorisation des titulaires de l'autorité parentale. [61] L'autorité parentale attribue aux parents des

[58] Etude du 28 août 2018 menée par la société McAffee
[59] Civ. 1ère, 21 mars 2006
[60] Civ.1ère, 8 janvier 1980, Bull.civ.I,n°18, D.1980.IR 258
[61] Civ. 1ère, 12 décembre 2000, n°98-21.311, X c/ Julien, Juris-Data n°2000-007309

droits et des devoirs vis-à-vis de leur enfant jusqu'à sa majorité ou son émancipation. Le principe est l'exercice conjoint de l'autorité parentale prévu à l'article 372 du Code Civil.[62] De ce fait, il faut l'accord des deux parents pour la diffusion de l'image d'un enfant et cela même en cas de séparation des parents comme le précise l'article 373-2 du Code Civil. [63] Toutefois, l'exercice conjoint de l'autorité parentale ne signifie pas que toutes les décisions doivent être prises par les deux parents d'un commun accord. En effet, le Code civil pose une présomption d'accord en cas d'accomplissement d'un acte usuel par l'un des parents. Or, il reste muet quant à la définition de cet acte. Il faut donc se pencher sur les décisions rendues par les Cours et les Tribunaux pour faire la distinction entre acte usuel et acte non usuel. Tout d'abord, les actes usuels sont les actes habituels, de faible gravité qui s'inscrivent dans la vie courante de l'enfant. La jurisprudence a considéré comme acte usuel l'établissement d'un passeport pour l'enfant mineur[64] ou bien l'inscription dans un établissement scolaire[65]. Pour ce type d'acte, un parent peut décider seul d'accomplir l'acte et l'autre parent sera présumé avoir donné son accord. Ensuite, les actes non usuels sont les actes dit comme étant importants, inhabituels, graves. Ils nécessitent toujours l'accord des deux parents. Une proposition de loi du 1er avril 2014 vise à définir l'acte non usuel comme étant : « L'acte qui rompt avec le passé et engage l'avenir de l'enfant ou qui touche à ses droits fondamentaux ». Ainsi, la jurisprudence a considéré comme actes non usuels le passage à la télévision d'un enfant dans un documentaire consacré aux familles de divorcés[66], ou bien les actions en justice exercées au nom de l'enfant mineur [67], ou encore le changement de nationalité de l'enfant[68]. Dès lors, si un parent agit sans l'accord de l'autre, il s'expose à engager sa responsabilité et à se voir diminuer de ses droits liés à l'autorité parentale.

Quid de la publication d'une photo de son enfant sur les réseaux sociaux ? La cour d'appel de Paris précise qu'est « interdit à chacun des parents de diffuser des photographies des enfants sur tous supports sans l'accord de l'autre parent »[69]. En se positionnant de la sorte, les juges montrent une certaine méfiance des réseaux sociaux et une volonté de protéger les enfants des dangers auxquels ils peuvent être exposés lorsque des photos d'eux sont publiées sur ces plateformes. Indirectement, avec cette position, la cour d'appel de Paris considère la diffusion de photos de son enfant sur les réseaux sociaux comme un acte non usuel nécessitant l'accord des deux parents. Elle se positionne dans le même sens que la cour d'appel de Versailles qui a souligné que : « la publication de photographies de l'enfant et de commentaires relatifs à celui-ci sur le site Facebook ne constitue pas un acte usuel mais nécessite l'accord des deux parents ». [70] Dans cette affaire, un

[62] Article 372 alinéa 1 C.civ : « Les père et mère exercent en commun l'autorité parentale ».
[63] Article 373-2 alinéa 1 C.civ : « La séparation des parents est sans incidence sur les règles de dévolution de l'exercice de l'autorité parentale. »
[64] CE 8 février 1999, Dr.fam.1999, n°40, note Murat
[65] CE. 13 avril 2018
[66] CA. Versailles, 11 septembre 2003
[67] CA Versailles, 31 janvier 2013, n° 11/03284, JurisData n° 2013-004990
[68] CCass, Civ.1, décembre 2013, n° 12-26161
[69] CA Paris, 9 février 2017, n°15-13956
[70] CA Versailles, 25 juin 2015, n°13-08349, JurisData n°2015-015861

père saisi le juge aux affaires familiales suite à la publication, sur le compte Facebook de la mère, des photos de leur enfant âgé de 4 ans. Il fonde sa requête sur le non respect de l'exercice conjoint de l'autorité parentale. La cour d'appel a fait droit à cette demande au motif que ce type de publication nécessite l'autorisation des deux parents. Ici, le juge aux affaires familiales s'est déclaré compétent. Cependant, dans un arrêt de la cour d'appel d'Aix-en-Provence, alors que la situation était identique, il résulte que : « le juge aux affaires familiales n'a pas compétence, aux termes des dispositions de l'article L.213-3 du code de l'organisation judiciaire pour statuer sur les actions relatives à la protection de l'image des enfants mineurs ». [71] Cette position s'explique par la différence de fondement. En effet, le fondement de la demande ne portait pas sur le non respect de l'autorité parentale, mais sur le non respect du droit à l'image. Par conséquent, lorsque la demande de suppression ou de cession des publications est fondée sur l'autorité parentale, le juge aux affaires familiales est compétent. En revanche, lorsque cette dernière est fondée sur le fondement du droit à l'image, le juge aux affaires familiales n'est pas le juge de droit commun compétent puisque l'atteinte au droit à l'image est sanctionnée sur le fondement de l'article 9 du Code civil qui consacre le droit au respect à la vie privée. Toutefois, la position de la cour d'appel de Versailles se démarque de celle qu'avait prise la cour d'appel de Bordeaux en 2011 alors que les faits étaient similaires : il s'agissait d'une mère qui désapprouvait les photos publiées par son ex-concubin de leur fille de 6 ans sur son profil Facebook et demandait à ce qu'elles soient retirées car elle n'avait pas consenti à la diffusion de ces images. Dans cet arrêt, la cour d'appel de Bordeaux déboute la mère de sa demande au motif que : « (…) les photographies de l'enfant s'inscrivent dans le cadre de la communication personnelle entre amis (photos d'anniversaire de l'enfant) (…) ». Autrement dit, selon les juges bordelais, si le compte Facebook est configuré en privé, c'est-à-dire de sorte à ce que seuls les « amis » puissent le consulter, l'accord de l'autre parent pour publier des photos sur le réseau social n'est pas nécessaire. D'après ce raisonnement, il faut distinguer : d'une part, les photos publiées et visibles par un groupe restreint correspondant à un acte usuel et ne nécessitant pas l'autorisation des deux parents ; d'autre part, les photos visibles et publiées par tout public correspondant à un acte non usuel et nécessitant l'autorisation des deux parents. Cependant, cette position reste isolée et la tendance est de considérer que le fait de publier des photos de son enfant sur les réseaux sociaux est un acte non usuel nécessitant donc l'accord des deux parents. La nécessité du double accord des titulaires de l'autorité parentale renforce donc la protection de l'enfant au regard de son droit à l'image.

S'il est essentiel que le droit à l'image, mais aussi le droit à la liberté d'expression et le droit à la vie privée soient assurés et respectés dans l'utilisation des réseaux sociaux, il également fondamental que la sécurité du mineur soit préservée face à la cybercriminalité. (Section 2)

[71] CA Aix-en-Provence, 10 septembre 2013, n°13-01400, Jurisdata 2013-024828

Section 2 : La lutte contre la cybercriminalité envers le mineur sur les réseaux sociaux

La révolution d'internet fait aujourd'hui partie intégrante de la vie de chacun, la jeune population née avec en a plus particulièrement intégré l'usage, jusqu'à parfois en faire une prolongation de sa vie. Si l'usage en est fait de manière réfléchie et maitrisé, c'est une mine d'information et de communication exceptionnel. Cependant, lorsque le jeune en abuse et se disperse dans son utilisation, allant parfois jusqu'à en perdre le contrôle, il s'expose à de nouveaux fléaux. La démocratisation et la vulgarisation des réseaux sociaux a fait naître une nouvelle délinquance à laquelle le législateur a dû faire face et qu'il a dû réprimer. La forme de cybercriminalité la plus communément connue est le cyberharcèlement dont les dégâts sont très contemporains. (Paragraphe 1) Par ailleurs, le législateur français a également réagi face à la criminalité sexuelle développée via internet et les réseaux sociaux en renforçant l'arsenal législatif afin d'encadrer une nouvelle menace : le grooming. (Paragraphe 2)

Paragraphe 1 : Le cyberharcèlement

Le harcèlement sur internet obéit aux mêmes mécanismes fondamentaux que le harcèlement classique et, pour les jeunes en particulier, le harcèlement scolaire. (A) En réaction au développement de cette délinquance et aux dégâts qu'elle occasionne de multiples dispositifs sont apparus et un certain nombre de structures ont été mises en place. C'est une lutte engagée autant par les pouvoirs publics que par les réseaux sociaux eux-mêmes. (B)

A) L'encadrement du cyberharcèlement corollaire du harcèlement scolaire

Le harcèlement est un délit qui consiste à imposer à une personne de façon répétée certains propos ou comportements qui portent atteinte à son intégrité physique ou psychique. [72] Ce délit est défini à l'article 222-32- 2-2 du Code pénal.[73] En clair, le harcèlement est caractérisé par deux éléments constitutifs : d'une part la répétition des comportements et sa fréquence, d'autre part l'intention de l'auteur ou par son effet sur la personne. Toutefois, pour caractériser l'infraction, l'intention malveillante n'est pas nécessaire : il suffit juste que la victime ait subi un dommage en

[72] P. Léger, « Le cyberharcèlement une infraction adaptée à la protection de la jeunesse en ligne », Dalloz IP/IT 2018 p. 346

[73] Article 222-33-2-2 du code pénal : « Le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni (…..) lorsqu'ils ont été commis par l'utilisation d'un service de communication au public en ligne. »

raison du harcèlement. La loi du 3 août 2018 [74] est venue élargir la définition du harcèlement. Désormais, le harcèlement peut être établi dès lors que plusieurs personnes s'en prennent à une même personne de façon concertée ou en sachant que leurs comportements constituent une répétition, même si chacun n'a agi qu'une seule fois. En droit français, le code pénal sanctionne aussi bien le harcèlement moral que le harcèlement sexuel.

De nos jours, le harcèlement moral apparaît de plus en plus via Internet, l'usage des réseaux sociaux et des téléphones portables. Selon le Ministère de l'Education Nationale, le harcèlement en ligne, appelé « cyberharcèlement » ou « cyberbullying », consiste en un acte agressif et intentionnel de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule et perpétré par un individu ou un groupe d'individus au moyen de communication électronique. Ce phénomène est apparu avec l'avènement des nouvelles technologies de l'information et de la communication. Les supports du cyberharcèlement peuvent être : les téléphones portables, les messageries instantanées, les forums, les chats, les jeux en ligne, les courriers électroniques, les réseaux sociaux ou bien les blogs. Le cyberharcèlement peut prendre diverses formes et représenter divers dangers. En premier lieu, le « flaming » qui est une forme de harcèlement à travers les réseaux sociaux consiste à envoyer des messages très violents, insultants ou menaçants. Ces attaques sont brutales et répétées. En second lieu, le « harassment » consiste à user mentalement la personne en multipliant les rumeurs à son sujet, tenir des propos diffamatoires et publier des informations dégradantes, vexantes ou blessantes de manière répétée. Ces petites attaques se font, principalement, sous formes de commentaires sur les réseaux sociaux. En troisième lieu, le dénigrement consiste à porter atteinte à l'image et la réputation d'une personne, en lançant toute sorte de rumeurs à son égard. L'idée est de décrédibiliser cette personne. En quatrième lieu, « l'exclusion » est une forme d'ostracisme puisque c'est une pratique qui a pour but de mettre volontairement une personne à l'écart d'un groupe. Cette exclusion peut avoir lieu sur les réseaux sociaux avec la création de « chats », c'est-à-dire de conversations se moquant d'une personne n'en faisant pas partie. En cinquième lieu, « l'usurpation d'identité » consiste à utiliser le pseudonyme d'une personne ou d'accéder à sa messagerie ou son profil et de se faire passer pour elle en envoyant des messages insultants à une autre personne. Le but de cette pratique est de nuire à la personne qui s'est faite insultée et à celle qui s'est fait usurper son identité. En sixième lieu, « l'outing » consiste à divulguer des informations intimes ou confidentielles sur une personne. En septième et dernier lieu, le « happy slapping » est une pratique qui a beaucoup fait parler au milieu des années 2000. Il s'agit de filmer une scène de violence ou une scène intime et de diffuser la vidéo sur les réseaux sociaux sans l'autorisation de la victime. Le harcèlement en ligne est sanctionné pénalement depuis la loi du 4 août 2014 [75] par la création de l'article 222-33-2-2 du

[74] Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes
[75] Loi n° 2014-873 du 4 août 2014 relative à l'égalité entre les femmes et les hommes

Code pénal qui encadre le délit de harcèlement moral. Donc, en droit français, il n'existe pas d'infraction spécifiquement dédiée au cyberharcèlement sur les mineurs. Toutefois, ce dit article prévoit que le harcèlement en ligne, d'une part, et envers une personne mineure de 15 ans ou moins, d'autre part, sont tout deux des circonstances aggravantes du délit de harcèlement moral. Le harcèlement est puni d'une peine d'un an d'emprisonnement et 15 000€ d'amende. En revanche, lorsqu'il s'agit de cyberharcèlement ou lorsque la victime est un mineur de moins de 15 ans ou une personne vulnérable ou subit une incapacité de travail de plus de huit jours, la peine encourue est de 2 ans et de 30 000€. Toutefois, en cas de cyberharcèlement sur mineur, la peine peut être portée à 3 ans de prison car deux circonstances aggravantes sont réunies : le cyberharcèlement et la minorité de la victime. Le législateur a donc bien pris en compte l'atteinte des mineurs par le harcèlement en ligne.

Si le cyberharcèlement est un phénomène récent, il peut être mis en parallèle avec le harcèlement scolaire, qui lui a toujours existé. D'après un rapport de l'UNICEF publié en 2018[76], « la moitié des élèves âgés de 13 à 15 ans dans le monde, soit près de 150 millions d'adolescents, rapportent avoir été exposés à la violence entre pairs à l'école et aux abords de l'école ». Le harcèlement scolaire est une violence physique ou morale exercée par un ou plusieurs élèves à l'encontre de l'un de ses pairs.[77] Le droit français ne dispose pas de loi spécifique sur le harcèlement scolaire, ce phénomène est rattaché à des composantes du harcèlement. Pourtant, nombreuses sont les conséquences qui découlent du harcèlement scolaire : la phobie scolaire, la dépression ou l'anxiété. Ce fléau débute à l'école et aujourd'hui se poursuit en dehors de l'enceinte des établissements scolaires avec l'hyperconnectivité des jeunes sur les réseaux sociaux. En outre, le cyberharcèlement peut être perçu comme un amplificateur du harcèlement scolaire traditionnel. Il s'agit d'une violence de proximité qui, le plus souvent, se diffuse entre les élèves. Cette cyberviolence est la continuité de ce qu'il se passe dans les établissements scolaires mais, cette fois-ci, sur la Toile. Aujourd'hui, la majorité des adolescents et même certains enfants possèdent un smartphone avec lequel ils peuvent se connecter aisément à Internet. Les conséquences de ce phénomène peuvent être très graves. Elles peuvent toucher la santé ou la scolarité du mineur. Le cyberharcèlement est donc plus intrusif que le harcèlement classique. Auparavant, lorsque l'enfant quittait l'école, il pouvait avoir des moments de répit en rentrant chez-lui : le soir, le week-end ou durant les vacances scolaires. Or, le drame du cyberharcèlement est que la persécution devient permanente, elle pénètre dans la sphère privée. De plus, le caractère non-verbal du harcèlement en ligne et la possibilité de rester anonyme libère les harceleurs de toute impunité et fait tomber une nouvelle limite. De part sa distance, le cyberharcèlement dispense les agresseurs d'un face à face

[76] UNICEF, « Violence à l'école et aux abords de l'école », 14 septembre 2018
[77] T. Labatut, « Harcèlement scolaire via internet et les médias sociaux : quels moyens de lutte ? », LPA 23 déc. 2019, n°149p4, p.11

avec leur victime, ce qui peut avoir pour effet d'exacerber la violence de leurs propos et de heurter d'autant plus leurs cibles. Enfin, la multiplicité des circuits par lesquels le harcèlement en ligne peut être pratiqué rend d'autant plus difficile le traquage et l'identification de ceux qui le pratiquent. Les réseaux sociaux peuvent donc être le théâtre du meilleur comme du pire. En écho à ce phénomène, les assurances scolaires ont intégré dans leur offre, depuis la rentrée 2020, le cyberharcèlement exercé dans la cour de récréation ou en dehors. [78] De plus, une lutte contre ce phénomène a vu le jour. (B)

B) La mise en place d'outils pour lutter contre le cyberharcèlement

Le harcèlement et le cyberharcèlement sont des fléaux qui dévastent l'école et la société. Dès 2011, suite à un rapport remis par Éric Debardieux, président de l'Observatoire International de la Violence à l'Ecole intitulé « Refuser l'oppression quotidienne : la prévention du harcèlement à l'Ecole », le ministère de l'éducation nationale, de la jeunesse et des sports a fait part d'un engagement pour les combattre : que ce soit dans les classes, les cours de récréation ou à travers les écrans. Dans ce rapport, le sociologue français préconisait de mener des campagnes pour promouvoir la lutte contre le cyberharcèlement, de contracter un accord avec Facebook pour que le réseau social ferme les comptes des harceleurs en cas de signalement de l'Education nationale et de former les mineurs à une utilisation positive des réseaux sociaux. Ainsi, dans la lutte contre le harcèlement en ligne sur les mineurs, le numéro vert national « Net Ecoute » a été mis en place afin de permettre une prise en charge des victimes. Les conversations sont 100% anonymes, gratuites et confidentielles. [79] De plus, le site internet www.netecoute.fr permet de demander des conseils en ligne ou bien de chater ou encore de contacter un conseiller par Skype. Le ministère de l'Education nationale a également réalisé la campagne « Stop harcèlement – agir contre le harcèlement » et depuis 2015, une journée de mobilisation a été instaurée dans les écoles. Désormais, le premier jeudi du mois de novembre est consacré à la journée nationale de la lutte contre le harcèlement. En complément de cette mobilisation de la part du ministère de l'éducation nationale, la CNIL ainsi que le CSA et des associations telles que « e-Enfance » ont pour mission de protéger les mineurs sur Internet.

Le législateur français a également pris conscience de la nécessité d'agir face à ce nouveau phénomène et est venu renforcer l'arsenal législatif. Ainsi, avec l'adoption de la loi du 7 octobre 2016[80] pour une république numérique, deux mesures sont venues renforcer la lutte contre le cyberharcèlement. D'une part, la création d'un droit à l'oubli numérique pour les mineurs

[78] P. Sirinelli et S. Prévost, « Réseaux… lument dangereux ! », Dalloz IP/IT, p.457
[79] Ministère de l'éducation nationale, de la jeunesse et des sports, « Prix « non au harcèlement » édition 2020 - https://www.education.gouv.fr/prix-non-au-harcelement-edition-2020-305092
[80] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique

permettant ainsi, au mineur victime de cyberharcèlement, d'obtenir l'effacement d'un contenu en ligne le concernant par une procédure accélérée. D'autre part, la création de l'article 226-2-1 du Code pénal[81] qui réprime notamment la pratique du revenge porn, c'est-à-dire rendre publique des images à caractère sexuel, sans le consentement de l'intéressé.[82] Puis, le législateur est également venu renforcer la lutte contre le cyberharcèlement avec une loi en date du 3 août 2018[83] qui vient réglementer l'usage du téléphone portable dans les établissements scolaires. Désormais, par principe, l'utilisation des téléphones portables est interdit dans les écoles et collèges. Toutefois, il est possible d'y déroger si le règlement intérieur de l'établissement scolaire autorise leur usage. De plus, afin de mieux répondre à cette problématique plusieurs rapports parlementaires ont été rendus. D'après le rapport parlementaire de la député Laetitia Avia[84], le droit répond en partie aux enjeux des propos haineux sur les réseaux sociaux, mais il y a un problème d'effectivité car deux obstacles ont été identifiés : « D'une part, la coopération entre les plateformes de communication en ligne et les autorités judiciaires est inefficace lorsqu'il s'agit de lever le principal obstacle à la poursuite des auteurs de contenus illicites : leur anonymat. (…) D'autre part, on ne peut que relever et regretter le faible nombre de plaintes déposées par les victimes de propos haineux sur Internet. ». En écho à ce rapport, le député a déposé une proposition de loi dont l'une des dispositions vise à mettre en place une meilleure collaboration entre la justice et les réseaux sociaux. La loi dite « Avia »[85] visant à lutter contre les contenus haineux sur Internet a été adoptée par le Parlement le 13 mai 2020. Or, la disposition phare, prévue à l'article 5 qui imposait aux réseaux sociaux de supprimer sous vingt-quatre heures les contenus haineux, a été censurée par le Conseil constitutionnel le 18 juin 2020[86]. En revanche, le conseil des Sages souligne le caractère louable du but de cette loi qui est de combattre la prolifération des propos haineux. De plus, la loi met tout de même en place un parquet spécialisé dans les messages de la haine en ligne et un observatoire de la haine en ligne rattaché au CSA. Enfin, l'un des gros problèmes du cyberharcèlement est l'anonymat des posts sur les réseaux sociaux ne permettant pas de déterminer l'auteur des propos. Pour y faire face, le droit français n'est pas assez armé et cette problématique occupe les débats politiques depuis plusieurs années. Si pour Jean Castex, premier ministre l'anonymat est « quelque chose de choquant » et « qu'il faudrait règlementer »[87] dans un entretien au journal Le Parisien, la question de la fin de l'anonymat divise la classe politique. Au delà de détruire la liberté qui ressort de l'anonymat, l'anonymat sur les réseaux sociaux est tout relatif. En effet, en cas d'enquête judiciaire, il est tout à fait possible d'identifier l'harceleur grâce aux

[81] Article 226-2-1 du C.pén. : « Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende. Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1. ».
[82] P. Le Maigat., « Revenge porn et cyberharcèlement. Schizophrénie ou déconnexion du juge pénal ? »,Gaz. Pal. 19 avr. 2016, n° 262j4, p. 12.
[83] Loi n°2018-698 du 3 août 2018 relative à l'encadrement de l'utilisation du téléphone portable dans les établissements d'enseignement scolaire
[84] Rapport visant à renforcer la lutte contre le racisme et l'antisémitisme sur internet, 21 septembre 2018, p.38
[85] Loi n°2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet
[86] Décision n°2020-801DC du 18 juin 2020 du Conseil Constitutionnel
[87] O. Beaumont, « Jean Castex face à nos lecteurs : « Il faut rétablir la confiance », Le Parisien, 15 juillet 2020

informations personnelles fournies telles que l'adresse mail, le numéro de téléphone ou l'adresse IP.

Le cyberharcèlement peut donc se faire à travers des pages web ou des mails, mais dans la majorité des cas, il a lieu sur les réseaux sociaux. En complément du droit, les réseaux sociaux prennent des initiatives pour lutter contre le cyberharcèlement. Aujourd'hui, une grande majorité d'entre eux disposent d'outils permettant le retrait, la suspension ou l'exclusion d'utilisateurs dès lors que des propos violents ou injurieux ont été tenus. Facebook, le plus célèbre réseau social pris conscience de l'ampleur de la problématique du cyberharcèlement. Lorsqu'une personne est victime d'insultes, elle a la possibilité de signaler l'harceleur. De plus, le réseau social a prévu, dans l'onglet « pages d'aides », une page reprenant différents conseils et consignes en cas de cyberharcèlement 88 et la possibilité d'accéder à une plateforme de prévention contre le harcèlement. 89 Cette manipulation est ouverte aussi bien aux personnes possédant ou non un compte. Pour celles qui disposent d'un compte, elles peuvent également signaler les commentaires ou photos comme « contenu abusif ». Quant à Twitter, considéré comme un haut lieu de liberté d'expression, il est souvent critiqué pour son inefficacité à trouver des solutions aux problèmes de cyberharcèlement. Crée en 2006, c'est seulement en 2020 que les ingénieurs de Twitter ont décidé de réagir à ce fléau. Une nouvelle option va permettre aux utilisateurs d'avoir le choix entre quatre configurations lorsqu'ils posteront un message. Ainsi, ils pourront choisir quels interlocuteurs sont autorisés à répondre à leurs messages. Cette nouvelle fonctionnalité fait aujourd'hui l'objet de tests. Elle n'est pas encore étendue à tous les utilisateurs. [90] Sur Instagram, la fonctionnalité permettant de laisser des commentaires sous des vidéos ou de photos partagés laisse, parfois, place à des propos malveillants. Face à cette problématique, la direction d'Instagram a réagi en mettant en place une nouvelle fonctionnalité afin d'essayer de protéger ses utilisateurs du traumatisme et de l'agression provoqué par certains commentaires. Cette fonctionnalité consiste à filtrer les commentaires non souhaités sur la base de mots-clés déterminés par l'utilisateur comme pouvant être traumatisants pour lui et donc indésirables. Enfin, avec SnapChat et son principe de durée limitée de visionnage d'une photo, les adolescents sont trop crédules sur le caractère éphémère de ces photos et se persuadent du risque zéro quant au partage et à la réutilisation de l'image qu'ils transmettent à leur contact. Cette croyance est très illusoire puisque l'éphémérité de leur photos et vidéos est très vite contournée par une simple capture d'écran qui pourra être diffusable à volonté. L'effet pervers de cette croyance les amène, parfois, à faire preuve de la plus grande inconscience par des partages très délurés et sans limite au prétexte qu'ils ne perdureront pas. Cela les affranchis de toute appréhension sur les effets de leur partage au motif que ceci disparaisse à court terme.

[88] Site Facebook : www.facebook.com/help/420576171311103/
[89] Site Facebook : *www.facebook.com/safety/bullying/*
[90] C. Follain, « Cyberharcèlement : Twitter va vous permettre de choisir qui a le droit de réagir à vos posts », LeMonde, 9 janvier 2020

Internet ne cesse donc jamais d'évoluer et les infractions qui s'y produisent se renouvellent tout autant ce qui rend difficile pour le législateur d'encadrer cet espace. Toutefois, il a rapidement réagi pour l'un des principaux dangers de la sphère numérique : le risque pour les mineurs d'y rencontrer des prédateurs sexuels. (Paragraphe 2)

Paragraphe 2 : Le grooming

La complexité de la notion de grooming est proportionnelle aux subterfuges mis en place par les prédateurs pour arriver à leurs fins. Le mode opérationnel très particulier du grooming a amené à créer une infraction spécifique pour sanctionner cette pratique qui s'avère être une étape préparatoire dans *l'iter criminis*. (A) La qualification et l'assimilation du grooming est complexe car cette pratique est souvent associée et à l'origine d'autres formes d'infractions plus lourdes. (B)

A) <u>La création d'une infraction propre pour un acte préparatoire</u>

Selon une récente étude, plus de la moitié des jeunes de 8 à 14 ans utilisent les réseaux sociaux. [91] Les jeunes s'y connectent grâce à leur smartphone, leur tablette ou même l'ordinateur familial, loin du regard de leurs parents. Il ressort que plus de 20% des jeunes de 11 à 13 ans échangent sur les messageries avec des personnes inconnues. Ce qui est d'autant plus inquiétant c'est que 15% d'entre eux reconnaissent s'être déjà retrouvés face à un adulte alors qu'ils pensaient discuter avec un enfant de leur âge. [92] Tout comme les enfants de moins de 15 ans passent outre les conditions générales d'utilisation pour la plupart des réseaux sociaux en déclarant un âge plus élevé lors de leur inscription, les adultes malintentionnés se créent facilement des profils qui n'ont rien à voir avec la personne qu'ils sont en réalité. Ainsi, toute personne peut dissimuler sa véritable identité derrière un « pseudo » sur Internet et certains adultes malveillants utilisent cette technique pour aborder des mineurs en ligne. L'essor de l'Internet et l'usage de plus en plus massif des réseaux sociaux a donc permis le développement de nouvelles formes de délinquance nécessitant l'adaptation de l'arsenal législatif. En effet, dans sa recommandation « Les Enfants du Net : pédopornographie et pédophilie sur l'Internet », rendue publique le 25 janvier 2005, le Forum des droits sur l'Internet souligne que le droit français ne prévoit pas « d'infraction décrivant spécifiquement le fait, pour un adulte, de rechercher les faveurs sexuelles de mineurs, en ligne ou hors ligne, ou le fait de rencontrer un mineur dans l'intention de commettre une atteinte ou une agression sexuelle ou un viol. ». Le Forum des droits sur l'Internet recommande donc la création

[91] Etude publiée par Statista Research Department le 29 mai 2019 interrogeant 1 506 personnes
[92] Etude Baromètre enfants et Internet publiée par Calysto en 2011

d'une nouvelle incrimination pénale afin de punir tout adulte qui émet des propositions à caractère sexuel envers un mineur ou cherche à rencontrer un mineur auquel il aurait adressé des propositions à caractère sexuel par le biais d'Internet. [93] L'idée de cette nouvelle incrimination est de combler l'absence de dispositions dans le droit français face à cette nouvelle pratique communément appelée « grooming » à l'international ou « pédopiégeage » en français. Le grooming est une dérive des réseaux sociaux car, selon l'agence anglaise National society for the prévention of cruelty to children Instgram, 70% des méthodologies de grooming impliquent l'utilisation d'un réseau social. D'après cette enquête, le réseaux social privilégié par les pédocriminels pour cette pratique serait Instagram (32% des cas), devant Facebook (23%) et Snapchat (14%). L'utilisation d'Instagram à des fins de grooming a connu une hausse de 200% entre 2017 et 2018. [94] Face à ces nouveaux comportements qui émanent des nouvelles technologies, le droit français et le droit international ont dû s'adapter.

En droit interne, la loi du 5 mars 2007 [95] relative à la prévention de la délinquance s'est préoccupée de la protection des mineurs, notamment, en créant l'article 227-22-1 du Code pénal afin d'incriminer toute proposition sexuelle faite à un mineur de 15 ans ou une personne se présentant comme telle, par un moyen de communication. [96] Concernant l'âge de 15 ans, au final, il importe peu : ce qu'il faut c'est que l'auteur des propositions les ai faites en pensant que la victime avait moins de 15 ans. Cet âge de 15 ans correspond à la majorité sexuelle en France. Au-delà de 15 ans, un mineur peut avoir des relations sexuelles avec un majeur, sauf s'il existe un lien d'ascendance ou d'autorité entre eux.[97] En dessous de cet âge, le mineur est considéré comme ne pouvant pas avoir de consentement éclairé ce qui justifie, pour cette infraction, que le législateur a retenu l'âge de 15 ans. L'incrimination du grooming met en lumière une double préoccupation contemporaine. [98] D'une part, la volonté de protéger les mineurs des dangers de ces nouveaux moyens de communication.[99] En effet, cet article vise les propositions sexuelles qui sont uniquement émises par un moyen de communication électronique. Par conséquent, les propositions faites hors ligne, dans le monde réel n'entrent pas dans le champ d'application. D'autre part, la volonté de prévenir des comportements pédophiles. Effectivement, l'élément matériel de cette infraction est la seule sollicitation du mineur de 15 ans par un majeur à des fins

[93] Recommandation du Forum des droits sur l'internet, « Les Enfants du Net (2): pédopornographie et pédophilie sur l'internet », 25 janvier 2005
[94] A. Renault, « Instagram, le réseau social favori des pédophiles », Slate, publié le 8 mars 2019
[95] Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance
[96] Article 227-22-1 du C.pén. : « Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
Ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre.
[97] Article 227-27 du C.pén. : « Les atteintes sexuelles sans violence, contrainte, menace ni surprise sur un mineur âgé de plus de quinze ans et non émancipé par le mariage sont punies de deux ans d'emprisonnement et de 30 000 euros d'amende : 1° Lorsqu'elles sont commises par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait ; 2° Lorsqu'elles sont commises par une personne qui abuse de l'autorité que lui confèrent ses fonctions. »
[98] AG. Robert, « Délit de proposition sexuelles faites à un mineur de quinze ans par un moyen de communication électronique (loi n°2007-297 du 5 mars 2007) », Dalloz RSC 2007 p.853, Chron.4
[99] V. A. Lepage, Les dispositions concernant la communication dans la loi du 5 mars 2007 relative à la prévention de la délinquance, Comm. com. élec. 2007, n° 6, Etude n° 13.

sexuelles sans attendre qu'il y ait un passage à l'acte. Ainsi, entre dans le champ d'application de cette infraction toute proposition d'acte à connotation sexuelle. Autrement dit, cet article punit, à titre autonome, un simple acte préparatoire.[100] Cette sanction de l'acte préparatoire interpelle car, en principe, il ne peut pas être sanctionné puisque l'auteur n'est pas entré dans la phase d'exécution et qu'il peut encore renoncer à son acte criminel. Or, ici, cette sanction se justifie par l'intérêt supérieur de protéger les mineurs face à des comportements pouvant conduire à une atteinte, c'est-à-dire à un commencement d'exécution. L'idée est donc de dissuader le groomer en permettant une incrimination le plus en amont possible dans *l'iter criminis*. Ainsi, cette nouvelle incrimination peut être perçue comme une tentative de l'infraction matérielle prévue à l'article 227-25 du Code pénal [101] qui sanctionne l'atteinte sexuelle sur un mineur de 15 ans, c'est-à-dire le fait pour une personne majeure d'avoir un comportement de type sexuel avec un mineur de 15 ans sans qu'il y ait eu de menace, contrainte ou violence. [102] De plus, dans un arrêt du 8 février 2017, la chambre criminelle a souligné que, si ces éléments ne sont pas réunis, il appartient aux juges de rechercher si ces faits ne relèvent pas plutôt de la qualification de propositions sexuelles d'un majeur à un mineur de 15 ans par un moyen de communication électronique, réprimée par l'article 227-22-1 du Code pénal. [103]

En droit international, le Conseil de l'Europe a réagi face aux dangers liés à l'utilisation des nouveaux moyens de communication par les mineurs. En effet, fortement engagé dans la lutte contre les violences envers les enfants, il a signé, le 25 octobre 2007, la Convention sur la protection des enfants contre l'exploitation et les abus sexuels. Cette Convention, également appelée « la Convention de Lanzarote », dispose que les Etats, en Europe et au-delà, doivent adopter des dispositions législatives spécifiques et prendre des mesures en vue de prévenir les abus sexuels contre les enfants, protéger les victimes et poursuivre les auteurs. La Convention de Lanzarote est donc entrée en vigueur le 1er juillet 2010 pour tous les Etats qui l'ont ratifié, la France en faisant partie. Ainsi, l'article 23 de la Convention [104] prévoit que « chaque partie prend les mesures législatives ou autres nécessaires pour ériger en infraction pénale le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant n'ayant pas atteint l'âge fixé en application de l'article 18, paragraphe 2, dans le but de commettre à son encontre une infraction établie conformément aux articles 18, paragraphe 1.a, ou 20, paragraphe 1.a, lorsque cette proposition a été´ suivie d'actes matériels conduisant à ladite rencontre. ». Autrement dit, la Convention de Lanzarote prévoit l'introduction d'une nouvelle infraction qui n'apparaît pas dans les autres instruments internationaux existant

[100] CONTE, « La loi sur la prévention de la délinquance : présentation des dispositions de droit pénal », Dr. pénal 2007. Chron. 9
[101] Article 227-25 du C.pén.: « Hors le cas de viol ou de toute autre agression sexuelle, le fait, par un majeur, d'exercer une atteinte sexuelle sur un mineur de quinze ans est puni de sept ans d'emprisonnement et de 100 000 € d'amende. »
[102] AG. Robert, *Op.cit*
[103] CCass. Crim. 8 février 2017, n°16-80102
[104] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée le 25 octobre 2007

dans ce domaine : le grooming. Afin d'aider les Etats à lutter contre le grooming, le Comité de Lanzarote a adopté le 17 juin 2015 un avis portant sur l'article 23 de la Convention accompagné d'une note explicative dans laquelle il donne des indications utiles pour incriminer cette pratique. Enfin, le dernier instrument international est la directive du Parlement et du Conseil de l'Union européenne relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie entrée en vigueur le 17 décembre 2011. [105]Elle reprend les grandes lignes de la Convention de Lanzarote et vient faire appliquer ce texte à tous les membres de l'Union européenne en exigeant l'adoption de mesures préventives et de dispositions législatives, administratives et judiciaires dans un délai de 2 ans. En ce qui concerne le grooming, le législateur européen souligne que : « *La sollicitation d'enfants à des fins sexuelles est une menace aux caractéristiques particulières dans le cadre de l'Internet, car ce dernier procure aux utilisateurs un anonymat sans précédent qui leur permet de masquer leur identité réelle et leurs caractéristiques personnelles telles que leur âge*. »[106] De plus, l'article 6 de la directive européenne prévoit la création spécifique d'une infraction pour cette pratique par tous les Etats membres. [107]

Pour conclure, il en ressort que les instruments internationaux ne sont pas venus chambouler la protection des mineurs en France face au grooming puisque la sanction de cette délinquance a été anticipée en droit interne avec la création de l'article 227-22-1 du Code pénal par la loi du 5 mars 2007. Or, contrairement au droit interne, selon la Convention de Lanzarote et la directive européenne, la responsabilité pénale de l'auteur des propositions peut être engagée uniquement si ces dernières ont été suivies d'actes matériels conduisant à une rencontre. Le législateur français n'en a pas fait une condition essentielle à la qualification de l'infraction. Toutefois, selon l'article 227-22-1 du Code pénal punit les simples propositions sexuelles de 2 ans d'emprisonnement et 30 000€ d'amende. Cette sanction s'explique par le fait que les abus sexuels en ligne, même s'ils n'aboutissent pas systématiquement à une rencontre physique, peuvent être très traumatisants pour les enfants. En revanche, dès lors qu'il y a une rencontre, le législateur français est plus sévère car ces peines sont portées à 5 ans d'emprisonnement et 75 000€ d'amende. Ainsi, le comportement fallacieux du groomer doit être alarmant car ce dernier peut avoir, par la suite, l'intention de commettre, d'autres infractions encore plus dangereuses. (B)

[105] Directive n° 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie venant remplacer la décision-cadre 2004/68/JAI du Conseil

[106] Considérant n°19 de la Directive n° 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011

[107] Article 6 alinéa 1 de la Directive n° 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 : « Les États membres prennent les mesures nécessaires pour que les comportements intentionnels suivants soient punissables: le fait pour un adulte de proposer, au moyen des technologies de l'information et de la communication, une rencontre à un enfant qui n'a pas atteint la majorité sexuelle, dans le but de commettre l'une des infractions visées à l'article 3, paragraphe 4, et à l'article 5, paragraphe 6, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre, est passible d'une peine maximale d'au moins un an d'emprisonnement.

B) Les préliminaires à la commission d'infractions plus graves

Considéré comme une infraction propre en droit français, le grooming a la particularité d'être avant tout un acte préparatoire à la commission d'une infraction plus grave. Dès lors qu'un mineur a été pris dans les filets d'un groomer, plusieurs dangers le guettent. La cour d'appel de Colmar a rendu un arrêt en date du 29 mai 2012[108] qui illustre parfaitement les étapes du grooming et les dangers qui peuvent en découler. Elle y sanctionne toutes les dérives qui en découlent et à quel point il a un effet boule de neige dévastateur. Dans cette affaire, un homme âgé de 31 ans s'était créé un faux profil Facebook se faisant passer pour une jeune fille d'une quinzaine d'années se disant bisexuelle afin d'entrer en contact avec des jeunes collégiennes. Pour choisir sa victime, ce dernier étudiait les informations figurant sur le profil de jeunes adolescentes avant de leur envoyer une invitation à partir de son faux profil. Une fois le contact établi, toujours en se faisant passer pour une mineure de 15 ans, il demandait à ses interlocutrices de brancher leur webcam et orientait la conversation vers des tendances sexuelles. Ensuite, il proposait de se déshabiller à la condition qu'elles fassent de même. Pour cela, il leur diffusait la vidéo d'une adolescente qu'il avait préalablement piégée et dont il avait obtenu une vidéo où elle se dénudait. Puis, il leur demandait de s'introduire des objets dans le sexe. En cas de refus, il contraignait ces jeunes victimes en usant du chantage ou de la menace de divulguer les éléments qu'il avait collectés les concernant. Toutes ses victimes étaient enregistrées à leur insu grâce à un logiciel qui permettait de capturer les vidéos. Le prévenu a été reconnu coupable en première instance et par la cour d'appel de Colmar de propositions sexuelles faites à un mineur de 15 ans par un majeur utilisant un moyen de communication électronique, de corruption de mineur, de captation d'images à caractère pornographique en vue de leur diffusion et de détention de l'image d'un mineur présentant un caractère pornographique.

Le grooming est donc un processus de préparation permettant à une personne d'adopter un comportement de prédateur afin de gagner la confiance d'un mineur de 15 ans dans le but de l'exploiter à des fins sexuelles. Cet arrêt illustre parfaitement les différentes étapes que le délinquant déploie dans son modus operandi. Pour ce faire, le groomer prend contact avec le mineur, la plupart du temps à travers les différents réseaux sociaux, afin d'évaluer sa vulnérabilité. Ensuite, le prédateur essaie de gagner la confiance de la victime en employant des techniques comme le partage de sentiments ou de secrets. Dès lors que la confiance est établie, l'agresseur essaie de profiter sexuellement de la relation en faisant des propositions sexuelles au mineur. Une fois que ce nouveau type d'abus sexuel se produit, l'agresseur utilise la menace et le chantage pour maintenir la participation et le silence de l'enfant. Au vu des faits de cette affaire, l'infraction de

[108] CA. Colmar, 29 mai 2012, n°12/00737 : Gaz. Pal. 2012.2.2701, note Lasserre Capdeville

propositions sexuelles à un mineur de 15 ans par la biais d'un moyen de communication électronique est caractérisée. De plus, le comportement adopté par cet homme témoigne bien de ce modus operandi. Toutefois, si le grooming n'est pas toujours facile à caractériser, dans cet arrêt la qualification de propositions sexuelles à un mineur de 15 ans par la biais d'une communication électronique a bien été retenue et de ces dernières ont découlé des infractions plus graves.

La frontière entre la qualification de propositions sexuelles à un mineur de 15 ans par communication électronique et de corruption d'un mineur de 15 ans est très sensible et ne tient qu'à la volonté, pour le délinquant, d'éveiller chez le mineur des pulsions sexuelles. Si l'article 227-22 du Code pénal[109] ne définit pas la corruption de mineur, l'article 334-3 de l'ancien Code pénal précisait qu'il s'agissait « d'incitation de mineur à la débauche ». Or, les éléments constitutifs de l'infraction ont été repris pour cette nouvelle qualification de corruption de mineur. [110] L'acte incriminé est donc défini seulement par son but, c'est-à-dire la corruption d'un mineur. [111] Ainsi, entre dans le champ d'application de ce texte le fait de faire accomplir des actes sexuels ou obscènes par le mineur,[112] ou bien de les accomplir sur lui ou devant lui[113]. Ici, en plus des propositions sexuelles, il est indéniable qu'il y a eu une volonté de la part du délinquant d'exciter ces mineures en leur diffusant des vidéos dans lesquelles une jeune fille (à laquelle il avait usurpé l'image) accomplissait des actes à connotation sexuelle. L'infraction de corruption de mineur est donc bien caractérisée et découle des propositions sexuelles faites par le prévenu. De plus, cette affaire témoigne que le grooming peut être caractérisé en même temps que la corruption de mineur.

Dans la majorité des cas de grooming, le délinquant cherche à obtenir des photos ou vidéos du mineur nu. D'ailleurs, la cour d'appel d'Aix-en-Provence a retenu l'application de l'article 227-22-1 du Code pénal envers un homme qui, après de nombreux échanges sur un forum de discussion, a demandé à une petite fille de 10 ans de se dénuder devant sa webcam et de se livrer à des gestes obscènes. [114] Mais il peut découler de ce nouveau délit d'autres délits plus graves tels que la détention d'image d'un mineur présentant un caractère pornographique ou la captation d'image à caractère pornographique d'un mineur en vue de sa diffusion comme le démontre l'affaire jugée par le cour d'appel de Colmar. L'article 227-23 du Code pénal punit distinctement la détention d'une image à caractère pornographique de la transmission et la captation d'une telle

[109] Article 227-22 du C.pén. : « Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communications électroniques (…) »

[110] M.-L. Rassat, « Fait de favoriser la corruption d'un mineur » : J.-Cl. pén., art. 227-22, fasc 20, 2008

[111] J. Lasserre Capdeville, « Infraction commises à l'encontre de mineurs par l'intermédiaire d'Internet », Gaz. Pal. 6 sept. 2012, n°GP20120906009, p.12

[112] CCass. Crim. 1er février 1995, n°93-82578, Bull. crim., n°43

[113] CCass. Crim. 11 septembre 2007, n°07-82018

[114] CA. Aix-en-Provence, 26 oct. 2011, Juris-Data n°032852

image.

Le délit de transmettre ou d'enregistrer une image à caractère pornographique d'un mineur est sanctionné à l'alinéa 1 de l'article 227-23 du Code pénal.[115] Cette infraction nécessite donc l'existence d'une image d'un mineur ayant un caractère pornographique et la fixation, l'enregistrement ou la transmission de cette dernière en vue de sa diffusion. De plus, il s'agit d'une infraction intentionnelle donc l'auteur devait avoir conscience de l'enregistrement ou la captation de l'image et du but de cet acte, c'est-à-dire la diffusion de l'image.

Quant au délit de détention d'une telle image , il est réprimé à l'alinéa 5 du même article.[116] Pour que l'infraction soit caractérisée il faut un acte de détention, peu importe que le support soit matériel ou dématérialisé et l'intention de l'auteur de les garder à sa disposition en connaissant le contenu des images.

Si dans un premier temps le contact avec l'enfant commence en ligne, cela peut donner lieu par la suite à une rencontre qui peut avoir des conséquences dramatiques et entrainer la commission d'infractions plus graves que le grooming. En effet, le délinquant peut chercher à rencontrer le mineur et avoir, de force, des relations sexuelles. Le législateur a pris soin de définir légalement l'infraction de viol à l'article 222-23 du Code pénal[117] comme étant : « tout acte de pénétration sexuelle, de quelque nature qu'il soit, commis sur la personne d'autrui ou sur la personne de l'auteur par violence, contrainte, menace ou surprise est un viol ». Le viol est un crime puni de 15 ans de réclusion criminelle et la peine est portée à 20 ans si la victime est un mineur de 15 ans[118] ou lorsque la victime a été mise en contact avec l'auteur des faits par un moyen de communication électronique.[119] En matière de viol, l'existence de l'élément moral est exigé : c'est une infraction intentionnelle qui nécessite la volonté d'accomplir l'acte de pénétration et que l'auteur ait conscience que sa victime n'est pas consentante. Concernant l'acte de pénétration, c'est l'élément qui va permettre de distinguer le viol de toutes les autres infractions sexuelles. Il doit être accompli sur la personne d'autrui et depuis la loi du 3 aout 2018[120] entre dans le champ d'application de cet article la pénétration commise sur la personne de l'auteur. Auparavant, le viol pouvait être qualifié uniquement en cas de pénétration de l'auteur sur la personne de la victime. Autrement dit, dès que la pénétration était imposée à celui qui la subissait, il s'agissait d'un viol, en revanche, lorsqu'elle était imposée à celui qui la pratiquait, il s'agissait d'une agression

[115] Article 227-23 al1 du C.pén. : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende. »

[116] Article 227-23 al5 du C.pén. : « le fait de (…) de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende. »

[117] Article 222-23 du C.pén. : « Tout acte de pénétration sexuelle, de quelque nature qu'il soit, commis sur la personne d'autrui par violence, contrainte, menace ou surprise est un viol. Le viol est puni de quinze ans de réclusion criminelle ».

[118] Article 222-24, 2° du C.pén. : « Le viol est puni de vingt ans de réclusion criminelle : (....) lorsqu'il est commis sur un mineur de quinze ans (…) »

[119] Article 222-24, 8° du C.pén. : « Le viol est puni de vingt ans de réclusion criminelle : (....) lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique »

[120] Loi du 3 août 2018 n°2018-703 renforçant la lutte contre les violences sexuelles et sexistes

sexuelle. De ce fait, une femme qui forçait un homme ou un homme qui forçait un autre homme à procéder à un acte de pénétration ne pouvait pas être condamné pour viol car seul l'auteur était pénétré. Désormais, ce n'est plus le cas et tout type de pénétration sexuelle volontairement imposée entre dans le champ d'application de l'article 222-23 du Code pénal. Toutefois, l'acte doit être de nature sexuelle, c'est-à-dire par un organe sexuel ou dans un organe sexuel. Concernant la violence, la contrainte, la menace ou la surprise, cela permet de caractériser l'absence de consentement de la victime qui pèse sur la qualification des faits et sur l'intention de l'auteur. Or, si le législateur ne le dit pas expressément, il ressort de l'élément matériel, c'est-à-dire de l'acte de pénétration sexuelle, la nécessité d'un contact entre l'auteur et la victime pour que le viol soit qualifié. Par conséquent, il faut une rencontre.

Cependant, le tribunal correctionnel de Bruxelles a rendu, le 25 septembre 2018, une décision novatrice dans laquelle il a retenu la qualification de viol en l'absence de contacts physiques. [121] Les faits étaient les suivants : un homme de 25 ans a harcelé sur les réseaux sociaux, pendant 5 ans, des jeunes filles âgées de 13 à 16 ans. Il leur demandait de se déshabiller devant leur webcam, de s'adonner à des pratiques sexuelles et de lui envoyer des photographies. En cas de refus, il les menaçait de diffuser des images d'elles, dénudées. Lors d'une conversation vidéo avec une jeune fille de 15 ans, il va plus loin et la force à effectuer une auto-pénétration sexuelle face à lui sous la menace de diffuser des images compromettantes qu'il avait en sa possession. Pour la juridiction belge, il s'agit d'un viol même s'il n'y a eu aucun contact physique entre la victime et son agresseur. Cette condamnation est une première en Belgique et tend à s'interroger sur les capacités du droit pénal français à appréhender le « viol à distance » ou « cyber-viol ». [122] L'article 375 du Code pénal belge définit le viol comme « tout acte de pénétration sexuelle, de quelque nature qu'il soit et par quelque moyen que ce soit, commis sur une personne qui n'y consent pas ». Contrairement au législateur français, le législateur belge ne précise pas que l'acte de pénétration doit être du fait de l'auteur. Ainsi, les juges belges ont une large marge d'appréciation du texte, ce qui leur a permis de considérer que l'élément matériel du viol était bien constitué par la contrainte et la menace qui a conduit à l'auto-pénétration. De plus, en reconnaissant ce « viol à distance », les magistrats belges mettent de côté le critère de contact physique entre l'auteur et la victime pour caractériser l'infraction.

En parallèle, en droit pénal français, l'auto-pénétration ne rentrerait pas dans le champ d'application de l'actuel article 222-23 du Code pénal qui exige expressément la pénétration de la victime par l'auteur ou la pénétration de l'auteur par la victime. En revanche, issu de la loi du 5 août 2013[123], l'article 222-22-2 du Code pénal dispose : « Constitue également une agression sexuelle le fait de contraindre une personne par la violence, la menace ou la surprise à subir une

[121] J-C Planque, « La répression du « cyber-viol » : simple adaptation ou prémices d'une révolution des concepts pénaux ? », Droit pénal n°2, Février 2019
[122] *Ibid*
[123] Loi n°2013-711 du 5 août 2013 portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France

atteinte sexuelle de la part d'un tiers". D'après une interprétation du texte, cette infraction autonome consiste à commettre les actes qui vont contraindre la victime à subir une atteinte sexuelle. De plus, le tiers en question dans la formule « (…) subir une atteinte sexuelle de la part d'un tiers » pourrait être interprété comme étant une autre personne que celle qui a fait l'usage de la violence, menace ou surprise pour contraindre la victime. Autrement dit, ce tiers peut être la victime elle-même qui s'inflige une atteinte sexuelle. Concernant la sanction de cette infraction, l'article précise que : « [...] peines prévues aux articles 222-23 à 222-30 selon la nature de l'atteinte subie et selon les circonstances mentionnées à ces mêmes articles [...] ». Ainsi, pour un acte d'auto-pénétration non consenti, les peines applicables sont celles du viol et les circonstances aggravantes sont identiques à celle d'un viol. Donc, selon le droit pénal français, pour de tels faits, la qualification de viol ne pourrait pas être retenue. Toutefois, l'application de l'article 222-22-2 du Code pénal permet d'avoir une réponse répressive satisfaisante puisqu'elle serait identique à celle d'un viol.

La position novatrice de la juridiction belge envoie un signal fort et peut être perçue comme une réelle prise de conscience du monde de la justice de l'évolution de la cybercriminalité liée à l'utilisation de plus en plus fréquente des réseaux sociaux pour communiquer. Le développement des nouvelles technologies, s'il ne l'est déjà, risque d'être à l'origine de changements importants en matière pénale. L'introduction de nouvelles infractions ou les évolutions procédurales connues jusqu'à ce jour ne suffiront plus et il faudra sans doute repenser un grand nombre des concepts pénaux. [124] Ce n'est pas parce qu'il s'agit d'informatique que le préjudice doit être considéré comme virtuel.

Le mineur n'est donc pas dépourvu de protection dans son usage des réseaux sociaux. En encadrant à la fois le cyberharcèlement et le grooming, le législateur a adapté les infractions pénales à la cybercriminalité dans l'idée de sécuriser la pratique par les mineurs des outils d'Internet. Ses droits fondamentaux sont également respectés à travers l'exercice du droit à la liberté d'expression mais également par la protection récente de ses données personnelles dans le cadre de son droit à la vie privée et la protection ancestrale du droit à l'image contrôlé par les titulaires de l'autorité parentale. Cependant, inachevée, son périmètre de sécurité reste limité et présente encore de nombreux manquements pour le préserver totalement. Le chemin pour y parvenir est encore bien long. (Chapitre 2)

[124] J-C Planque, « La répression du « cyber-viol » : simple adaptation ou prémices d'une révolution des concepts pénaux ? », Droit pénal n°2, Février 2019, Etude 4

CHAPITRE II : La protection limitée du mineur sur les réseaux sociaux

Le monde juridique se doit de s'adapter au monde virtuel qui évolue et qui prend une place de plus en plus importante dans la vie de chacun, en particulier dans celle des mineurs. Ces derniers constituent une cible privilégiée car ils sont des usagers de plus en plus précoces et intenses des réseaux sociaux. Face aux dangers de ces nouveaux outils de communication, leur protection est en cours de construction et loin d'être aboutie. D'une part, malgré sa volonté de se soucier de la protection du mineur, le législateur a des difficultés à la rendre totalement efficace. En créant et instaurant la majorité numérique, il avait pour objectif de préserver la sécurité des mineurs en venant restreindre l'accès autonome des mineurs aux différents services d'Internet. Toutefois, avec du recul, il ressort que sa mise en place n'est pas une réponse adaptée aux nombreux dangers que soulèvent les pratiques numériques des plus jeunes. (Section 1) D'autre part, nombreux sont les parents qui n'ont pas conscience des enjeux d'une exposition de leur enfant sur les réseaux sociaux, que ce soit de leur initiative ou de celle du mineur. Cette exposition, parfois excessive, entraine des conséquences non-négligeables quant à la sécurité du mineur, son développement et son avenir. Un travail doit être fait pour qu'il y ait une prise de conscience et un encadrement de cette surexposition. (Section 2)

Section 1 : La majorité numérique : une protection hypocrite du mineur

Depuis leur création, les réseaux sociaux ont constamment évolué, connaissant un succès exponentiel. Leur succès est tel qu'aujourd'hui ils font partie intégrante de la vie quotidienne d'une grande majorité de citoyens, y compris pour les plus jeunes. D'ailleurs, si la vie des jeunes sur les réseaux sociaux est devenue une extension naturelle de leur vie sociale, ils ne sont pas toujours conscients de la face cachée de l'iceberg. Face aux côtés néfastes de ces plateformes a et à la vulnérabilité des mineurs, de nombreux questionnements sont apparus quant à leur utilisation pour les mineurs : faut-il leur interdire ? Ou est-il préférable de superviser leur utilisation ? Désormais trop encrés dans la société et devenu vital pour les plus jeunes, il était donc inconcevable de leur interdire l'utilisation. En revanche, le législateur a décidé de venir les accompagner dans cette

utilisation en instaurant une majorité numérique. D'un point de vu théorique, la majorité numérique est venue apporter une protection essentielle au mineur. (Paragraphe 1) D'un point de vue technique, elle est perçue comme une fausse promesse de protection du mineur. (Paragraphe 2)

Paragraphe 1 : L'apparence protectrice de la majorité numérique

La majorité est le statut juridique que la loi attache à une personne qui est en âge d'exercer seule ses droits et libertés car elle est reconnue pleinement capable et responsable. En droit français, il existe plusieurs types de majorités avec des seuils d'âges différents. En réponse à l'évolution ainsi qu'à l'utilisation grandissante des nouvelles technologies, le droit s'est adapté et est venu créer une majorité numérique. (A) Dans le cas d'une inscription sur un réseau social, cette majorité numérique vient se substituer à la limite d'âge prévue par la plateforme. (B)

A) La notion de majorité numérique

En matière civile, la majorité civile a fait l'objet de plusieurs réformes. Si sous l'Ancien régime elle était fixée à 30 ans pour les hommes et 25 ans pour les femmes, en 1792 elle est abaissée à 21 ans pour les deux sexes. Mais, depuis la loi du 5 juillet 1974, elle est fixée à l'article 414 du Code civil qui dispose que : « la majorité est fixée à dix-huit ans accomplis ; à cet âge, chacun est capable d'exercer les droits dont il a la jouissance ». La majorité civile est donc l'âge fixé par la loi pour user de ses droits civils ou politiques et à partir duquel une personne est considérée comme juridiquement capable et responsable. Ainsi, fixée à 18 ans pour les hommes et pour les femmes, la majorité confère, en droit civil, la capacité juridique. A partir de cet âge, il est donc possible de s'engager et de passer un contrat selon le droit des contrats comme le prévoit l'article 1145 du Code civil[125].

En matière pénale, la majorité pénale doit est l'âge à partir duquel un individu est soumis au droit commun de la responsabilité pénale et ne bénéficie plus de l'excuse atténuante de minorité, c'est-à-dire d'un adoucissement de peine. Elle est fixée à 18 ans. Quant à la majorité sexuelle, elle a été définie par le Conseil Constitutionnel le 17 février 2012[126] en réponse d'une question prioritaire de constitutionnalité envoyée par la chambre criminelle de la Cour de cassation. Ainsi, le Conseil Constitutionnel considère que la majorité sexuelle correspond à « l'âge à partir duquel un mineur peut valablement consentir à des relations sexuelles (avec ou sans pénétration) avec une

[125] Article 1145 al1 du C.Civ. : « Toute personne physique peut contracter sauf en cas d'incapacité prévue par la loi. »
[126] Décision n°2011-222 QPC du 17 février 2012 du Conseil Constitutionnel

personne majeure à condition que cette dernière ne soit pas en position d'autorité à l'égard du mineur ». Elle est fixée à 15 ans par l'article 227-25 du Code pénal[127] qui sanctionne l'atteinte sexuelle sur mineur.

En matière numérique, la majorité numérique est une notion apparue que très récemment en droit français. Le consentement exprimé par les mineurs concernant le traitement des données à caractère personnel est difficile à appréhender. Lorsque le mineur utilise les réseaux sociaux, il manifeste sa volonté et exprime donc un consentement au sens du droit des contrats.[128] Or, est-ce qu'un mineur peut consentir en ligne ? Peut-il passer un contrat en ligne ? Si, d'après l'ancien article 389-3 du Code civil[129] et le nouvel 1149 du Code civil[130], un mineur peut passer seul des actes de la vie courante, c'est-à-dire qui ne feraient courir aucun risque, la Commission des clauses abusives a souligné que l'ouverture d'un compte sur les réseaux sociaux par un mineur n'entre pas dans la catégorie des actes de la vie courante[131]. Cette position s'explique par le fait qu'en concluant les contrats, ils acceptent les conditions générales d'utilisation et le traitement de leurs données à caractère personnel. Or, selon une enquête de la CNIL et de Génération numérique, seulement 41% des jeunes âgés de 11 à 14 ans savent que les réseaux sociaux peuvent utiliser les contenus qu'ils publient.[132] Face à l'ampleur du partage et de la collecte des données qui augmentent de manière exponentielle, la protection des données à caractère personnel a créé de nouveaux défis. A fortiori du fait que les individus publient de plus en plus et de plus en plus jeune.

La Commission Européenne a donc décidé de remettre de l'ordre, dans le cadre du « Paquet européen de protection des données », notamment avec de nouvelles règles applicables aux responsables de traitement des données personnelles. L'idée est de mieux protéger les plus jeunes contre l'exploitation de leurs données et de les accompagner dans leur apprentissage de l'univers numérique et des réseaux sociaux. En outre, le RGPD adopté le 27 avril 2016 détermine à l'article 8 [133] des conditions particulières concernant le consentement du mineur dans le cadre du traitement de données, par des services de sociétés de l'information, fondé sur le consentement. Par exemple, les réseaux sociaux. Ainsi, il fixe par défaut la majorité numérique à 16 ans mais impose aux Etats membres, à partir de son entrée en vigueur le 25 mai 2018, la mise en place d'un âge minimum compris entre 13 et 16 ans pour qu'un mineur puisse consentir seul à l'inscription d'un réseau

[127] Article 227-25 du C.pén. : « Hors le cas de viol ou de toute autre agression sexuelle, le fait, par un majeur, d'exercer une atteinte sexuelle sur un mineur de quinze ans est puni de sept ans d'emprisonnement et de 100 000 € d'amende. »
[128] B. Charrier, « Le consentement exprimé par les mineurs en ligne », Dalloz IP/IT 2018 p.333
[129] Ancien article 389-3 al 1 du C.civ. : « L 'administrateur légal représentera le mineur dans tous les actes civils, sauf les cas dans lesquels la loi ou l'usage autorise les mineurs à agir eux-mêmes. »
[130] Article 1149 al1 du C.Civ : « Les actes courants accomplis par le mineur peuvent être annulés pour simple lésion. Toutefois, la nullité n'est pas encourue lorsque la lésion résulte d'un événement imprévisible. »
[131] Recommandation de la Commission des clauses abusives n°2014-02, 7 novembre 2014, relative aux contrats proposés par les fournisseurs de services de réseaux sociaux
[132] Enquête CNIL – Délibération n°2017-299 du 30 novembre 2017 portant avis sur un projet d'adaptation au droit de l'Union européenne de la loi n°78-17 de janvier 1978 (demande d'avis n°170233753)
[133] Article 8 du RGPD : « Le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans. »

social. A ce titre, en France, la loi du 20 juin 2018[134] relative à la protection des données personnelles est venue réviser et adapter la loi Informatique et Libertés du 6 janvier 1978 en fixant ce seuil à 15 ans.[135] Cette réforme est une évolution notable car, jusqu'ici, la majorité numérique n'était pas déterminée et définie dans la loi française et l'âge minimum pour accéder aux plateformes en ligne était librement défini par ces dernières sans qu'aucune vérification ne puisse être faite. De plus, elle renforce cette protection en prévoyant également que « le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne. ».

Les Etats Unis avaient déjà traité le problème de la collecte des données à caractère personnel des mineurs à travers le Children's Online Privacy Protection Acte (COPPA) en date du 21 octobre 1998, entré en vigueur le 21 avril 2000. Le Federal Trade Commission (FTC) en charge de l'application du texte et à l'origine du Children's Online Privay Protection Rule précise les contours de cette loi. Le COPPA a donc fixé à 13 ans l'âge à partir duquel un mineur peut agir seul et donner son consentement sans l'autorisation de ses représentants légaux à la collecte de ses données personnelles.

La majorité numérique correspond donc à l'âge auquel la loi considère un mineur comme propriétaire de ses données personnelles. Par conséquent, il peut consentir seul à un traitement de ses données à caractère personnel sans l'aval de ses représentants légaux. Il est donc en mesure d'accepter ou non que des services tiers aient accès à ses données pour les collecter à des fins commerciales. Ici, tous les services qui collectent des données personnelles telles que le nom, prénom, date de naissance et bien d'autres sont concernés. [136] La majorité numérique est donc l'âge légal à partir duquel un mineur peut, par exemple, ouvrir un compte sur un réseau social sans avoir besoin du consentement des titulaires de l'autorité parentale. En dessous de cet âge, le responsable de traitement devra recueillir un double consentement : celui du mineur et celui de la personne exerçant l'autorité parentale. Le but n'est donc pas d'interdire l'accès aux réseaux sociaux mais d'encadrer l'utilisation pour que les jeunes l'utilisent de façon responsable et intelligente. A coté de cette limite d'âge posée par la majorité numérique, de part la nationalité juridique des réseaux sociaux qui sont, pour leur plus grand nombre, d'origines américaine, la première limite d'âge qui s'impose à tout mineur qui s'inscrit est de 13 ans. Le mineur doit donc faire face à une double limite d'âge pour son inscription sur un réseau social. (B)

[134] Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles

[135] Article 20 de la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles *: «* En application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans. »

[136] P.Verge, « Qu'est-ce que la majorité numérique fixée à 15 ans en France ? », Lefigaro, 9 février 2018

B) Une double limite d'âge pour l'inscription du mineur sur un réseau social

Afin de protéger au mieux les mineurs dans l'utilisation qu'ils font des réseaux sociaux, un âge minimum d'inscription a été instauré. Les plus utilisés par les jeunes tels que Facebook, Instagram, Snapchat ou Twitter n'ouvrent leurs portes virtuelles qu'aux enfants âgés de plus de 13 ans. Cet âge minimal correspond à la règle 3-6-9-12[137] : le moins d'écrans possible avant 3 ans, pas de console personnelle avant 6 ans, un accès à Internet accompagné d'un adulte à partir de 9 ans et un accès seul à Internet à partir de 12 ans. Cet âge minimum de 13 ans, requis pour l'inscription sur un réseau social, trouve son origine dans les dispositions américaines établies au travers du COPPA qui a précédé de presque de deux décennies la mise en place du RGPD. En théorie, le COPPA ne s'applique qu'aux enfants de nationalité américaine. Dès lors, lorsqu'un responsable de traitement s'adresse à un mineur de nationalité américaine, peu importe où il se situe dans le monde, il devra respecter cette loi. Toutefois, la FTC précise que les fournisseurs de services en ligne basés aux Etats-Unis doivent également se soumettre à la loi, même s'ils collectent les données personnelles d'enfants étrangers. Au regard du nombre de réseaux sociaux présents sur le sol américain et du nombre d'utilisateurs provenant du monde entier, notamment de la France, le COPPA a un impact international. La Californie, plus particulièrement via la Silicon Valley, s'est révélée devenir une véritable pépinière à réseaux sociaux. Facebook, Instagram, Snapchat ou encore Twitter y ont vu le jour. C'est donc sous l'encadrement du droit américain que ces sociétés ont établi leurs conditions d'utilisation. La règle de l'âge minimum est donc très majoritairement fixé à 13 ans par alignement sur le COPPA. Ce texte a donc initié la protection des mineurs français utilisateurs de réseaux sociaux avant l'entrée en vigueur du RGPD et de la loi 20 juin 2018 relative à la protection des données personnelles. Cependant, tout droit national établissant sa majorité numérique à un âge supérieur à 13 ans voit sa limite d'âge se substituer à celle-ci.

Suite à l'adoption du RGPD, le législateur français a pris conscience que, très majoritairement, les enfants étaient inscrits sur des réseaux sociaux sans pour autant avoir une maturité leur permettant de comprendre les tenants et les aboutissants de leur inscription. C'est pour cette raison que la loi du 20 juin 2018 relative à la protection des données personnelles est venue fixer, suite à un large consensus né lors des débats menés devant la Commission des lois de l'Assemblée, le seuil de la majorité numérique à 15 ans tandis que la version initiale du projet de loi prévoyait de la fixer à 16 ans. En effet, le projet de loi relatif à la protection des données personnelles avait décidé de conserver l'âge de 16 ans, âge de la majorité numérique fixée par défaut par le RGPD. Cependant, une opposition est apparue entre la position du Sénat et celle de l'Assemblée Nationale.

[137] Règle créée par le psychiatre Serge Tisseron et relayée par l'Association Française de Pédiatrie Ambulatoire

Aux yeux des sénateurs, il était préférable de maintenir ce seuil de 16 ans au motif que de le baisser ferait des mineurs des cibles privilégiées de ces éditeurs de services manipulant les données personnelles. Tandis que pour les députés, le seuil de 15 ans est plus adapté au motif que le mineur est en âge d'entrer au lycée et dispose du discernement nécessaire pour appréhender l'univers numérique le rendant apte à s'inscrire sur un service qui collecte ses données personnelles sans l'autorisation du titulaire de l'autorité parentale.[138] Autrement dit, cet âge de 15 ans correspondrait à l'acquisition d'une maturité suffisante pour prendre conscience des enjeux et des risques liés à la communication en ligne des données à caractère personnel. [139] Toutefois, pour certains parlementaires il fallait oser fixer ce seuil à 13 ans car il devait être cohérent avec la pratique des adolescents sur Internet car ils n'attendent pas d'avoir 15 ans pour être inscrits sur un réseau social. Cependant, il semble douteux qu'un mineur de 13 ans ait la capacité de saisir les conséquences du traitement et de la collecte des données personnelles. En effet, le consentement repose sur la politique de confidentialité, qui la plupart du temps, est incomprise ou non lue par les majeurs : ce qui laisse penser qu'un mineur de 13 ans ne sera pas plus vigilant et averti en la matière et que cet âge n'est pas adapté pour la majorité numérique. L'âge retenu est donc celui de 15 ans même s'il peut paraître utopique d'exiger, d'un mineur de 13 à 15 ans, un consentement du titulaire de l'autorité parentale sachant que 85% des enfants de 12 à 13 ans [140]disposent d'un accès Internet via un téléphone mobile et qu'il est extrêmement difficile de contrôler les réseaux sociaux sur lesquels ils s'inscrivent. Le choix de cet âge semble découler d'un choix quelque peu politique, pas véritablement axé sur un souci de protection, permettant d'harmoniser la loi française car l'âge de la majorité sexuelle et celui à partir duquel les données de santé d'un mineur peuvent être prises en compte par les sondages étaient déjà fixés à 15 ans.

Il est intéressant de préciser que cette limite d'âge de 13 ans pourrait être amenée à évoluer. En effet, Mark Zuckerberg, fondateur et président général de Facebook, considère son réseau social comme un outil éducatif et a affirmé, à de nombreuses reprise, dans le cadre de conférence de presse, vouloir supprimer cette limite d'âge. [141] Facebook s'intéresse aux enfants de plus en plus jeunes car le réseau social vient de lancer en 2017, aux Etats Unis, une version de messagerie instantanée « Messenger Kids » dédiée aux 6-12 ans sans aucune publicité et un contrôle des parents. L'objectif de cette messagerie instantanée est d'initier les mineurs à l'univers des réseaux sociaux dès le plus jeune âge. [142] Toutefois, si l'évolution de cette limite d'âge est étudiée, elle n'est pas encore d'actualité. Les mineurs français font donc face à une double limite d'âge pour l'utilisation des réseaux sociaux : d'une part l'âge de 13 ans qui est l'âge minimum requis pour l'inscription à un réseau social et d'autre part l'âge de 15 ans qui est l'âge de la majorité numérique

[138] J.Lausson, « 15 ans ou 16 ans ? Députés et sénateurs en désaccord sur la « majorité numérique ». », Numerama, 14 mars 2018
[139] B. Charrier, « Le consentement exprimé par les mineurs en ligne », Dalloz IP/IT 2018 p.333
[140] Etude réalisée en 2018 par BVA pour Wiko auprès de 1000 jeunes représentatifs des 12-17 ans
[141] C. Manara, *Réseaux sociaux : 101 questions juridiques*, Editions Diateino, septembre 2013, p.27
[142] V.Letesse, « Pourquoi créer une majorité numérique », France culture, 8 février 2018

permettant au mineur de consentir seul à l'inscription à un réseau social. Si, en théorie, la majorité numérique apporte protection au mineur, en pratique, cette protection est inexistante. (B)

Paragraphe 2 : L'inefficacité de la majorité numérique

La majorité numérique est donc un moyen d'autoriser l'accès aux réseaux sociaux pour le mineur, tout en supervisant son utilisation dans le but de le protéger. Cependant, cette protection n'est qu'apparente puisque son efficacité dépend du contrôle qu'il peut en être fait. Or, à ce jour, il n'est procédé à aucun contrôle officiel et fiable de la limite d'âge de la personne qui s'inscrit sur un réseau social. (A) De plus, la disparité du seuil de la majorité numérique entre les Etats membre de l'Union européenne n'est également pas sans poser problème et certains obstacles à cette protection. (B)

A) Une protection illusoire du mineur par l'absence de contrôle d'âge

En France, s'il est théoriquement impossible de s'inscrire sur les réseaux sociaux avant l'âge de 13 ans et sans le consentement du titulaire de l'autorité parentale entre 13 et 15 ans, aucune vérification sérieuse n'est mise en place et de nombreux jeunes passent outre ces limites. En effet, près de 63% des 11-14 ans fréquenteraient un réseau social avec ou sans l'accord de leurs parents[143]. Ces deux interdits ne sont donc que des protections de façade et donne lieu à s'interroger sur leur efficacité en pratique. Si l'article 8-2 du RGDP[144] précise que le responsable de traitement doit vérifier que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale, aucun outil n'a été prévu par la loi pour s'assurer qu'un enfant âgé de 13 à 15 ans souhaitant s'inscrire sur un réseau social ait obtenu, en amont, l'accord du titulaire de l'autorité parentale. Autrement dit, alors que ce consentement parental est une nécessité comme base légale pour le traitement, il peut s'inscrire en toute impunité sans qu'aucune vérification ne vienne le stopper dans sa démarche. De plus, pour un adolescent de moins de 13 ans, il lui suffit de modifier sa date de naissance pour pouvoir ouvrir un compte en toute liberté. Cette pratique est avérée puisque selon une enquête réalisée par la CNIL, 4 enfants sur 10 de moins de 13 ans ont menti sur leur âge pour s'inscrire sur un réseau social [145]. Ces failles qui permettent un contournement des règles existent dans le processus d'inscription de tous les réseaux sociaux, qu'il s'agisse de Facebook, Instagram, Snapchat ou Twitter.

[143] Enquête réalisée par la CNIL en juin 2018
[144] Article 8-2 du RGPD : « Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.
[145] Enquête réalisée par la CNIL en juin 2018

Ce contournement des règles est possible du fait qu'aucun dispositif de vérification renforcée n'a été mis en place car il est difficile de trouver des solutions adaptées aux méthodes d'inscription sur les réseaux sociaux. La facilité d'accès aux réseaux sociaux manifeste donc la difficulté qu'il existe aujourd'hui à vérifier l'identité des utilisateurs. Ces mesures de majorité numérique et d'âge minimum requis ayant vocation à être protectrices sont donc de fausses promesses. Elles font croire aux parents qu'ils ont les moyens de protéger leurs enfants sur les réseaux sociaux alors que ce n'est pas le cas. Or, au-delà de la question de la collecte des données à caractère personnel, se pose également la question du contenu auquel ces jeunes ont accès lorsqu'ils sont sur les réseaux sociaux. D'ailleurs, d'après l'association e-Enfance : « *l'illusion de règles incontournables risque d'avoir des effets pervers en mettant les parents à distance des usages numériques* ». Il est donc indispensable d'envisager des solutions pour rendre ces règles correctement applicables. L'enjeu étant de mettre en place une protection efficace.

C'est dans cet objectif que le Groupe de travail de l'Article 29 sur la protection des données a apporté des précisions sur le contrôle du consentement du titulaire de l'autorité parentale[146]. Le rapport du G29 recommande d'obtenir des informations concernant le titulaire ayant donné l'autorisation. Par exemple, il pourrait s'agir des coordonnées, d'une adresse mail ou autres. Toutefois, le groupe de travail fait une distinction entre un faible risque et un risque élevé face au traitement des données. En fonction de ce qui est retenu, ces informations réclamées seraient plus ou moins poussées. Une autre solution envisagée est d'obliger les réseaux sociaux à recueillir un justificatif confirmant l'autorisation et l'exercice de l'autorité parentale avant l'ouverture du compte de chaque mineur âgé entre 13 et 15 ans[147]. Le problème est que cette solution est très contraignante et pas réaliste en pratique. Le problème est que ces règles sont susceptibles de contournement par les jeunes. L'idée d'un consentement vérifiable demeure difficile à mettre en place car lorsqu'un mineur s'inscrit sur un réseau social, bien souvent, il n'est pas accompagné de ses responsables légaux et est seul derrière son écran. Or, obtenir le consentement d'une personne qui n'est pas derrière l'écran semble une mission très compliquée pour les réseaux sociaux.

En ce qui concerne le contrôle de l'âge minimal requis pour l'inscription sur un réseau social, la mise en place d'un contrôle par la vérification des pièces d'identité est également fréquemment envisagé. Cependant, cette solution est critiquable car elle nécessiterait l'envoi de documents d'identification. Or, les cartes d'identité comportent des données sensibles et l'accès à ces informations par les réseaux sociaux est contestable car il porterait atteinte à la vie privée et à la protection des données à caractère personnel. Ce contrôle est donc difficile à mettre en œuvre. Outre l'accès aux services de la société d'information tels que les réseaux sociaux, cette problématique est la même pour l'ensemble des sites internet qui nécessitent la majorité,

[146] Groupe de travail « article 29 » sur la protection des données, Lignes directrices sur le consentement au sens du règlement 2016/679 adoptées le 28 novembre 2017
[147] B.Charrier, *Op. cit.*

numérique ou non, de l'enfant pour y accéder. Cette question de contrôle se pose également pour les sites pornographiques. Si la collecte des identités bancaires a été soulevée comme solution permettant la vérification d'âge, la CNIL a souligné, dans l'une de ses recommandations, que la vérification de l'âge à partir de la carte bleue n'est pas une finalité déterminée et légitime[148]. Ce principe de minimisation des données a été renforcé avec l'entrée en vigueur du RGPD qui prévoit à l'article 5-1 c) que le traitement des données à caractère personnel doit être adéquate, pertinent et limité à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Par conséquent, cette solution ne pourrait également pas être retenue pour l'utilisation des réseaux sociaux. En Belgique, un projet de « e-carte d'identité » est envisagé. L'idée est de doter tous les citoyens belges d'une carte d'identité numérique. Cette proposition peut amener à la réflexion. Il pourrait être intéressant de mettre en place un système similaire à celui de la sécurité sociale. Ainsi, à l'âge de la majorité numérique, le mineur devra se recenser auprès d'un service pour qu'une carte d'identité numérique lui soit remis. Cette carte comporterait un numéro, comme le numéro de sécurité social présent sur les cartes vitales, qui devra être renseigné pour toute inscription ou ouverture d'un site qui nécessite un contrôle. Toutefois, cette idée présente plusieurs contraintes. Tout d'abord, il faudrait un lecteur de carte, ce qui peut paraître compliqué. Ensuite, une coopération entre les sites web et les Etats serait indispensable. De plus, cette carte numérique serait, probablement, liée à une collecte de données à caractère personnel ce qui peut faire l'objet de nombreuses réticences quant à sa mise en place. Enfin, les visites de sites web risqueraient d'être retracées et archivées. Or, cela porterait atteinte au droit à la vie privée.

Les réseaux sociaux envisagent de prendre les devants et d'adopter eux-mêmes des outils de contrôle. A titre d'exemple, Facebook songe à mettre en place des analyses des photos publiées permettant de détecter si l'âge minimum requis et le consentement du titulaire de l'autorité parentale ont été respectés. Ainsi, si sur la photo publiée par l'enfant il y a un gâteau d'anniversaire qui compte moins de 15 bougies, un mail d'alerte serait envoyé[149]. De plus, si ce réseau social ferme quotidiennement des milliers de comptes, au regard du nombre de comptes existants et s'ouvrants tous les jours, fermer la totalité des comptes d'enfants de moins de 13 ans serait une mission quasiment impossible[150]. Une autre solution avancée est d'autorisée la CNIL à sanctionner lourdement le responsable de traitement lorsque l'accès à son service n'a pas respecté la majorité numérique. Toutefois, il est indéniable que la mise en place d'outils efficaces pour faire respecter les règles nécessite un dialogue entre les plateformes, les pouvoirs publics et la CNIL.

---

[148] Recommandation de la CNIL - Délibération n° 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n°03 034 du 19 juin 2003

[149] « Protection des mineurs sur internet : un amendement pour abaisser la majorité numérique à 15 ans vient d'être voté » , «www.demarchesad-ministratives.fr , 26 janvier 2018

[150] C.Manara, *Réseaux sociaux : 101 questions juridiques* , Edition Diateino, septembre 2013, p.27

En vue d'adopter des recommandations pour clarifier le cadre applicable aux données personnelles des mineurs et de proposer des conseils pratiques, la CNIL a lancé une consultation publique. Cette consultation publique, ouverte du 21 avril 2020 au 8 juin 2020 et directement accessible sur le site de la CNIL sous format de questionnaire, s'adressait principalement aux acteurs du domaine de l'éducation comme les associations lycéennes et étudiantes ou bien des spécialistes des droits des enfants ou encore des institutions et associations œuvrant dans le domaine de l'enfance et de la famille. De prime à bord, les principes posés par les textes nationaux et européens paraissent clair, mais la CNIL a noté que ces textes ne précisent pas certains points. Le premier point vise les capacités juridiques d'un mineur à effectuer seul certains actes sur Internet. La CNIL s'interroge sur la possibilité d'un enfant à créer des profils utilisateurs sur les plateformes de jeux vidéo en ligne et des réseaux sociaux. Il était possible de répondre à cette question et de préciser à partir de quel âge un enfant peut effectuer de tels actes. Le second point vise les modalités de vérification de l'âge et de recueil du consentement. La CNIL a proposé certaines solutions comme le recours à un système de contrôle parental permettant de poser des filtres et de bloquer certains sites ou bien l'envoi d'un SMS ou d'un message aux titulaires de l'autorité parentale pour obtenir leur consentement ou encore la possibilité pour les responsables légaux de préciser la date de naissance du mineur et les limites de leur consentement. Le troisième point vise la mise en place de garanties complémentaires afin d'interdire ces dispositifs qui incitent les mineurs à rester en ligne. Le quatrième et dernier point vise les modalités d'exercice par les mineurs de leurs droits sur leurs données et les services concernés par la limite d'âge de 15 ans tels que le droit d'accès, de rectification, d'effacement ou d'opposition. La CNIL a donc pu recueillir l'avis de toutes les personnes qui se sentent concernées par ces problématiques. Cette consultation publique permettra l'élaboration de contenus dédiés sur le site web de la CNIL ainsi que sur le site Educnum. Toutefois, l'absence de la vérification de l'âge et du consentement n'est pas la seule faille de la majorité numérique. La « marge de manœuvre » laissée aux Etats pour la fixation de l'âge de la majorité numérique affaiblie la protection. (B)

B) <u>Une protection inégale des mineurs européens</u>

En droit européen, l'adoption du RGPD a été un progrès considérable puisqu'il a permis d'uniformiser la protection des données à caractère personnel dans les Etats membres pour de nombreuses situations. Toutefois, cette uniformité n'est pas totale car comme il est précisé dans le préambule du RGPD au considérant 10[151], sur certains aspects, une « marge de manœuvre » est laissée aux Etats afin de préciser ou compléter les solutions apportées par le règlement. Cette série

[151] Considérant 10 du préambule du RGPD : « (…) Le présent règlement laisse aussi aux États membres une marge de manoeuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées « données sensibles »). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite »

de domaines pouvant se prêter à une modulation nationale est très étendue car le Conseil d'Etat en a comptabilisé une cinquantaine[152]. Les Etats ont donc dû accompagner l'entrée en application du RGPD par des mesures législatives et réglementaires notamment pour le régime du consentement requis pour le traitement des données personnelles d'un mineur dans le cadre de l'offre de services de sociétés de l'information. La notion de consentement est associée à l'âge à partir duquel une personne est en mesure de consentir : cet âge est régulièrement différent en fonction des Etats. D'ailleurs, la fixation du seuil de la majorité numérique, c'est-à-dire l'âge à partir duquel une personne peut consentir au traitement de ses données à caractère personnel, ni échappe pas. En effet, l'article 8 du RGPD a instauré une règle relativement simple selon laquelle le mineur âgé de 16 ans peut consentir seul au traitement de ses données personnelles et en dessous de 16 ans doit obtenir le consentement du titulaire de la responsabilité parentale. Mais cette règle se complexifie par sa mise en application car le règlement européen a laissé une marge de manœuvre aux Etats membres en leur permettant d'abaisser cette limite d'âge, à la condition de ne pas descendre en dessous de 13 ans. En outre, les Etats ont pu fixer selon leurs convictions un seuil différent. Or, cette marge de manœuvre laissée aux Etats n'est pas sans poser quelques difficultés[153].

Le premier problème vise la disparité entre les Etats quant à la protection du mineur face au traitement des données à caractère personnel suite à une utilisation modérée ou non de cette marge de manœuvre. Effectivement, pour sa part, la France a fixé la majorité numérique à l'âge de 15 ans. En dessous, entre 13 et 15 ans, le mineur devra avoir le consentement du titulaire de l'autorité parentale. Ainsi, en abaissant d'un an l'âge de la majorité prévue par défaut par le RGPD, le législateur français a donc usé modérément de sa marge de manœuvre. Parallèlement, l'Allemagne n'a en revanche pas usé de son droit de moduler ce seuil puisqu'elle a décidé de fixer la majorité numérique à 16 ans, c'est-à-dire l'âge prévu par défaut par le RGDP. Toutefois, selon les spécialistes, fixer l'âge à 16 ans n'est pas très réaliste car les jeunes utilisent les réseaux sociaux bien avant 16 ans, voir même avant 13 ans. A contrario, d'autres Etats ont fait des choix moins protecteurs. C'est le cas du Royaume-Uni, l'Espagne, l'Irlande et la Belgique qui ont décidé d'abaisser purement et simplement la majorité numérique à 13 ans. Hors de l'Europe, les Etats Unis ont également fixé cette majorité numérique à l'âge de 13 ans. Cette position est moins protectrice car à cet âge, les enfants n'ont pas encore conscience de la notion de vie privée et des conséquences qui peuvent en découler. Le second problème vise le conflit de lois au sein de l'Union européenne suite aux modulations opérées par les Etats membres. Par exemple, quid de la validité du consentement d'un mineur domicilié dans l'un des Etats membres de l'UE qui donne un accord à un responsable de traitement hébergé dans un autre Etat membre ? C'est une situation développée par M-E ANCEL, professeur d'Université, qui a retenu le cas d'un mineur de 14 ans

[152] CE, avis sur un projet de loi portant adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 7 décembre 2017, p. 3, n° 7
[153] M-E. Ancel, « D'une diversité à l'autre », Revue critique de droit international privé, 2019, p.647

résidant en France qui consent au traitement de ses données à caractère personnel par un responsable de traitement situé en Belgique. [154] D'après l'article 3 §1 du RGPD[155], le règlement est applicable dans cette situation car le traitement des données personnelles est effectué en Belgique, donc dans un pays faisant partie de l'Union Européenne. De ce fait, le RGPD prévoit pour les Etats membres une marge de manœuvre pour ce type de consentement : en vertu de l'article 45 de la loi Informatique et Libertés[156], la loi française prévoit qu'un mineur de 15 ans doit consentir conjointement avec le titulaire de l'autorité parentale au traitement de ses données personnelles ; tandis que l'article 7 §1 de la loi belge du 30 juillet 2018[157] prévoit qu'un mineur de 13 ans ou plus peut consentir seul. Or, d'après l'article 3 – II de la loi Informatique et Libertés[158], la législation française est applicable car le mineur réside en France, mais d'après l'article 4 §1 de la loi belge du 30 juillet 2018[159], la législation belge est également applicable car le responsable de traitement des données est établi en Belgique. Il y a donc bien conflits de lois car cette situation est susceptible d'être régie à la fois par la loi française et la loi belge. De plus, ces deux règles sont incompatibles car, selon le droit français, le consentement du mineur de 14 ans est nul alors que, selon le droit belge, il est valable et conforme à la loi. Si le RGPD avait imposé un âge identique à tous les Etats, ce conflit n'aurait pas eu lieu. Cette marge de manœuvre laissée aux Etats en est à l'origine. Le troisième problème vise la gestion des différents âges du consentement par le responsable de traitement. Cette disparité de la majorité numérique entre les Etats doit, en théorie, être prise en compte par les responsables de traitement. Cette pratique nécessite que le responsable de traitement prenne en compte le lieu où se situe la personne concernée et chaque législation nationale applicable. Cette idée obligerait la mise en place d'actions complexes telles que « *la distinction des consentements par pays pour chaque filiale, une transmission des consentements au sein de la maison mère dans le cas où une filiale collecte un consentement d'une personne concernée non ressortissante du pays où la filiale est établie, la programmation d'algorithmes pour déterminer quelles personnes concernées peuvent bénéficier des emailings et dans quels pays* » [160] . Or, pour les réseaux sociaux tel que Facebook, les conditions générales d'utilisation ne prennent pas en compte cette disparité et sont les mêmes que ce soit pour un mineur résidant en Belgique, en France ou en Allemagne.

---

[154] *Ibid*

[155] Article 3 §1 du RGPD : « Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

[156] Article 45 alinéa 1 de la loi Informatique et Libertés : « En application du 1 de l'article 8 du règlement (UE) 2016/679 du 27 avril 2016, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans. »

[157] Article 7 §1 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : « En exécution de l'article 8.1 du Règlement, le traitement des données à caractère personnel relatif aux enfants en ce qui concerne l'offre directe de services de la société de l'information aux enfants, est licite lorsque le consentement a été donné par des enfants âgés de 13 ans ou plus ».

[158] Article 3 – II de la loi Informatique et Libertés : « Les règles nationales prises sur le fondement des dispositions du même règlement renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France. ».

[159] Article 4 §1 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : « La présente loi s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire belge, que le traitement ait lieu ou non sur le territoire belge. ».

[160] K.Lobry, « Le consentement des mineurs sur internet : une vraie problématique pour les entreprises », DPO, 29 octobre 2018

Même si cette protection est contestable en pratique, en instaurant la majorité numérique le législateur a fait un premier pas pour venir protéger le mineur du traitement de ses données personnelles. Or, pour pouvoir avoir une protection accomplie, il est essentiel de revoir sa mise en œuvre. Un travail doit également être fait face à la surexposition du mineur sur les réseaux sociaux. (Section 2)

Section 2 : La protection du mineur surexposé : enjeu législatif et préventif

Se connecter sur son réseau social de prédilection et communiquer à travers cette plateforme de façon abondante et intime des photos et vidéos de son enfant est devenue une pratique habituelle pour de nombreux parents. Cette surexposition du mineur sur les réseaux sociaux tend à s'interroger sur la prise en compte de l'intérêt de ce dernier par ses représentants légaux, allant ainsi à l'encontre de sa protection. (Paragraphe 1) De plus, l'absence d'obligation de prévention, pour lui ou son entourage, et de droit spécialisé pour le cyberespace affaibli la protection qui peut lui être apportée. (Paragraphe 2)

Paragraphe 1 : Une surexposition à l'encontre de l'intérêt du mineur

Les photos d'enfants sur les réseaux sociaux n'ont jamais été aussi populaires et les comptes de bébés éclosent de plus en plus. Dès lors que les responsables légaux ont, tous les deux, donné leur consentement pour publier des photos du mineur sur les réseaux sociaux, rien ne leur interdit de le faire. Toutefois, cette nouvelle tendance à partager l'image et le quotidien de son enfant soulève quelques interrogations au regard des notions de vie privée et d'empreinte numérique des mineurs. (A) Cette surexposition et les produits qui en découlent positionnent des enfants comme de vrais travailleurs du web. La monétisation des contenus peut donc poser problème en cas de parents peu scrupuleux. (B)

A) Les dangers de publications massives d'images d'un mineur par ses représentants légaux

Pour les psychologues, l'exposition de l'enfant par ses parents sur les réseaux sociaux s'explique par le fait que ce dernier est fétichisé, perçu comme une sorte de trophée venant parfois valoriser le parent dans sa capacité d'être un parent présent, aimant et parfait. Or, idéalement, le lien entre un parent et un enfant doit être le plus authentique possible. Le parent n'a pas besoin de

poster de photos de son enfant pour montrer à quel point il est un bon parent. Cependant, il est difficile, voir quasiment impossible d'interdire à un parent de publier des photos de son enfant sur les réseaux sociaux. En effet, lorsque l'enfant est mineur, ses responsables légaux, généralement ses parents, exercent tous les droits de ce dernier, dont le droit à l'image. Le droit à l'image est censé être protégé par le consentement des titulaires de l'autorité parentale et d'après la jurisprudence, une photo de mineur ne peut être utilisée sans l'accord des deux parents, notamment pour la publication du cliché sur les réseaux sociaux. Concrètement, les responsables de l'autorité parentale doivent consentir tous les deux à la diffusion de l'image sans avoir à demander l'avis du mineur pour pouvoir le faire. Le consentement du mineur n'a donc aucune valeur légale. D'ailleurs, 34% des parents considèrent qu'ils ont le droit d'afficher des photos sans le consentement de leur enfant et 13% pensent que c'est uniquement aux parents de décider si une photo peut être ou non diffusée car 25% des parents pensent que leur enfant est trop jeune pour décider[161]. Or, dès que le mineur est capable de s'exprimer, il est intéressant de le consulter en lui demandant son accord, au moins symbolique. Cette démarche lui permet de prendre conscience de son droit à l'image et du respect qui doit lui être apporté. Elle permet également au mineur d'être plus respectueux du droit à l'image d'autrui. De plus, il faut garder à l'esprit que si l'exercice du droit à l'image est détenu par la personne qui possède l'autorité parentale, ce droit appartient avant tout au mineur. Ainsi, toute prise de décision dans le cadre de l'exercice de l'autorité parentale doit prendre en compte l'intérêt de l'enfant. Autrement dit, pour l'exercice du droit à l'image du mineur, le parent doit veiller à ce que les photos publiées de son enfant ne soient ni dégradantes, ni humiliantes. Il est essentiel que les parents pensent à leur responsabilité avant de poster des photos de leurs enfants car cet acte peut impacter leurs e-réputation dès le plus jeune âge. Cet acte perçu comme anodin pour une majorité de parents n'est pourtant pas sans danger.

En grandissant et en prenant conscience des conséquences et de l'impact de la diffusion de son image sur le web, le mineur peut considérer comme préjudiciable le fait d'avoir sa vie privée exhibée sur les réseaux sociaux par ses parents. Quid de l'action de l'enfant, devenu majeur, envers ses parents qui auraient postés des clichés de lui mineur sur les réseaux sociaux ? La situation s'est présentée devant le Tribunal civil de Rome en janvier 2018. Un jeune homme, âgé de 16 ans, après avoir porté plainte contre sa mère qui publiait sans cesses des photos de lui sur Facebook, a saisi la juridiction italienne pour divulgation de sa vie privée sur les réseaux sociaux. S'appuyant sur l'article 96 de la Constitution italienne selon lequel l'image d'une personne ne peut pas être exposée sans son consentement, les juges italiens se sont positionnés en faveur du jeune homme. Le sujet d'une photo en possède donc les droits et ce principe est rappelé dans les conditions générales d'utilisation de Facebook qui prévoit que les utilisateurs acceptent de « ne pas poster du contenu ou prendre une quelconque action sur Facebook qui contrevient ou viole le droit de

[161] Etude du 28 août 2018 menée par la société McAffee

quelqu'un d'autre ou autrement viole la loi ». Le tribunal a donc ordonné à la mère de ce jeune homme de retirer et ne plus poster de photos de lui sur Facebook. En cas de non respect et de récidive, celle-ci sera condamnée à verser 10 000€ de dommages et intérêts. En France, cette situation ne s'est pas encore présentée du fait que la génération touchée par cette surexposition sur les réseaux sociaux n'est pas encore majoritairement majeure et n'est pas en capacité de requérir en justice. Reste à voir ce que l'avenir réserve : ce type d'action en justice pourrait apparaître dans un futur très proche et les juridictions françaises pourraient aller dans le sens de ceux qui se retourneraient contre leurs parents. L'article 9 du Code Civil garantit le droit au respect de la vie privée pour chacun sans compter l'article 226-1 du Code pénal qui prévoit que toute personne ayant diffusé ou publié des images d'une personne sans son consentement encourt une peine d'un an de prison et une amende de 45 000 euros. De plus, "le fait de conserver, porter ou laisser porter à la connaissance du public" une photo prise dans ces conditions est puni des mêmes peines comme le dispose l'article 226-2 du Code pénal. De ce fait, en cas de contentieux, si la diffusion d'une photo de son enfant sur Facebook vient à être démontrée comme être une manière de la rendre publique, l'atteinte à la vie privée pourra être retenue.

Si le compte n'est pas suffisamment protégé, amis et famille ne sont pas les seuls à avoir accès aux photos. Le risque lié à l'accessibilité par des étrangers est la récupération d'images à des fins pédopornographiques. D'ailleurs, en 2015, la viralité du « Motherhood Challenge » sur Facebook a obligé la gendarmerie nationale à rappeler les dangers que pouvaient engendrer cette pratique.[162] A l'occasion de ce challenge, de nombreuses photos d'enfants ont émergé sur le réseau social car les mères étaient invitées à publier des photos de leurs enfants et ensuite nominer d'autres amies à faire de même de sorte à ce que cela face une chaîne. De ce fait, les forces de l'ordre ont diffusé un message alarmant sur leur propre page Facebook : « *Préservez vos enfants ! (…) certes, vous pouvez être toutes/tous fières ou fiers d'être une maman ou un papa de magnifiques bambins, mais attention ! Nous vous rappelons que poster des photos de ses enfants sur Facebook n'est pas sans danger ! Il est important de protéger la vie privée des mineurs et leur image sur les réseaux sociaux. Parfois, les bons moments méritent d'être "juste" partagés dans la vraie vie !* ». Parfois, plus que la photo en elle-même, le danger peut se trouver dans des détails permettant de retracer la localisation de l'enfant. Beaucoup de réseaux sociaux indiquent l'emplacement d'un utilisateur lorsqu'une photo est publiée. Afin d'éviter de divulguer cette information, il faut que les parents s'assurent, au moment du partage de la photo sur un réseau social, que cette fonction a été désactivée car elle peut être une cause d'enlèvement.

Enfin, à travers ce phénomène de sharenting, de nombreux enfants, parfois avant même dès leur naissance, vont posséder une empreinte numérique. Cette empreinte numérique désigne l'ensemble des traces laissées volontairement ou non sur le web, notamment par le biais de

[162] N. Leroux, « A-t-on le droit de publier des photos de ses enfants sur les réseaux sociaux ? », avril 2019, Chronique

partages sur les réseaux sociaux. Il s'agit d'une donnée, or les données des mineurs font l'objet d'un traitement particulier. Un mineur ne pouvant pas consentir seul au traitement de ses données jusqu'à 15 ans, ce sont les responsables légaux qui sont chargés de le faire à sa place. Cependant, les titulaires de l'autorité parentale ne sont pas toujours conscients des conséquences juridiques que peut entrainer le choix de créer l'existence numérique du mineur. De part la création de cette empreinte numérique, plusieurs acteurs seront autorisés à traiter les données du mineur et des problématiques au regard de leur vie privée peuvent apparaitre.

Par conséquent, être responsable de l'image d'un mineur prend un tout nouveau sens avec les réseaux sociaux. Les titulaires de l'autorité parentale, principalement les parents, doivent prendre conscience de leur responsabilité et de l'impact de leur choix face à l'exposition du mineur sur les réseaux sociaux. Cette surexposition, au regard de toutes les traces numériques persistantes qu'elle peut laisser, n'est pas sans danger sur l'équilibre moral et la sécurité de l'enfant, mais aussi sur la relation parents-enfants qui peut être entachée par un litige en devenir. Ne faudrait-il pas interdire aux parents de rendre public les photos ou vidéos de leur progéniture sur les réseaux sociaux? Ou les obliger à demander l'autorisation du mineur avant de poster un cliché de ce dernier ? L'usage exponentiel des réseaux sociaux par la société n'a donc pas fini de faire bouger et évoluer le droit français car la surexposition des enfants par leurs parents sur ces plateformes a été à l'origine de certaines dérives devant être encadrées. Certains parents filment leur enfant au quotidien et diffusent cela sur des chaînes YouTube avec un modèle économique très concret puisque les chaines font des millions de vues. Ici, l'enfant n'est plus un trophée mais une valeur marchande. (B)

B) <u>Le travail des enfants sur les réseaux sociaux non encadré</u>

Néo (14 ans) , Swan (7 ans), Kalys (11 ans), Athéna (6 ans) sont tous liés par un point commun: enfants stars du web et parfois depuis plusieurs années malgré leur jeune âge.
Leur notoriété, ils la doivent à des vidéos postées sur YouTube dans lesquelles ils ouvrent des colis, testent des jouets, réalisent des défis, cuisinent ou font des tutoriels. A travers ces vidéos, les parents mettent en scène leur progéniture afin d'exposer leur vie quotidienne et de la partager avec leur communauté. Ces « vlogs » sont une sorte de carnet intime en vidéo et peuvent parfois s'apparenter à de la télé-réalité avec des scénarios écrits et une mise en scène dans le but d'imiter la réalité. La durée de ces vidéos est variable : elles peuvent être courtes, de 3 à 4 minutes ou très longues, de 25 à 30 minutes. Quant à la fréquence de publication, elle est également variable en fonction des chaînes : certaines chaînes publient une vidéo par jour, d'autres en publient une par semaine. Ce phénomène de chaines « familiales » est né aux Etats Unis et s'est répandu en France

depuis plusieurs années faisant apparaître des chaînes suivies par des millions d'abonnées. Ainsi, Swan est suivie par 4,4 millions d'abonnés, son frère Néo cumule 1,6 et presqu'autant pour Kalys et Athéna de la chaîne Studio Bubble Tea, suivie par 1,55 millions de personnes. [163]Au départ, ces vidéos amatrices étaient réalisées avec naturel et peu de moyens. Aujourd'hui, entre matériel de qualité et gimmick en début et fin de chaque vidéo, elles ont tout de professionnelles. Ainsi, alors que ces chaînes familiales connaissent un développement beaucoup d'interrogations se posent quant à qualification de leur activité. S'agit-il d'un loisir ou bien d'un travail ? Est-ce une forme d'exploitation par les parents de leur progéniture ?

Pour la génération Z, génération hyperconnectée, les réseaux sociaux sont devenus leur média principal. Selon une étude de l'agence DEFY Media datant de 2015, les jeunes portent plus d'intérêt aux vidéos en ligne qu'à la télévision. En effet, 96% des 13-17 ans regardent des vidéos en ligne, que ce soit sur YouTube ou sur les réseaux sociaux, pour une durée moyenne de 11 heures par semaine. En revanche, le visionnage de la télévision dépasse difficilement les 8 heures par semaine pour 80% des adolescents. [164]Le développement d'Internet et l'intérêt grandissant pour les réseaux sociaux ont été à l'origine de l'apparition de nouvelles professions telles que « Youtubeur », « Instagrameur » et plus généralement « influenceur ». A partir du moment où une personne crée du contenu sur Facebook, Instagram, YouTube ou Snapchat et qu'elle développe une communauté, elle est appelée « influenceur ». Un influenceur est une personne disposant d'un fort pouvoir de suggestion sur le public et tire parti de sa notoriété pour promouvoir des produits ou des services. [165] Sa notoriété et sa visibilité lui permettent de passer des contrats avec des marques pour faire la promotion de produits, c'est-à-dire des placements de produits dans les contenus vidéos qu'ils diffusent. Les médias sociaux sont devenus peu à peu les canaux de communication privilégiés des marques, au travers de ces stars du web. Si les premiers partenariats sont apparus dans les années 2000, aujourd'hui, ils sont pleinement ancrés dans les stratégies marketing des marques. Entre réception de produits et voyages pour les promouvoir, sous l'influence des réseaux sociaux, les rêves et les vocations des enfants de la fin du 20e siècle ont subitement changé pour s'orienter vers ces nouveaux métiers puisque 34,2% des 6-17 ans révéraient de devenir une star du web. [166]Les jeunes s'identifient à travers ces Youtubeurs et veulent leur ressembler. Pour cela, des écoles visant à former les futurs Youtubeurs ont ouvert en France.

[163] R. David, « Une proposition de loi pour encadrer les enfants influenceurs sur YouTube », Europe 1, 6 décembre 2019
[164] C. Pastezeur, « FOBO, thumbstopper et influence de YouTube, le rapport des jeunes à la vidéo en ligne décrypté », Air of Melty, mars 2015
[165] T. Girard-Gaymard, « Les influenceurs et le droit », Recueil Dalloz 2020, p.92
[166] J. Dirnhuber, « Children turn backs on traditional careers in favour of internet fame, study finds », The Sun, mai 2017

La loi française interdit aux enfants de moins de 16 ans de travailler[167] , âge auquel ils sont libérés de l'obligation scolaire. Toutefois, il peut être dérogé à ce principe puisque l'emploi d'enfants mineurs est fréquent dans le milieu du spectacle, de la publicité ou de la mode. Afin d'éviter tout abus et de protéger l'enfant-artiste, le législateur français a mis en place une réglementation stricte et spécifique. Le Code du travail encadre donc le métier d'enfant-artiste aux articles L.7124-1 à L.7124-35, mais également aux articles R.7124-1 à R.7124-38. Dès lors, une autorisation individuelle doit être délivrée par le préfet de région après avis de la Commission Départementale de protection de l'enfance en plus de l'autorisation parentale. De plus, les modalités de travail font l'objet de règles propres et les rémunérations perçues sont placés à la Caisse des Dépôts et consignations jusqu'à la majorité de l'enfant. [168]

Si le numérique ne doit pas échapper à l'Etat de droit, aujourd'hui, il y a un inquiétant vide juridique sur les conditions de travail des enfants sur le Web. En effet, ces enfants, parfois très jeunes engendrent des fortunes en dehors de tout cadre légal et ne se rendent pas compte de l'activité commerciale qui entoure leur vidéo. Ces vidéos nécessitent un important investissement : du temps de travail pour leur préparation et leur réalisation et de l'argent pour l'achat du matériel. Cet investissement augmente au fur et à mesure que la chaîne gagne en nombres de vues, de likes et d'abonnés. Par conséquent, au vu de ces éléments, les enfants qui interviennent dans ces vidéos exercent un travail. [169] Or, ces enfants influenceurs, de moins de 16 ans, qu'ils soient Youtubeurs, Instagrameurs ou autre, ne bénéficient pas de protection par le droit du travail.

La presse met de plus en plus en lumière les dérives de ces chaînes YouTube familiales faisant de ces enfants des influenceurs en herbe. A travers le film « Selfie » (sortie en janvier 2020) Thomas Bidegain, réalisateur français, dénonce ces familles prêtes à tout pour augmenter l'audience de leur chaîne YouTube. Entre scénarisation des enfants, pression des parents pour qu'ils affichent un sourire sur les vidéos et chaque détail du quotidien filmé, ces familles productrices cherchent par tous moyens de monétiser au mieux les contenus audiovisuels qu'ils publient. Cette motivation excessive néglige parfois l'intérêt et le bien être de l'enfant. Aux Etat-Unis, un père mettait en scène ses filles de 9 et 7 ans dans des vidéos promotionnelles pour des jouets ou des scènes de vie quotidienne. Le contenu des vidéos a fait polémique et ce dernier a été accusé de maltraitance sur ses enfants car il imposait des canulars cruels à ses enfants : jeter un crapaud dans le bain de ses enfants ou étaler de la mousse à raser sur le visage de l'une de ses filles

[167] Article L.1724-1 code du travail : « Un enfant de moins de seize ans ne peut, sans autorisation individuelle préalable, accordée par l'autorité administrative, être, à quelque titre que ce soit, engagé ou produit :
1° Dans une entreprise de spectacles, sédentaire ou itinérante ;
2° Dans une entreprise de cinéma, de radiophonie, de télévision ou d'enregistrements sonores ;
3° En vue d'exercer une activité de mannequin au sens de l'article L. 7123-2 ;
4° Dans une entreprise ou association ayant pour objet la participation à des compétitions de jeux vidéo au sens de l'article L. 321-8 du code de la sécurité intérieure. »

[168] Article L7124-9 du code du travail : « Une part de la rémunération perçue par l'enfant peut être laissée à la disposition de ses représentants légaux. (…) Le surplus est versé à la Caisse des dépôts et consignations et géré par cette caisse jusqu'à la majorité de l'enfant. »

[169] T. Labatut, « L'exploitation des mineurs dans les médias sociaux : faut-il s'alerter ? », Lextenso- Petites affiches – n°113- p.10

en pleurs. Sa chaîne a été supprimée par YouTube. Condamné à 5 ans de mise à l'épreuve et le retrait de la garde de ses enfants.

C'est pour cette raison que, le 25 juillet 2018, l'association l'Observatoire de la parentalité et de l'éducation numérique (Open) a saisi, Geneviève Avenard, défenseure des enfants, afin de dénoncer une activité professionnelle illicite. [170] L'Open estime que ces jeunes effectuent « un travail exercé sans officialisation et sans encadrement juridique aux fins de protéger l'enfant mineur » et craint que cette activité mette « en péril leur développement physique et psychologique ». En effet, selon la fréquence de tournage et la durée des vidéos, les enfants peuvent y consacrer beaucoup de temps. Le droit du travail n'encadre ni les horaires ni les durées de tournage de ces enfants. Pour une grande majorité des familles, ces activités relèvent du loisir. Or, dès lors qu'un lien de subordination, une prestation de travail et une rémunération peuvent être constatés, il ne s'agit plus d'un loisir mais d'un travail déguisé. De plus, un enfant influenceur génère des revenus par son activité sur les réseaux sociaux. Ne reconnaissant pas cette exploitation commerciale de l'image, le code du travail n'encadre pas le versement des rémunérations qui en découle. De ce fait, les revenus sont directement perçus par les parents et l'enfant n'est pas assuré d'en recevoir une part. Cette absence de protection actuelle pourrait donner lieu à une génération de futurs Jordy. Ancien bébé star dans la chanson, à sa majorité, le jeune a assigné son père pour escroquerie car ce dernier a détourné la totalité des revenus de son fils à des fins personnelles, sans les avoir placé sur un compte bloqué. Enfin, en plus de l'impact sur le développement physique ou psychologique, cette surexposition des enfants peut engendrer les risques d'un cyberharcèlement.

Face à ce vide juridique, le député Bruno Studer a déposé une proposition de loi visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de 16 ans sur les plateformes en ligne.[171] L'objectif est de garantir les droits de l'enfant et de lutter contre toute forme de travail dissimulé. Elle a été adoptée en première lecture et à l'unanimité par l'Assemblée nationale le 12 février 2020, puis en première lecture par le Sénat le 25 juin 2020. L'adoption par le Sénat aura été cependant précédé par quelques révisions portant sur les modalités de versement des revenus sur le compte de la Caisse des dépôts, les modalités d'application des sanctions et les chartes adoptées par les plateformes afin de favoriser l'information et la sensibilisation des mineurs sur les conséquences de la diffusion de leur image. Cette proposition de loi devra être reprise par amendements parlementaires au moment de l'examen du projet de loi de réforme de l'audiovisuel, au premier semestre 2020. [172] Ainsi, après les enfants mannequins, acteurs et plus récemment les joueurs esportifs, ce sont bientôt les enfants influenceurs qui seront protégés par le Code du travail.

[170] A. Leclair, « Le troublant phénomène des enfants stars sur YouTube », Le Figaro, 30 juillet 2018
[171] Proposition de loi visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne présenté par Bruno Studer
[172] P. Croquet, « Une proposition de loi pour encadrer les activités des enfants youtubeurs et e-sportifs », Le monde 04 décembre 2019

En premier lieu, cette proposition de loi a vocation à qualifier de travail l'animation d'une chaîne YouTube, et plus globalement, l'activité des influenceurs mineurs. Ainsi, l'article 1 de la proposition de loi prévoit un régime protecteur pour les enfants influenceurs similaire à celui déjà applicable pour les enfants travaillant dans le monde du spectacle, du mannequinat ou des compétitions esportives. Désormais, si l'activité de l'enfant est considérée comme un travail, les parents devront solliciter une autorisation individuelle de travail ou un agrément auprès d'une commission départementale. Ce régime est similaire à celui déjà applicable aux enfants du spectacle et garantit des conditions d'emploi compatibles avec la scolarisation et la santé de l'enfant. L'actuel régime des enfants artistes prévoit, que ce soit pour les moins de 16 ans ou les 16-18 ans, une durée de travail maximum de 8 heures par jours et de 35 heures par semaine avec des aménagements possibles. En revanche, si l'activité de l'enfant ne relève pas du droit du travail, le mineur est tout de même protégé puisqu'une obligation de déclaration est prévue. Ainsi, cette proposition de loi vise à responsabiliser les parents puisque, dès que l'enfant influenceur dépassera un certain seuil de temps passé et de revenus, son activité devra être déclarée. Ces seuils seront fixés par décret. En second lieu, cette proposition de loi encadre le versement des revenus générés par ces enfants. L'article 3 prévoit, jusqu'à la majorité de l'enfant, le versement de la majeure partie de ces revenus sur le compte de la Caisse des dépôts et consignations. En troisième lieu, les articles 2 et 4 visent à responsabiliser les plateformes. D'une part l'article 2 oblige les plateformes à retirer toute vidéo qui met en scène un mineur de moins de 16 ans et fait une entorse au droit du travail. D'autre part, l'article 4 renforce la détection des contenus audiovisuels problématiques par les plateformes et crée une obligation de coopération avec les autorités publiques. En quatrième et dernier lieu, la proposition de loi soumet les plateformes à une certaine vigilance. L'article 5 crée un droit à l'oubli pour les mineurs dont l'image est diffusée par une plateforme de partage de vidéos. Ainsi, les images postées sur la plateforme devront être obligatoirement retirées par cette dernière dès lors que le mineur en fait la demande.

S'il est indispensable de légiférer, ce qui ferait de la France une pionnière en la matière, lorsque le législateur veut protéger les mineurs et s'attaque à la réglementation de l'usage des réseaux sociaux par ces parents, il est à craindre dans ce combat que ce ne soit qu'une esquive. D'après Michael Stora, encadrer juridiquement ces pratiques semble insuffisant quand la seule réponse efficace, face à l'abus et les dérives, serait l'interdiction absolue de ces chaines familiales. Contrairement aux enfants mannequins ou acteurs qui exercent leur activité hors du cadre familial, les chaînes « familiales » font des parents des réalisateurs/ producteurs et des enfants des acteurs au sein de la famille. Cette absence de frontière, entre professionnel et familial, peut être pervers car il sera difficile de vérifier que les familles respectent à la maison les conditions de travail posées par la loi. Toujours selon le psychologue, la proposition de loi aurait dû interdire les

rémunérations de partenariat avant un certain âge afin d'éviter aux parents la tentation des collaborations.

Cette surexposition du mineur, qu'elle soit de son initiative ou non, et les conséquences qu'elle peut entrainer montre la nécessité d'encadrer, de manière plus appropriée, les dangers de l'utilisation des réseaux sociaux et de mieux former les plus jeunes à les affronter. (Paragraphe 2)

Paragraphe 2 : La révision du cadre législatif et préventif pour une meilleure protection

Face à l'évolution permanente des nouvelles technologies et leur place de plus en plus importante dans la société, le législateur est venu modifier et aménager le droit commun. Cependant, cette adaptation a ses limites. La création d'un nouveau droit dédié au cyberespace semble donc indispensable. (A) Un travail est également nécessaire quant à la sensibilisation du mineur face aux dangers réels du monde virtuel. Pour le protéger, il est primordial qu'il connaisse les valeurs et les moyens liés à une bonne pratique du numérique et de savoir réagir en cas de problèmes. Cette prévention commence à se mettre en place mais elle se doit d'être encore plus poussée et plus présente dans le quotidien du mineur afin qu'il soit armé et accompagné dans une bonne utilisation des réseaux sociaux. (B)

A) Le droit du cyberespace : un droit 3.0

Après une lecture analytique des textes et lois pour le développement de cette étude, il ressort que la protection du mineur internaute est assurée par l'application du droit commun. En effet, afin de répondre à cette problématique moderne, le législateur est venu aménager des dispositions préexistantes laissant parfois un vide juridique. Si, en théorie, le recours au droit commun peut paraître adéquate, la pratique montre que ce n'est pas une solution adaptée puisqu'elle ne permet pas une protection absolue et aboutie du mineur. Ainsi, plusieurs difficultés sont apparues dans la mise en œuvre de la protection prévue par le droit commun. La première vise, l'incapacité juridique du mineur le mettant sous la tutelle de ses représentants légaux : les droits de l'enfant sont donc restreints et se sont les titulaires de l'autorité parentale qui les exercent en son nom. Or, les choix de ces derniers impactent directement le mineur et peuvent avoir, sans qu'ils n'en soient conscients, des conséquences dans le futur pour l'enfant. C'est ce qui passe avec la surexposition de l'enfant par ses parents sur les réseaux sociaux, sur le fondement de l'exercice du droit à

l'image. La seconde vise, les difficultés d'identification derrière un écran. Si dans le monde réel, il est possible et facile d'identifier l'âge d'une personne, le monde virtuel présente de nombreuses contraintes rendant difficile cette pratique. Or, bénéficiant d'une réglementation juridique spéciale pour son accès aux réseaux sociaux et de la mise en place de dispositions dans l'optique de le protéger, le mineur doit nécessairement faire l'objet d'une identification. De plus, les techniques d'identification applicables au monde réel, telles que la vérification de la carte d'identité, ne conviennent pas au monde virtuel. Ainsi, l'utilisation du droit commun n'est pas appropriée car celui-ci ne prend pas en compte les spécificités du cyberespace. Le cyberespace et les réseaux sociaux ne sont donc pas un terrain de non droit. Toutefois, l'aménagement et la révision des textes de droit commun demeurent insuffisants à la protection du mineur dans le cyberespace. L'instauration d'une réglementation visant à régir les infractions commises dans le cyberespace paraît indispensable pour permettre au mineur d'avoir une protection accomplie. [173]

La création d'une telle réglementation permettrait également de s'attarder sur des problématiques nées de l'utilisation du numérique mais qui ne sont pas traitées par le droit commun. De nombreuses études montrent que le mineur pourrait être une victime des écrans. Depuis 2012, le temps passé par les 10-16 ans sur les réseaux sociaux a augmenté de 62,5% et continue de croître. Ils passent en moyenne 2,6 heures par jour sur ces plateformes. Inquiets de l'ampleur de ce phénomène, certains professionnels parlent « d'addiction » et précisent que cette utilisation massive des écrans et des réseaux sociaux par les jeunes viendrait impacter leur socialisation et leur développement. En effet, elle serait à l'origine de difficultés de concentration, de manque de sommeil et viendrait affaiblir le lien social que les enfants déploient. En outre, une réglementation spécifique pourrait venir créer une disposition interdisant, aux réseaux sociaux, d'utiliser des techniques de « racolages » telles que les notifications incessantes ou les contenus personnalisés, afin de limiter l'utilisation des écrans et des réseaux ainsi que de réagir à leurs méfaits. [174]

En plus de l'application du droit commun, la protection du mineur sur le cyberespace nécessite de recourir à un droit spécifique prenant en compte les spécificités du cyberespace ainsi que le statut juridique du mineur. Toutefois, pour protéger le mineur, il est indispensable de créer des mesures juridiques et techniques qui prennent à la fois en compte sa vulnérabilité, mais également les spécificités du web. L'une des caractéristiques du cyberespace est qu'il s'agit d'un réseau transnational. Malgré l'adoption du RGPD, règlement européen, la protection du mineur sur Internet, et par conséquent sur les réseaux sociaux, est régit par l'adaptation de textes nationaux. Ainsi, cette protection est soumise à la confrontation de législation de nombreux pays. La lutte

[173] C. Nlend, *La protection du mineur dans le cyberespace* , Editions Néressis, 12 août 2010
[174] J.Henno, « Comment décrocher les ados de leurs écrans ? », LesEchos, 28 octobre 2019

contre les cybercriminels fait partie de la protection du mineur sur les réseaux sociaux. Du fait du caractère multinational de l'Internet, elle peut parfois être compliquée à mettre en place. En effet, des conflits de lois peuvent apparaître et produire des solutions différentes pour des faits identiques. La meilleure réponse à cette difficulté serait la création d'institutions policières et judiciaires internationales dédiées au cyberespace et permettant une protection égalitaire du mineur dans tous les pays. [175] Cette idée reviendrait à instaurer une réglementation internationale. Le droit applicable à Internet serait alors un droit applicable à tout pays dans des circonstances similaires. Si la France montre une certaine volonté de réfléchir à un code mondial de bonne conduite dans le cyberespace, il existe de vraies divergences, de fond, concernant les visions des Etats dans la recherche d'une cybersécurité. [176] Les pays démocratiques auraient plus la capacité de développer une politique juridique commune que les pays autocratiques. Donc, la coopération entre tous les Etats, indispensable pour un tel projet, rend la tâche extrêmement difficile.

La protection du mineur sur le cyberespace est une problématique universelle qui nécessite donc une solution internationale. Cependant, au regard du développement et de la diversité idéologique des différents pays dans le monde, une telle loi semble utopique de part sa complexité à être adoptée et de sa mise en vigueur. Si la prévention du mineur ne peut pas remplacer une réglementation, elle peut, tout de même, être une solution non négligeable permettant, à ce dernier, d'avoir les outils nécessaires pour se protéger et se défendre dans ce monde virtuel. (B)

B) <u>La nécessité de mieux sensibiliser pour mieux protéger</u>

La prévention des dangers d'Internet, notamment avec l'utilisation des réseaux sociaux, est indispensable pour une bonne protection du mineur. En sensibilisant le mineur sur certains points, il pourra prendre conscience et se prémunir des risques qu'il peut rencontrer dans l'usage des réseaux sociaux. Le premier point vise la maîtrise des paramètres de confidentialité. Il est important qu'il prenne le reflexe de limiter la visibilité de ses publications. Le second point est la sensibilisation à la réflexion qui est primordiale avant toute publication sur les réseaux sociaux. Il faut qu'il comprenne que toute information laissée sur Internet ne s'efface pas, ou très difficilement, et qu'elle peut être vue et enregistrée par de nombreuses personnes. Le mineur doit également avoir conscience que, pour sa sécurité, il ne doit pas trop dévoiler sa vie privée sur les réseaux sociaux. Le troisième point concerne la protection de ses informations personnelles. Le quatrième point consiste à enseigner à l'enfant à être méfiant des rencontres qu'il peut faire en ligne. Il doit être avisé que n'importe qui peut se cacher derrière un pseudonyme, notamment des

[175] M. Gargouri, « La protection du mineur fae aux dangers du cyberespace », LegiTeam, lecture, Juillet 2019
[176] H.Meddah, « La France en première ligne pour règlementer le cyberespace », LeMonde, 21 mars 2017

personnes malintentionnées. Le cinquième point est de lui faire comprendre qu'il est important de dialoguer, avec un adulte, de son utilisation d'Internet. Ainsi, certaines infractions telles que l'atteinte à la vie privée par le traitement des données personnelles, le cyberharcèlement ou le grooming pourraient être déjoué grâce à une bonne sensibilisation du mineur.

L'école est un très bon tremplin pour sensibiliser les mineurs des risques de l'utilisation des nouvelles technologies et des outils qui en découlent pour, à terme, leur amener une protection optimale. Dans cet optique de prévention, le brevet informatique et internet, aussi appelé « B2i », a été instauré dans les collèges et lycées. Ce diplôme a pour vocation d'évaluer les compétences des élèves dans plusieurs domaines : savoir être responsable sur internet, savoir organiser des recherches d'information à partir d'outils numériques, mais aussi communiquer et travailler en réseau. La plateforme d'évaluation et de certification des compétences numériques PIX est venue se substituer à ce brevet informatique. L'objectif de cette plateforme est d'offrir un service public pour évaluer en ligne le niveau de maîtrise des connaissances et de compétences numériques. Elle est accessible gratuitement aux collégiens, lycéens, étudiants ainsi qu'aux pour les professionnels. Or, ces outils ne traitent pas, en particulier, de l'utilisation des réseaux sociaux et des risques et dangers pouvant en émaner. De plus, ils ne s'adressent pas à l'école élémentaire alors que les mineurs ont accès de plus en plus tôt aux nouvelles technologies et à internet puisqu'en moyenne les enfants reçoivent leur premier smartphone à l'âge de 9 ans et neuf mois et que 28% des enfants possèdent, dès l'âge de 10 ans, leur propre tablette.[177] Donc, malgré la mise en place de ces dispositifs de prévention, cette dernière n'est pas aboutie au vu de l'usage que font les mineurs des nouvelles technologies.

En parallèle, afin de permettre aux élèves, les « cybercitoyens » de demain, d'avoir une compréhension et un usage autonome et responsable des médias, l'éducation aux médias et à l'information a été instaurée dans le système éducatif suite aux préconisations de l'UNESCO. L'EMI est une éducation citoyenne aux médias permettant aux élèves d'avoir une lecture critique et distanciée de ce qu'ils peuvent trouver dans les médias. Elle permet aussi la compréhension et l'usage de ces derniers par tous les élèves qui, pour une grande majorité aujourd'hui, sont à la fois lecteurs et diffuseurs de contenus. Etant aujourd'hui considérés comme des médias, les réseaux sociaux entrent dans le champ d'application de cet enseignement au même titre que la presse papier ou numérique. Ainsi, cet enseignement interdisciplinaire s'inscrit dans le Parcours Citoyen, l'un des quatre parcours éducatifs prévus par la loi de refondation de l'Ecole de 2013. Cependant, cet enseignement demande encore à être amélioré et complété pour faire des mineurs des internautes avertis. En effet, contrairement à d'autres disciplines, l'EMI est une discipline transversale n'ayant pas de place à part entière dans le programme scolaire. De plus, il est décentralisé puisque chaque

[177] F.Bayard, « Smartphones : les enfants reçoivent leur premier téléphone à 9 ans », Phoneandroid, 12 février 2020

établissent décide de quelle manière il souhaite le mettre en œuvre. Si certains établissements utilisent les réseaux sociaux en classe dans le cadre de travaux afin d'initier les élèves à une bonne utilisation de ces derniers, d'autres ont une approche différente de cet enseignement et ne s'intéressent pas à l'usage de ces plateformes. Dès lors, une inégalité sur la sensibilisation apparaît entre les élèves en fonction des établissements. Enfin, si l'EMI remplit bien son rôle dans la préparation du mineur à l'exploitation des informations qu'il trouve via les réseaux sociaux et notamment à la détection de la mésinformation, en revanche, il ne le prépare pas du tout à la vigilance dont il doit faire preuve lors de la pratique des réseaux sociaux. Donc, il ne permet pas d'armer le mineur face au danger et la prévention des mineurs, notamment aux réseaux sociaux, n'est pas intégrée au cursus scolaire. Cette absence de prévention est due à des enjeux politiques et économiques. Beaucoup d'établissements souhaiteraient y procéder, toutefois, ils n'ont pas forcément les moyens financiers nécessaires et la mettre en place s'avère difficile.

En complément des dispositifs scolaires, des associations se sont spécialisées dans une sensibilisation des dangers du Web auprès des jeunes et des parents afin d'apporter des clés et des prises de conscience. Face aux parents inquiets de l'utilisation des réseaux sociaux par leurs enfants, par méconnaissance de ce domaine, les associations comme e-Enfance viennent leur donner des ressources pour qu'ils sachent dans quel environnement leur progéniture évolue. Ces associations interviennent également dans les établissements scolaires, de l'école élémentaire au lycée. Il est important de sensibiliser dès le plus jeune âge afin que les enfants prennent de bons réflexes le plus tôt possible. Toutefois, s'il est intéressant et utile que de telles associations viennent faire de la sensibilisation dans les classes, celle ci ne produira aucun effet si aucun suivi en la matière n'est fait.

La prévention dans le cadre du système scolaire ou par des associations est très importante pour la protection du mineur. Toutefois, elle reste limitée et doit être complétée, en amont, par un travail de prévention de la part de la famille du mineur. Tout d'abord, cette prévention dans le milieu familial peut se faire par un dialogue entre le mineur et ses parents. Si les mineurs peuvent sembler à l'aise dans l'utilisation des réseaux sociaux, ils ne sont pas forcément connaisseurs de l'ensemble des risques. Il est crucial que les parents définissent des règles d'utilisation avec, par exemple, des horaires d'utilisation adaptés à l'âge de chacun. Puis, le contrôle parental, installé sur le matériel utilisé, peut être un complément dans l'optique de protéger le mineur et de le prévenir des dangers. Il permet aux parents de paramétrer le filtrage de contenus indésirables, mais également de contrôler ou restreindre l'utilisation d'internet et l'accès aux réseaux sociaux en limitant la durée horaire de connexion de l'enfant. C'est une façon de rendre l'enfant autonome. De plus, ce type de dispositif peut être un moyen pour les parents de bloquer l'accès à certains sites ou réseaux sociaux et peut s'installer sur tout type de périphérique connecté : ordinateur,

tablette ou téléphone portable. Cependant, il faut bien avoir conscience que le contrôle parental doit, uniquement, être considéré comme un outil d'aide dans l'éducation du mineur à l'utilisation d'internet et de ses services. Et ne pas perdre de vu qu'aucun logiciel ne peut assurer une sécurité totale car les enfants ont tendance à les contourner. La meilleure des sécurités reste donc le dialogue avec le mineur mais aussi l'encadrer dans son utilisation des réseaux sociaux. Enfin, afin que les parents ne soient pas dépassés par l'évolution des outils numériques, il est primordial qu'ils restent informés. Malgré la volonté et les efforts pour se tenir à jour, les parents se font quand même surprendre et distancer, parfois impuissants et néophytes face à l'usage intensif des réseaux sociaux par leurs enfants bien plus expérimentés qu'eux en la matière.

Aujourd'hui, faisant partie d'une société de l'information et de la communication en constante évolution, il est indispensable que les enjeux de la maîtrise du numérique et des technologies soient compris par les mineurs : d'une part pour leur protection et d'autre part pour leur intégration à la société comme futur citoyen. En définitive, et contre toute attente, la meilleure protection du mineur dans l'usage des réseaux sociaux reste lui-même. Son « éducation » numérique est indispensable et fera sa force. C'est en l'armant des bons outils qu'il réussira sa croisade dans les méandres du Web. Mais en la matière, beaucoup reste à faire.

BIBLIOGRAPHIE :

Ouvrages spéciaux :

- Conte , *La loi sur la prévention de la délinquance : présentation des dispositions de droit pénal*, Droit pénal 2007.
- Fauchoux V., Bruguière J-M. et Deprez P., *Le droit de l'internet, lois, contrats et usages* , 2e édition 2013, LexisNexis p. 7.
- Girard-Gaymard T., *Les influenceurs et le droit,* Recueil Dalloz 2020, p.92
- Manara C., *Réseaux sociaux : 101 questions juridiques* , Editions Diateino, septembre 2013, p.27
- Marino L., *Le droit d'accès à internet, nouveau droit fondamental* , Recueil Dalloz 2009, p.2045
- Nlend C., *La protection du mineur dans le cyberespace* , Editions Néressis, 12 août 2010

Articles :

- Ancel M-E, « *D'une diversité à l'autre* », Revue critique de droit international privé, 2019, p.647
- Bardin M., « *Le droit d'accès à internet : entre « choix de société »* et protection des droits existants » , RLDI 2013, n°91
- Beaumont O., « *Jean Castex face à nos lecteurs : « Il faut rétablir la confiance »* », Le parisien,15 juillet 2020
- Bensoussan A., « *Le « droit à l'oubli » sur internet* », Gaz. Pal. 6 février 2010, n°37, P.3
- Bigot C., « *Régulation des contenus de haine sur internet : retour sur le désaveu infligé par le Conseil constitutionnel à l'encontre de la loi dite « Avia »* », Recueil Dalloz 2020, p.1448
- Charrier B., « *Le consentement exprimé par les mineurs en ligne* », Dalloz IP/IT 2018 p.333
- Croquet P., « Une proposition de loi pour encadrer les activités des enfants youtubeurs et e-sportifs », Le monde 04 décembre 2019
- David R., « *Une proposition de loi pour encadrer les enfants influenceurs sur YouTube* », Europe 1, 6 décembre 2019
- Dirnhuber J., « *Children turn backs on traditional careers in favour of internet fame, study finds* », The Sun, mai 2017
- Fassi-Fihri R., « *Quel droit pour les réseaux sociaux ?* », Revue de droit public, n°3, 1er mai 2018 p.685
- Follain C., « *Cyberharcèlement : Twitter va vous permettre de choisir qui a le droit de réagir à vos posts* », LeMonde, 9 janvier 2020
- Foret O., « *Le droit à l'oubli des mineurs* », Dalloz IP/IT 2018, p.350
- Gargouri M., « *La protection du mineur fae aux dangers du cyberespace* », LegiTeam, lecture, Juillet 2019
- H.Meddah H., « *La France en première ligne pour règlementer le cyberespace* », LeMonde, 21 mars 2017
- Henno J., « *Comment décrocher les ados de leurs écrans ?* », LesEchos, 28 octobre 2019
- Labatut L., « *Harcèlement scolaire via internet et les médias sociaux : quels moyens de lutte ?* », LPA 23 déc. 2019, n°149p4, p.11
- Labatut T., « *L'exploitation des mineurs dans les médias sociaux : faut-il s'alerter ?* », Lextenso- Petites affiches – n°113- p.10
- Lasserre Capdeville J., « *Infraction commises à l'encontre de mineurs par l'intermédiaire d'Internet* », Gaz. Pal. 6 septembre 2012, p.12

- Lausson J., « *15 ans ou 16 ans ? Députés et sénateurs en désaccord sur la « majorité numérique »*. », Numerama, 14 mars 2018
- Le Maigat P., « *Revenge porn et cyber-harcèlement. Schizophrénie ou déconnexion du juge pénal ?* »,Gaz. Pal. 19 avril 2016, n° 262j4, p. 12.
- Leclair A., « *Le troublant phénomène des enfants stars sur YouTube* », Le Figaro, 30 juillet 2018
- Léger P., « *Le cyberharcèlement une infraction adaptée à la protection de la jeunesse en ligne* », Dalloz IP/IT 2018 p. 346
- Leloup D., « *Malgré les lois, l'Etat a abandonné aux réseaux sociaux l'arbitrage de la liberté d'expression* », Le Monde, 19 février 2020
- Leroux N., « *A-t-on le droit de publier des photos de ses enfants sur les réseaux sociaux ?* », avril 2019, Chronique
- Letesse V., « *Pourquoi créer une majorité numérique* ? », France culture, 8 février 2018
- Lobry K., « *Le consentement des mineurs sur internet : une vraie problématique pour les entreprises* », DPO, 29 octobre 2018
- Mariez J-S. et Godfrin L., « *Censure de la « loi Avia » par le Conseil constitutionnel : un fil rouge pour les législateurs français et européen ?* », Dalloz actualité, 29 juin 2020
- Mouron P., « *L'accès aux réseaux sociaux est un droit constitutionnel selon la Cour suprême des Etats-Unis* », Revue européenne des médias et du numérique, IREC, 2017, pp.62-64.
- Mouron P., « *L'accès aux réseaux sociaux est un droit constitutionnel selon la Cour suprême des Etats-Unis* », Revue européenne des médias et du numérique, IREC, 2017, pp.62-64
- Péron M., « *Libre propos sur le droit à l'oubli numérique* », RDLF2017, chron. n°15
- Planque J-C, « *La répression du « cyber-viol » : simple adaptation ou prémices d'une révolution des concepts pénaux ?* » , Droit pénal n°2, Février 2019
- Rassat M-L., « *Fait de favoriser la corruption d'un mineur* » : J.-Cl. pén., art. 227-22, fasc 20, 2008
- Renault A., « *Instagram, le réseau social favori des pédophiles* », Slate, publié le 8 mars 2019
- Robert AG., « *Délit de proposition sexuelles faites à un mineur de quinze ans par un moyen de communication électronique (loi n°2007-297 du 5 mars 2007)* », Dalloz RSC 2007 p.853, Chron.4
- Sirinelli P.et Prévost S., « *Réseaux… lument dangereux !* », Dalloz IP/IT, p.457
- Tambou O., « *Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déférencement* ». , RTD Eur. 2016, p.249
- Untersinger M. et Piquard A., « *La loi Avia contre la haine en ligne largement rétoquée par le Conseil constitutionnel* », LeMonde, 18 juin 2020
- Verge P., « *Qu'est-ce que la majorité numérique fixée à 15 ans en France ?* », Lefigaro, 9 février 2018

Lois, règlements et directives :

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée le 25 mai 2018
- Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance
- Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet

- Directive n° 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie venant remplacer la décision-cadre 2004/68/JAI du Conseil
- Loi n°2013-711 du 5 août 2013 portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France
- Loi n° 2014-873 du 4 août 2014 relative à l'égalité entre les femmes et les hommes
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
- Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes
- Loi n°2018-698 du 3 août 2018 relative à l'encadrement de l'utilisation du téléphone portable dans les établissements d'enseignement scolaire
- Loi n°2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

Jurisprudence :

- Civ.1ère, 8 janvier 1980, Bull.civ.I,n°18, D.1980.IR 258
- CCass, Civ.1re, 16 octobre 1984, n°83-11.786, Bull. civ. I, n°268
- CJUE, 2e chambre, Salvatore Grimaldi c/ Fonds des maladies professionnelles, 13 décembre 1989, n°322/88, Recueil de jurisprudence 1989, p.04407
- CCass. Crim. 1er février 1995, n°93-82578, Bull. crim., n°43
- CCass, Civ.2e, 5 mars 1997, n°95-14.503
- CE 8 février 1999, Dr.fam.1999, n°40, note Murat
- Civ. 1ère, 12 décembre 2000, n°98-21.311, X c/ Julien, Juris-Data n°2000-007309
- CA. Versailles, 11 septembre 2003
- Civ. 1ère, 21 mars 2006
- CCass. Crim. 11 septembre 2007, n°07-82018
- Décision n°2009-580 DC 10 juin 2009 du Conseil Constitutionnel
- CA. Aix-en-Provence, 26 oct. 2011, Juris-Data n°032852
- Décision n°2011-222 QPC du 17 février 2012 du Conseil Constitutionnel
- CA. Colmar, 29 mai 2012, n°12/00737 : Gaz. Pal. 2012.2.2701, note Lasserre Capdeville
- CEDH, 2e section, Ahmet Yildirim c/ Turquie, 18 décembre 2012, n°311/10
- CA Versailles, 31 janvier 2013, n° 11/03284, JurisData n° 2013-004990
- CA Aix-en-Provence, 10 septembre 2013, n°13-01400, Jurisdata 2013-024828
- CCass, Civ.1, décembre 2013, n° 12-26161
- CJUE, 13 mai 2014, « Google Spain SL, Google Inc./ Agencia Española de Protección de Datos, Mario Costeja González », C-131/12
- CA Versailles, 25 juin 2015, n°13-08349, JurisData n°2015-015861
- CCass. Crim. 8 février 2017, n°16-80102
- CA Paris, 9 février 2017, n°15-13956

- CE. 13 avril 2018
- Décision n°2020-801DC du 18 juin 2020 du Conseil constitutionnel

Avis et recommandations :

- Avis 5/2009 sur les réseaux sociaux en ligne, Groupe de travail « Article 29 » sur la protection des données, adopté le 12 juin 2009
- Recommandation n°2008/2160 du Parlement européen du 26 mars 2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet
- Recommandation de la CNIL - Délibération n° 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n°03 034 du 19 juin 2003
- Recommandation de la Commission des clauses abusives n°2014-02, 7 novembre 2014, relative aux contrats proposés par les fournisseurs de services de réseaux sociaux
- Recommandation du Forum des droits sur l'internet, « Les Enfants du Net (2): pédopornographie et pédophilie sur l'internet », 25 janvier 2005

ANNEXES

Entretien avec Michael Stora

Psychologue et psychanalyste, cofondateur de l'Observatoire des Mondes Numériques en Sciences Humaines

- **Quels sont les effets positifs et négatifs des réseaux sociaux pour le développement de l'enfant ?**

Effets positifs : les réseaux sociaux sont un amplificateur de la construction de l'image de soi qui est un moment important dans l'adolescence. Il s'est d'abord fait dans le cours de récréation, les soirées et avec l'apparition des réseaux sociaux plus précisément des blogs, cela a permis d'y contribuer. A travers les blogs, l'adolescent pouvait se mettre en scène sous diverses facettes et a permis une créativité. L'adolescence est une période de souffrance ainsi la part sombre, la part liée à la sexualité ou encore la part liée à la culture pouvaient se mettre en scène.
A l'époque, Skyrock proposait des outils très libres (photoshop…) cela permettait vraiment d'avoir un espace de mise en scène. Le réseau social était un espace de construction identitaire.
Avec l'avènement de Facebook et Instagram, la dimension négative est apparue par le fait qu'au fond, Facebook est née peu de temps après la télé réalité et c'est devenu un « internet réalité ». Même si les adolescents ne sont plus sur Facebook, Instagram propose une philosophie très emprunte d'une culture anglosaxone-américaine, c'est-à-dire, une culture de l'hyper positivité, de la performance, de la réussite et de la beauté. Finalement, la part la plus sombre n'avait pas à être citée. Sont apparus des adolescents qui suivaient sur Instagram des influenceuses et qui pouvaient déprimer, se sentir très mal à l'aise face à ces influenceurs.

- **Le droit à l'image des mineurs est exercé par les parents à partir de l'autorité parentale qui est en principe conjointe. Toutefois, il doit être exercé dans l'intérêt de l'enfant. Est-ce que l'exposition d'un enfant sur les réseaux sociaux est contraire à l'intérêt de l'enfant ?**

OUI. Pourquoi beaucoup de parents montrent leurs enfants ? C'est souvent inquiétant. L'enfant est fétichisé, c'est une sorte de trophée qui vient parfois valoriser le parent dans sa capacité d'être un parent présent, aimant et parfait. Tout cela est fait dans un faux semblant. Le lien entre un parent et un enfant doit être idéalement le plus authentique possible. Il n'y a pas besoin d'avoir d'images pour montrer à quel point on est un bon parent ou suffisamment bon.
Avec l'avènement de cette forme de téléréalité, certaines dérives sont apparues. Certains parents filmaient leur enfant au quotidien et diffusaient cela sur des chaînes YouTube avec un modèle économique très concret car les chaines font de millions de vus. L'enfant n'était plus un trophée mais une valeur marchande alors qu'il n'avait rien demandé. Cela peut avoir un impact sur la relation parent-enfant dans son authenticité et on peut imaginer qu'à l'adolescence, l'enfant porte plainte contre ses parents pour violation de son image. (Ex cas aux Etats Unis) C'est une bonne chose de montrer que lorsque l'on publie une photo de son enfant, on se doit de lui demander une autorisation au moins symbolique. Il y a une nécessité de légiférer. Pour les enfants mannequins ou acteurs, on est dans un cadre qui n'est pas celui de la famille, donc c'est très différent. On n'est pas un acteur au sein de sa famille, on est soi.

- **Interdire les rémunération partenariat avant un certain âge ? Evite la tentation des parents pour les collaborations.**

Il faudrait interdire ces chaines qui diffusent de manière régulières des épisodes sur le quotidien des enfants, de la famille. Certains ont tenté de le faire dans le cadre de documentaire, mais c'était différent. Cela était réalisé pour un but bien précis.
Lorsque les parents deviennent réalisateurs/ producteurs de l'intimité familiale, on est dans un faux semblant qui est assez pervers.

- **Comment un enfant peut se construire sainement lorsqu'ils se sentent observé ? Suivis par des milliers d'abonnés, ils sont loin des problématiques de cours de récréation.**

C'est complexe. On est dans une société où l'image est devenue un repère incontournable, comme une manière d'exister et de reconnaissance. Cela peut avoir un impact sur le fait que cela puisse d'un côté les gêner dans le fait où ils pourraient se dire : est-ce que l'on m'aime parce que j'ai de nombreux abonnés ou est-ce que l'on m'aime pour ce que je suis ?
C'est toute la problématique. C'est ce qui explique que les enfants ont des exigences de liens beaucoup plus authentiques. Ce n'est que bien plus tard, quand ils sont adultes, qu'ils peuvent découvrir l'hypocrisie sociale qui est parfois nécessaire lorsque l'on est des adultes. Toutefois, les enfants et d'autant plus les adolescents, sont dans cette exigence de liens le plus authentiques possibles. Si le nombre de likes, l'influence de l'enfant va faire que tout d'un coup les gens vont

l'aimer parce qu'il a des likes, cela va poser problème dans une sorte de relation en faux-self qui est une pathologie que les psychologues rencontrent dans les cabinets c'est-à-dire lorsque les parents projettent sur l'enfant quelque chose qu'il n'est pas ce qui peut donner avoir des problématiques, plus tard, d'un exhibitionnisme mortifère.
Ex : les jeunes actrices Disney lorsqu'elles deviennent majeures, elles ont un besoin de ternire et de choquer leur image. Elles veulent sortir de cette image très lisse et idéalisée, c'est une marque de souffrance.

- **Plus contrôler l'âge minimum – est-ce que ce n'est pas compliqué de contrôle l'âge minimum ? est-ce que cela ne peut pas entrainer un effet pervers en interdisant ? est-ce qu'il ne faudrait pas plutôt autoriser mais éduquer les parents et les enfants à l'utilisation de cet outil que sont les réseaux sociaux ?**

90% des français sont soucieux de ce que deviennent leurs données personnelles, mais ces 90% de français ne peuvent pas quitter les réseaux sociaux.
« Facebook c'est comme ta mère, tu as envie de la quitter, mais tu n'y arrive toujours pas. ». En gros, on est pris dans une sorte de lien où le réseau social est un espace maternant, on se sent moins seul. En réalité, ce que l'on publie sur Facebook ou Instagram est rarement en lien avec la réalité car les gens publient des clichés de moments où tout va bien. C'est souvent du fake. Les données que l'on va avoir ce n'est pas forcément par rapport à ce que l'on publie, mais c'est par rapport aux like. Le scandal cambridge analytica a montré que l'on sait des choses sur nous, surtout par rapport à ce que l'on like. Il faudrait une éducation afin que les gens comprennent de quoi il s'agit. Puis, la génération Z est une génération qui est beaucoup plus réaliste que la génération milléniale car elle a grandi avec les réseaux sociaux. Au collège, dans les cours d'éducation civique et morale, tous les profs montrent aux élèves comment il est important de faire attention à ce que l'on publie. Toutefois, ce n'est pas la seule éducation civique qu'il faudrait avoir. Concernant la e-réputation, c'est très compliqué. L'encadrement juridique qui est entrain de se construire au niveau international permettra que le sentiment de liberté existe réellement. Souvent, au nom de la liberté d'expression, on a fait tout et n'importe quoi. La liberté existe uniquement parce qu'il y a un cadre. Plus ce cadre sera forgé, plus il sera possible d'évoquer ce que l'on pense. Toutefois, les algorithmes sont là pour nous protéger, mais malheureusement, ils nous enferment. Rien ne vaut la différence, hors sur les réseaux on nous propose que des gens qui ont les mêmes points de vus.

Entretien avec Monsieur Jacques Henno

Journaliste, auteur et conférencier, spécialiste des nouvelles technologies.

- **La majorité numérique instaurée par le RGPD afin d'apporter une protection pour les mineurs est-elle réelle efficace ?**

Cette protection est totalement illusoire. Avant la mise en place du RGPD et de la majorité numérique, la plupart des réseaux sociaux refusaient l'inscription des mineurs de moins de 13 ans. La majorité étant américains, ils sont soumis au Children's Online Privacy Protection Act (COPPA) qui est un texte qui oblige tout site internet qui utilisait les données des enfants de moins de 13 ans à recueillir l'autorisation écrite des parents. Cette démarche étant extrêmement compliquée à mettre en place, une grande partie des réseaux sociaux refusait l'inscription des mineurs de moins de 13 ans. Toutefois, malgré le COPPA, il y avait déjà énormément d'enfants de moins de 13 ans qui s'inscrivaient et mentaient sur leur âge. Par conséquent, le RGPD et la mise en place d'une majorité n'a strictement rien changé. A partir du moment où il n'y a pas d'obligation de contrôle ou de système déclaratif de l'âge, c'est extrêmement compliqué de vérifier l'âge d'une personne sur internet.

- **Comment s'assurer de l'âge effectif des mineurs ou le consentement du titulaire de l'autorité parentale lors de l'inscription sur un réseau social ?**

Pour l'instant aucun Etat n'est parvenu à vérifier le véritable âge de l'utilisateur. En Belgique, il était question de doter tous les citoyens d'une carte d'identité numérique, d'une « e-carte d'identité ». En France, il y a également eu un vague projet similaire. Le problème est que sa mise en place est compliquée car il faudrait un lecteur de carte, mais également que tous les enfants soient dotés d'une carte d'identité. Or, en France ce n'est pas obligatoire d'avoir une carte d'identité. Ce contrôle à partir d'une e-carte d'identité serait extrêmement compliqué en pratique car un enfant qui souhaite s'inscrire sur un réseau social et en âge de le faire, mais qui n'a pas de carte d'identité ne pourra pas le prouver.
Ce contrôle de l'âge sur internet est un vieux problème. En 2005, lors d'une conférence de la famille qui avait pour thème « les mineurs face à la pornographie », cette problématique de vérification de l'âge et de s'assurer qu'un enfant ne puisse pas accéder à un site pornographique avait déjà été soulevé.

Dans les faits, un tiers des enfants ont un smartphone et vont sur les réseaux sociaux. Facebook disait qu'ils ferment régulièrement des comptes d'enfants de moins de 13 ans.

- **Sur les réseaux sociaux, les mineurs sont-ils protégés du contenu violent parfois présent sur internet ?**

Tous les contenus violents, pornographiques etc… sont filtrés par les plateformes elles-mêmes. Il y a beaucoup de modérateurs qui sont mis en place et on ne voit pas beaucoup de contenus violents sur les réseaux sociaux même si les contrôles sont extrêmement compliqués. Le vrai problème ce sont les « fake news ».

- **La prévention des mineurs sur les dangers de l'utilisation des réseaux sociaux est-elle essentielle pour leur permettre de bénéficier d'une bonne protection ? Et qu'en est-il de la place qui lui est accordée en France ?**

Je fais de la prévention dans les écoles, tout comme certaines associations spécialisées ou des spécialistes qui en font à titre individuel. Il y a des choses qui sont mises en place. Toutefois, tous les collèges et lycées ne bénéficient pas de prévention de l'usage du numérique et des réseaux sociaux. Il y a donc une inégalité entre les élèves. Il faudrait peut-être voir pour rendre cette prévention obligatoire et faire partie du programme scolaire. Parfois, dans certains établissements, le professeur de technologie ou bien le professeur de français ou le responsable du centre de documentation et d'information font des choses. Cette prévention peut donc être assurée par une personne de l'établissement ou une personne extérieure. Il y a beaucoup de choses qui se font : certains établissements demandent aux élèves de devenir eux-mêmes ambassadeurs de leur protection, il y a un programme au niveau européen etc…Toutefois, il est impossible de savoir si tous les élèves sont concernés.

- **Sur le travail des mineurs à travers les réseaux sociaux – chaîne YouTube – projet de loi de Bruno Studer?**

Il faudrait encadrer cette pratique. Pourquoi pas reprendre le cadre mis en place pour les enfants acteurs. Par exemple, bloquer l'argent sur un compte auquel ils peuvent accéder à leur majorité même si les parents ont plus ou moins la gérance.

- **<u>Est-ce que selon vous la protection du mineur est assurée à l'aune des réseaux sociaux ?</u>**

Non, comme écrit dans l'article « Comment décrocher les ados de leurs écrans ? », au retour d'un voyage d'étude aux Etats-Unis dans la Sillicon Valley et après avoir interviewé des spécialistes sur l'impact des réseaux sociaux sur les enfants, pré-adolescents et adolescent, pour beaucoup d'entre eux, les réseaux sociaux devraient être assujettis à une réglementation particulière des lors qu'ils s'adressent à des mineurs pour qu'ils n'utilisent pas les mêmes outils de captation de l'attention. Les outils qu'ils utilisent déjà pour les adultes pourront toujours être utilisés, mais vis à vis des enfants il faudrait des outils totalement différents. Par exemple, peut être s'assurer que les enfants ne passent pas autant de temps sur les réseaux sociaux, c'est-à-dire qu'ils aient le droit à un certain laps de temps ou bien, que les enfants soient prévenus du caractère addictif des réseaux sociaux et que les astuces utilisées leur soient bien expliquées etc… Beaucoup de choses pourraient être mises en place et cela irait dans le bon sens. Aujourd'hui, le grand danger pour les mineurs c'est qu'ils sont extrêmement influençables au regard des autres, en particulier les pré-adolescents. Les mineurs passent énormément de temps et prennent de mauvaises habitudes de consommation sur les réseaux sociaux. Au vu du temps qu'ils passent dessus, les réseaux sociaux vont être mis en concurrence avec le travail scolaire, la vie famille, les sorties entre amis. Il est donc essentiel qu'une réglementation extrêmement rigoureuse soit mise en place. La prévention est très importe, mais il faudrait également qu'il y ait des contraintes très fortes sur les réseaux sociaux eux-mêmes qui se croient clairement au dessus des lois. Ce qui n'est pas souvent évoqué et qui est tabou c'est la pression commerciale et publicitaire de la part des réseaux sociaux sur les journaux européens ou américains. Par exemple, des pages énormes de publicité de la part de Google sur le contrôle parental, qui en pratique ne fonctionne pas si bien que cela. En Europe ou aux Etats-Unis, il y a beaucoup de journaux qui sont « à la botte » des réseaux sociaux parce qu'ils espèrent qu'une chose c'est d'avoir un cachet publicitaire de la part de ces plateformes. De plus, pour de nombreux réseaux sociaux, les mineurs sont leur cible marketing et par conséquent, ils ne respectent pas certaines contraintes. Aujourd'hui nous sommes dans un capitalisme de l'attention, une nouvelle forme de capitalisme, il faut donc de nouvelles contraintes. Surtout pour protéger les plus jeunes. D'ailleurs, il faudrait peut-être voir pour étendre cette protection car les dégâts délétères de ces réseaux sociaux apparaissent sur les mineurs mais également sur les jeunes adultes. Il ne faut pas sous estimer les contraintes techniques que rencontrent les réseaux sociaux.

Entretien avec un coordinateur pédagogique de l'association e-Enfance

- **Comment se passe les journées de sensibilisation que pour faites auprès des jeunes/ parents/ professionnels concernant l'utilisation des réseaux sociaux ?**

Chez e-Enfance il y a deux pôles de travail. Le premier pôle est un pôle intervention qui présente plusieurs modules. Le premier, les interventions dans les établissements dès la primaire (dès le CE2) jusqu'à la terminale dans les établissements. Le second, les conférences professionnelles pour tout type de professionnels qu'en font la demande (dans le médical, des mairies, des enseignants, des éducateurs…). Le troisième, les conférences pour les parents. Le quatrième est spécifique aux 17-30 ans, qui est une tranche d'âge qui utilise beaucoup internet et qui a l'impression d'être sachant alors que parfois elle ne l'utilise pas de la bonne manière. L'association intervient sans jugement de valeur, elle est là pour faire de la prévention et à aucun moment elle dit : « il faut agir de cette manière, c'est la bonne solution ». L'association apporte des clés et des prises de conscience.

- **Est-ce que les parents inquiets de l'utilisation des réseaux sociaux par les jeunes ?**

Ils ne sont pas forcément inquiets de l'utilisation à proprement parlé. Ils sont inquiets car ils n'y connaissent pas beaucoup de choses. Le fait d'être dans l'ignorance c'est compliqué. L'association vient donner des ressources aux parents afin qu'ils sachent dans quel environnement leurs enfants évoluent : que ce soit autour des réseaux sociaux, des jeux vidéos, de la protection des données personnelles, de l'e-réputation sur Internet etc… Avec les parents, l'association mêle à la fois contenu théorique et débats éducatifs.

- **La prévention a commencé à être intégrée dans les programmes scolaires (B2i, la plateforme PIX, l'EMI), mais cette sensibilisation est basée sur l'utilisation des nouvelles technologies pour la recherche d'information et pas forcément pour une utilisation privée comme celle des réseaux sociaux. Est-ce qu'il faudrait amener plus de prévention dans les programmes solaires et dans les écoles ?**

C'est une bonne question et c'est très compliqué d'y répondre. Le problème est qu'il y a tout un enjeux politique et économique qui s'y mêle. Comment fait-on cette prévention ? Qui va la faire ? C'est compliqué de la mettre en place (suivant les zones géographiques, suivant les dénominations des établissements). Puis, il y a beaucoup d'établissements qui souhaiteraient la faire mais qui

n'ont pas forcément les moyens de la faire. L'association e-Enfance aimerait que tous les enfants de France aient accès à la prévention. L'association travaille dès l'école primaire car c'est dès cet âge là que les bons réflexes se prennent.

- **La prévention faite à ce jour est-elle suffisante ou faut-il lui accorder une place plus importante ?**

La prévention est là mais le problème c'est sa mise en place et sa régularité. Le problème est que venir faire une sensibilisation dans une classe c'est très intéressant mais si derrière il n'y a rien qui se fait, ce sera de la poudre aux yeux. La prévention ne cherche pas à avoir un résultat direct, c'est sur le long terme qu'elle se voit.

- **Combien d'enfants avez-vous rencontré en 2019 ?**

En 2019, il y a eu 105 000 personnes sensibilisées en France, plus de 5 000 interventions et 97% d'établissements satisfaits. Sur la ligne Net Ecoute, numéro vert dont l'association e-Enfance est gestionnaire, c'est plus de 10 000 appels à l'année et c'est en constante augmentation tous les ans.

TABLE DES MATIERES :

REMERCIEMENTS : .....

TABLES DES ABREVIATIONS : .....

SOMMAIRE : .....

INTRODUCTION : 1

CHAPITRE I : LA PROTECTION AVEREE DU MINEUR SUR LES RESEAUX SOCIAUX 8

SECTION 1 : LE RESPECT DES DROITS FONDAMENTAUX DU MINEUR DANS L'UTILISATION DES RESEAUX SOCIAUX 8

Paragraphe 1 : L'exercice du droit à la liberté d'expression par l'accès aux réseaux sociaux . 9

A) Du droit d'accès à Internet au droit d'accès aux réseaux sociaux 9

B) L'exercice du droit à la liberté d'expression sur les réseaux sociaux 13

Paragraphe 2 : La protection du droit à la vie privée et du droit à l'image sur les réseaux sociaux 16

A) La protection du droit à la vie privée par la protection des données à caractère personnel 16

B) La protection du droit à l'image par le double consentement des titulaires de l'autorité parentale 20

SECTION 2 : LA LUTTE CONTRE LA CYBERCRIMINALITE ENVERS LE MINEUR SUR LES RESEAUX SOCIAUX 23

Paragraphe 1 : Le cyberharcèlement 23

A) L'encadrement du cyberharcèlement corollaire du harcèlement scolaire 23

B) La mise en place d'outils pour lutter contre le cyberharcèlement 26

Paragraphe 2 : Le grooming 29

A) La création d'une infraction propre pour un acte préparatoire 29

B) Les préliminaires à la commission d'infractions plus graves 33

CHAPITRE II : LA PROTECTION LIMITEE DU MINEUR SUR LES RESEAUX SOCIAUX 38

SECTION 1 : LA MAJORITE NUMERIQUE : UNE PROTECTION HYPOCRITE DU MINEUR .. 38

Paragraphe 1 : L'apparence protectrice de la majorité numérique 39

A) La notion de majorité numérique 39

B) Une double limite d'âge pour l'inscription du mineur sur un réseau social 42

Paragraphe 2 : L'inefficacité de la majorité numérique 44

A) Une protection illusoire du mineur par l'absence de contrôle d'âge 44

B) Une protection inégale des mineurs européens 47

SECTION 2 : LA PROTECTION DU MINEUR SUREXPOSE : ENJEU LEGISLATIF ET PREVENTIF 50
Paragraphe 1 : Une surexposition à l'encontre de l'intérêt du mineur 50
A) Les dangers de publications massives d'images d'un mineur par ses représentants légaux 50
B) Le travail des enfants sur les réseaux sociaux non encadré 53
Paragraphe 2 : La révision du cadre législatif et préventif pour une meilleure protection 58
A) Le droit du cyberespace : un droit 3.0 58
B) La nécessité de mieux sensibiliser pour mieux protéger 60
BIBLIOGRAPHIE : 64
ANNEXES 68