
La protection (des données à caractère personnel) du mineur protégé. Analyse comparative du RGPD. Étude de la Directive 2018/1808 du 2 octobre 2018 relative à la fourniture de services de médias audiovisuels (Directive "Services de médias audiovisuels"), compte tenu de l'évolution des réalités du marché

Auteur : Moreau, Gladys

Promoteur(s) : Van Cleynenbreugel, Pieter

Faculté : Faculté de Droit, de Science Politique et de Criminologie

Diplôme : Master en droit, à finalité spécialisée en mobilité interuniversitaire

Année académique : 2020-2021

URI/URL : <http://hdl.handle.net/2268.2/12094>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

« La protection des données à caractère personnel du mineur protégé. Analyse comparative du RGPD. Étude de la Directive 2018/1808 du 2 octobre 2018 relative à la fourniture de services de médias audiovisuels (Directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché. »

Gladys MOREAU

Travail de fin d'études
Master en droit à finalité spécialisée interuniversitaire
Année académique 2020-2021

Recherche menée sous la direction de :
Monsieur Pieter VAN CLEYNENBREUGEL
Professeur

RESUME DU TRAVAIL

Les mineurs ont-ils conscience des tenants et aboutissants de leurs pratiques numériques ? Sont-ils conscients des traces qu'ils laissent sur Internet ?

Au coeur du régime de la protection des données en droit européen, le consentement est défini comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

À priori, le traitement des données d'un mineur devrait remplir les mêmes conditions que pour tout traitement. Cependant, sur les six bases légales prévues par le « **Règlement Général sur la Protection des Données** », deux connaissent des aménagements lorsque la donnée traitée concerne un mineur.

Par conséquent, la vulnérabilité des mineurs suppose, lorsqu'une mise en balance est faite entre leurs intérêts et les intérêts légitimes du responsable de traitement, que ce soit toujours les intérêts des mineurs qui priment.

Lorsque la personne concernée est alors mineure au moment de la collecte des données, celle-ci est tout à fait en mesure d'obtenir l'effacement de ses données dans les meilleurs délais.

La nouvelle « **Directive sur les services de médias audiovisuels** » va entraîner d'importantes modifications sur cette matière. Cette Directive détermine le socle minimal de règles applicables dans tous les Etats membres de l'Union européenne aux services audiovisuels. Elle promeut la diversité culturelle et régit notamment la publicité, le placement produit et la protection des mineurs. Les plateformes de partage de vidéos seront également soumises à des règles visant à assurer que les spectateurs, et en particulier les mineurs, soient mieux protégés contre les contenus violents ou préjudiciables ou les discours de haine.

Dans le cadre de ce travail de fin d'études, nous comparerons la situation d'un majeur et d'un mineur sous la protection de leurs données personnelles au niveau de l'Union européenne, et nous nous poserons la question de savoir, s'il n'y a-t-il pas un manque de cohérence entre ces deux instruments européens.

REMERCIEMENTS

Fruit de plusieurs mois de travail, plusieurs personnes ont contribué à la réalisation de ce travail de fin d'études.

Tout d'abord, je souhaiterais remercier mon promoteur, le Professeur VAN CLEYNENBREUGEL pour avoir suscité mon intérêt dans le domaine du Droit européen, notamment à travers le cours de « *Droit matériel européen* » et plus particulièrement, à travers les cours de mon master en droit, « *Advanced european law* » et « *European competition law* ». Je le remercie également pour sa disponibilité et pour ses précieux conseils.

Je tiens également à témoigner ma reconnaissance à mon entourage pour leur assistance tout au long de ces études.

Enfin, j'adresse mes sincères remerciements à ma mère et à ma grand-mère pour leur soutien inconditionnel tout au long de ce parcours universitaire, ainsi que pour les nombreuses relectures de mes travaux universitaires et, en particulier, celui-ci.

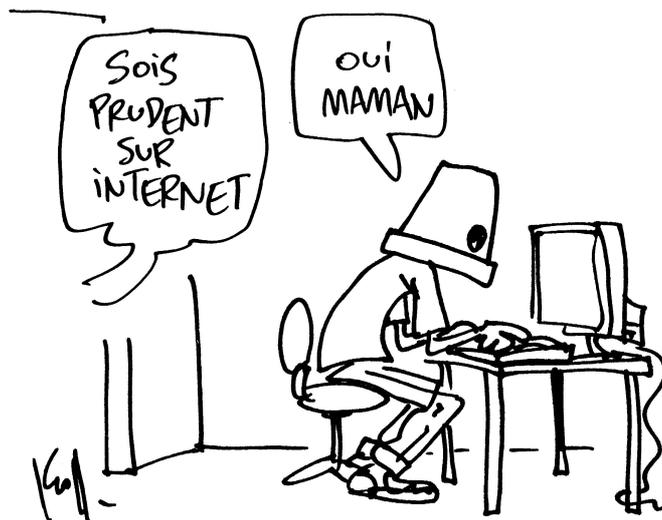


TABLE DES MATIERES

Introduction 10

TITRE 1 : La protection des données personnelles 13

A. Le cadre juridique de la protection des données personnelles 13

Chapitre 1 : Règlement Général sur la Protection des Données 13

Chapitre 2 : Notions préalables 14

Chapitre 3 : Objectifs 15

Chapitre 4 : Principes clés du RGPD 18

A. Le consentement 19

B. La transparence 21

C. La responsabilité 22

B. Une protection spécifique des enfants 23

Chapitre 1 : Les raisons d'une telle protection 23

Chapitre 2 : La protection juridique des données des enfants 24

1. La protection offerte par les Conventions internationales et régionales 25

2. La protection offerte à l'échelle de l'Union européenne 26

2.1 La Charte des droits fondamentaux de l'Union européenne 26

2.2 Le RGPD 28

a. Les services de la société de l'information 28

b. La notion d'« enfant » 30

c. La vulnérabilité de l'enfant 30

d. Le consentement comme base de traitement des données à caractère personnel 31

e. L'âge du consentement 32

f. La responsabilité parentale 33

g. Le principe de la transparence 34

h. Le principe de responsabilité de l'enfant - une faiblesse du RGPD 34

Chapitre 3 : Enquêtes en Europe : le réseau social « Tik Tok ». 35

Chapitre 4 : Tableau récapitulatif : majeur / mineur - RGPD 36

C. Les droits subjectifs 38

Chapitre 1 : La notion d'oubli 39

Chapitre 2 : L'infailibilité de la mémoire d'Internet 40

Chapitre 3 : La protection spécifique des mineurs d'âge 40

TITRE 2 : Directive 2018/1808 du 2 octobre 2018 relative à la fourniture de services de médias audiovisuels (Directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché 41

Chapitre 1 : Définitions et objectif 41

Chapitre 2 : La priorité de la nouvelle Directive : la protection des mineurs 44

TITRE 3 : Un manque de cohérence entre d'une part, le RGPD et d'autre part, la

Directive SMA ? 45

Chapitre 1 : Les objectifs 45

Chapitre 2 : Le règlement ou la directive 46

Chapitre 3 : Une complémentarité 48

Chapitre 4 : Un avenir numérique pour l'Europe 49

Conclusion générale 52

Bibliographie 54

Législation 54

Jurisprudence 57

Doctrine 58

Introduction

« *Tout ce qui augmente la liberté augmente la responsabilité* », disait Victor Hugo².

L'importance des flux internationaux des données à caractère personnel est hors de doute. Avec la mondialisation de l'économie et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données à caractère personnel ne cesse de croître³.

Le marché mondial du numérique est aujourd'hui dominé par les GAFA⁴ et l'Union européenne doit résoudre un conflit entre, d'une part, la protection des données personnelles et, d'autre part, la promotion d'une logique de marché intérieur numérique qui postule la liberté du commerce des données⁵.

Les sites et réseaux sociaux ne sont pas les seuls lieux d'échange et de collecte des données personnelles de nos enfants. Les téléphones, avec la multitude d'applications et services connectés téléchargés ainsi que la géolocalisation, sont une inépuisable source pour tracer tant de données, telles que les données de localisation ; les déplacements ; les données de carte de crédit ; les achats effectués en ligne ; les centres d'intérêts ; et bien d'autres encore. Ces données sont ensuite stockées pouvant être détournées et utilisées à mauvais escient⁶.

A l'heure actuelle, qui n'utilise pas l'un ou l'autre réseau social, que ce soit Facebook, Instagram, Twitter ou d'autres ? Ces réseaux sociaux fascinent autant qu'ils inquiètent, tout particulièrement dans leur rapport avec la vie privée. Ainsi, rares sont les écrits évoquant le sujet qui ne citent Orwell et l'emblématique « *Big brother is watching you* »⁷.

Depuis plusieurs années, le traitement des données personnelles a changé d'échelle pour devenir un phénomène de masse, à l'échelle de la planète entière, tant du point de vue de la quantité que de la diversité des données produites qui peuvent être collectées et traitées.

Cette nécessité de protéger les données personnelles récoltées sur internet n'est pas une nouveauté car il existait auparavant, une directive européenne qui allait dans ce sens. Le

² C. FÉRAL-SCHUHL, « Comment les droits de la personne concernée sont-ils renforcés ? », in *Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2015, pp. 221-222.

³ M. GALLARDO MESEGUER, « Aperçu de la dimension internationale du règlement général sur la protection des données à caractère personnel », in *Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2015, p. 117.

⁴ Google, Apple, Facebook et Amazon.

⁵ C. BARREAU, « Le marché unique numérique et la régulation des données personnelles », *Réalités industrielles*, 2016, n° 3, pp. 37-41.

⁶ A. CARRÉ, sous la supervision de G. MATHIEU et B. VAN KEIRSBILCK
Défense des enfants internationale Belgique, « La protection des données des enfants dans le monde numérique », outil pédagogique n°2018-07, décembre 2018, p.5 (disponible sur : <https://www.dei-belgique.be/index.php/component/jdownloads/send/46-la-protection-des-donnees/389-la-protection-des-donnees-des-enfants-dans-la-monde-numerique.html>).

⁷ L. PAILLER et F. MARCHADIER, « Les réseaux sociaux sur Internet et le droit au respect de la vie privée », Bruxelles, Larcier, 2012, p. 5.

principal acte juridique de l'UE en matière de protection des données était la 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. Elle a été adoptée en 1995, date à laquelle plusieurs États membres avaient déjà adopté des lois nationales sur la protection des données. La libre circulation des marchandises, des capitaux et des personnes au sein du marché interne requérait la libre circulation des données, celle-ci ne pouvait être réalisée qu'à condition que les États membres puissent s'appuyer sur un niveau uniforme élevé de protection des données⁸.

Cependant, le besoin d'une mise à jour à la lumière de l'essor du numérique se faisait ressentir. Compte tenu de la rapidité des développements technologiques, l'UE a adopté une nouvelle législation en 2016 afin d'adapter les règles relatives à la protection des données à l'ère du numérique. Il était donc souhaitable que l'Union européenne s'adapte aux évolutions technologiques, ce qui a été fait à la suite de l'adoption du Règlement général sur la protection des données, le RGPD⁹.

Le mineur, de par son jeune âge et son inexpérience, est généralement perçu comme une personne vulnérable. Son immaturité physique, économique et psychologique justifie de le protéger de ses propres faiblesses ainsi que de la possible malveillance des autres¹⁰. Cette vulnérabilité se renforce dans l'environnement numérique. Toutefois, même si le mineur est généralement à l'aise avec les nouvelles technologies et dispose le plus souvent d'un téléphone facilitant l'accès à internet, les dangers d'internet pour les plus jeunes sont très souvent mis en avant.

Pour protéger ces mineurs et cette vulnérabilité, le RGPD se veut soucieux de cette problématique et met en place un régime spécifique de protection de données personnelles.

La protection des données personnelles est une chose mais l'audiovisuel en est une autre pour l'Union européenne. Les mineurs étant de plus en plus attirés par du contenu audiovisuel, il était préférable de les protéger sur ce point. La Commission a présenté une mise à jour des dispositions de la Directive SMA pour dégager un meilleur équilibre des règles qui s'appliquent aux organismes traditionnels de radiodiffusion, aux fournisseurs de vidéos à la demande et aux plateformes de partage de vidéos, notamment lorsqu'il s'agit de protéger les enfants.

* * *

A travers ce travail, nous analyserons le système en vigueur de la protection des données personnelles : quel est l'objectif poursuivi par le Règlement Général sur la Protection des Données ? Quels en sont les principes clés ? Quels sont les droits qui y sont repris ?

⁸ GIAKOUMOPOULOS, G., BUTTARELLI, G., O'FLAHERTY, M., « Manuel de droit européen en matière de protection des données », Luxembourg, 2019, p.33.

⁹ Publications Office of the EU, *op. cit.*, p.20.

¹⁰ A. NOTTET, « Le consommateur mineur », *R.G.D.C.*, 2014, p. 40

Ensuite, nous nous concentrerons sur le cadre juridique de la protection spécifique des mineurs dans le cadre de la protection de leurs données personnelles, de manière général, à l'international et à l'Europe.

En outre, nous analyserons plus en détail la manière dont le Règlement Général sur la Protection des Données gère cette protection spécifique des mineurs.

Enfin, nous nous intéresserons à la nouvelle Directive sur les services de médias audiovisuels qui a pour objectif de moderniser le cadre juridique du secteur audiovisuel européen avec intérêt majeur, la protection des mineurs.

Tout au long de cette étude, nous nous consacrerons à ces deux questions : *Comment la protection des mineurs sera-t-elle assurée au niveau de l'UE ? Y a-t-il un manque de cohérence entre les deux instruments européens, ci après, RGPD et Directive SMA ?*

TITRE 1 : La protection des données personnelles

A. Le cadre juridique de la protection des données personnelles

Chapitre 1 : Règlement Général sur la Protection des Données

L'Union européenne n'est certes pas démunie d'instruments de protection, mais force est de constater que les limites du droit positif étaient totalement dépassés en raison d'un faible degré d'harmonisation et de l'avènement du numérique¹¹.

Pendant près de 15 ans, la directive 95/46/CE¹² s'est imposée comme l'instrument central de la réglementation en matière de protection des données dans l'UE. La Commission européenne a évalué sa mise en œuvre en 2003 et 2007, concluant les deux fois qu'il n'y avait pas besoin de révisions. En 2010¹³, cependant, la Commission a annoncé que le moment des révisions était venu¹⁴.

Depuis l'adoption de cette directive, les évolutions technologiques qu'ont connues nos sociétés ont été considérables. L'avènement des réseaux sociaux a ainsi profondément modifié nos rapports interpersonnels et notre conception du vivre ensemble. Étant toujours plus connectés, nous diffusons allègrement des informations nous concernant à qui le veut, qu'il s'agisse de proches ou d'inconnus vivant aux antipodes.

Dans un environnement de numérisation massive et systématique des données, la directive s'avérait totalement inadaptée à la monétisation de la donnée personnelle par les géants de l'internet, peu soucieux de respecter les droits et libertés fondamentales des individus¹⁵.

Il s'est donc avéré indispensable de mettre à jour les droits de la personne concernée, qui sont un des piliers de notre système européen de protection des données, en vue de rester en phase avec cette évolution¹⁶.

¹¹ C. CASTETS-RENARD, A. STROWEL, et I. DE LAMBERTERIE, I. DE, « Quelle protection des données personnelles en Europe ? », Bruxelles, Larcier, 2015, p.25.

¹² 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, *J.O.C.E.*, L 281/31, 23 novembre 1995 ; ci-après, la *Directive*.

Ce texte a été, à de multiples reprises, complétés par divers textes communautaires, notamment en 2002 par la directive 2002/58/CE du 12 juillet 2002 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques, appelée la directive vie privée et communications électroniques.

¹³ La consultation publique sur «l'approche globale de la Commission en matière de protection des données à caractère personnel dans l'Union européenne» s'est déroulée du 4 novembre 2010 au 15 janvier 2011. Pour un résumé des contributions reçues, voir l'annexe 4 de l'analyse d'impact de la Commission accompagnant sa proposition initiale pour les données générales Règlement sur la protection, p. 54–73.

¹⁴ B. VAN ALSENOY, *Data protection law in the EU : roles, responsibilities and liability*, Cambridge, Intersentia, 2019.

¹⁵ C. CASTETS-RENARD, A. STROWEL, et I. DE LAMBERTERIE, I. DE, *op. cit.*, p.26.

¹⁶ T. TOMBAL, « Les droits de la personne concernée dans le RGPD », in *Les droits de la personne concernée dans le RGPD*, s.l., Larcier, 2018, p. 407.

Pour répondre à ces évolutions numériques, l'Union européenne s'est dotée d'un nouveau cadre juridique en matière de protection des données à caractère personnel. Le législateur européen a considéré que la directive 95/46/CE nécessitait une mise à jour car cette dernière avait été transposée différemment par les pays de l'Union Européenne.

En 2016, l'Union européenne a adopté le Règlement n° 2016/679 « *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* », désigné sous les termes de Règlement Général sur la Protection des Données (« RGPD »)¹⁷. Il aura fallu plus de 4 années de négociations, quelques 3 999 amendements entre la version initiale de 2012 et celle du Parlement européen de 2014 pour aboutir à un texte comprenant 173 considérants explicitant pas moins de 98 articles.

Ce Règlement est entièrement et directement applicable par les Etats membres de l'Union européenne dans leur propre système juridique depuis le 25 mai 2018, au même titre que les lois et autres textes adoptés par leurs autorités nationales respectives. Il est donc également entré en vigueur en Belgique à cette date et a été intégré à l'ensemble des lois et textes belges, même s'il a été complété depuis par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Le RGPD doit être respecté par tous en Belgique et peut être invoqué devant les tribunaux belges.

Ce texte marque la volonté d'une harmonisation au niveau européen. Le RGPD vise à renforcer les droits des citoyens européens mais aussi à responsabiliser les entreprises et organismes traitant des données à caractère personnel¹⁸.

Par ailleurs, pour assurer son application, le Règlement met en place des autorités de contrôle indépendantes dans chaque Etat membre, qui ont d'importants pouvoirs de conseil, d'enquête, de sanction, et qui forment entre elles un réseau supervisé par le Comité européen de la protection des données. La Belgique a décidé d'étendre les pouvoirs de la Commission de la Protection de la Vie Privée pour remplir ces missions. La Commission a pris le nom d'Autorité de protection des données.

Enfin, le RGPD s'applique partout dans l'Union européenne dès lors que les données concernées sont celles d'un citoyen européen, quelle que soit la localisation du site ou de l'application utilisée. Ceci est évidemment capital dans le contexte d'internationalisation du monde numérique.

Chapitre 2 : Notions préalables

¹⁷ Le règlement général sur la protection des données (RGPD) est une loi européenne qui régit le traitement des données à caractère personnel dans tous les États membres de l'UE. Le RGPD exige que les sites web, les entreprises et les organisations demandent et obtiennent le consentement explicite des utilisateurs avant de traiter des données à caractère personnel, par exemple par le biais de cookies et de traceurs sur un site web.

¹⁸ S. M'HAMDI, « "RGPD" : quelle protection pour vos données personnelles ? », Institut national de la consommation (INC), 10 octobre 2019 (disponible sur : <https://www.inc-conso.fr/content/rgpd-quelle-protection-pour-vos-donnees-personnelles>).

À titre préliminaire, il est pertinent de définir quelques notions du RGPD. Concernant les concepts élémentaires, les auteurs du RGPD ont recouru dans l'ensemble à ceux de l'ancienne Directive :

- La donnée à caractère personnel est définie comme « *toute information se rapportant à une personne physique identifiée ou identifiable* »¹⁹ par exemple : noms et prénoms, identifiants, numéros d'identification, téléphones, emails, données comportementales dès lors qu'elles peuvent être rattachées à un individu. Ce sont toutes les informations qui se rapportent à une personne, adulte ou enfant. Il s'agit également de toutes les traces laissées par une personne sous une forme ou une autre, à chaque fois qu'elle entre en contact avec le monde numérique ;
- Le traitement est « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel (...)* »²⁰. Ce sont toutes les opérations ou les suites d'opérations qui peuvent être effectuées sur les données à caractère personnel. Il s'agit par exemple de les collecter, les enregistrer, les classer, les structurer, les utiliser, les diffuser, les vendre, les effacer, les modifier, etc. La liste n'est encore une fois pas exhaustive ;
- Le responsable de traitement est la personne « *qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »²¹.
- Concernant les personnes concernées par ces traitements, le RGPD indique qu'il doit s'agir « *de données qui se rapportent à une personne physique vivante identifiée ou identifiable* »²².

Chapitre 3 : Objectifs

La Cour de justice de l'Union européenne rappelle que « *la Directive 95/46 vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel* ». Le RGPD a un objet identique²³.

Cette réaffirmation de l'objet n'est pas sans intérêt dès lors qu'il rappelle de manière claire, d'une part, que la personne concernée est le sujet central et, d'autre part, que cela induit une

¹⁹ Directive , art. 2.a) et RGPD, art. 4.1.

²⁰ Directive, art. 2.b) et RGPD, art. 4.2.

²¹ Directive, art. 2.d) et RGPD, art. 4.7.

²² Directive, considérant n° 26 et RGPD, considérant n° 27 du RGPD.

²³ C.J.U.E., *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, 5 juin 2018, point 26.

définition large de la notion de « *responsable du traitement* » qui participe et permette une telle protection²⁴.

Le RGPD est ambitieux. Parmi les objectifs annoncés figurent la contribution au « *bien-être* » des individus²⁵ ou encore le fait que « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* »²⁶.

Le Règlement concerne uniquement la protection des données personnelles rattachées à des personnes physiques, ainsi qu'aux identifiants en ligne (tels que les adresses IP²⁷ et les « *cookies* »²⁸) et à d'autres types d'identifiants qui sont associés, par les équipements et les applications, aux utilisateurs de l'internet²⁹. En effet, les traces du passage des utilisateurs, laissées par ces identifiants, permettent de profiler les personnes physiques auxquelles ils sont attribués³⁰.

Le RGPD et la directive ePrivacy³¹, également appelée « Directive cookie », régissent la manière dont un site web peut utiliser des « *cookies* » pour suivre les visiteurs de l'UE. L'objectif de la Directive Cookie est d'harmoniser les différentes législations et d'accompagner la réforme du RGPD.

Cependant, il est nécessaire de mettre à jour l'actuelle Directive « vie privée et communications électroniques » de 2002 afin de tenir compte des nouvelles évolutions technologiques et commerciales, telles que l'utilisation généralisée actuelle de la voix sur IP et

²⁴ J. HERVEG et J.-M. VAN GYSEGHEM, « La protection des données à caractère personnel en droit européen - Chronique de jurisprudence (2018): Personal data protection in European law - Column of case-law (2018) », 2019, p.82.

²⁵ Considérant 2 du Règlement.

²⁶ Considérant 4 du Règlement.

²⁷ C.J.U.E., deuxième ch., 19 octobre 2016, *Breyer*, C-582/14, EU:C:2016:779.

La question qui se posait était de savoir si une adresse IP pouvait être qualifiée de donnée personnelle permettant d'identifier un individu ? La Cour avait constaté qu'une adresse IP dynamique, enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public, constitue, à l'égard dudit fournisseur, une donnée à caractère personnel (article 2 directive 95/46/CE), lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce à des informations supplémentaires dont dispose le fournisseur d'accès à Internet de cet individu.

²⁸ Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web. Les cookies ont de multiples usages : ils peuvent servir à mémoriser votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des fins statistiques ou publicitaires, etc. (définition de la CNIL : Commission nationale de l'informatique et des libertés (France)).

²⁹ Considérant 30 du Règlement.

³⁰ T. Tombal, *op. cit.*, p.408.

³¹ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

La directive « Vie privée et communications électroniques » (ePrivacy) est une directive européenne qui régit l'utilisation des données dans le secteur des communications électroniques dans l'UE. La loi européenne sur les cookies régit l'utilisation des données par les sites web, les entreprises et les fournisseurs de services, la manière dont ils sont autorisés à les traiter, à les utiliser et à quelle fin ils sont autorisés à les partager.

des services de messagerie et de courrier électronique en ligne, ainsi que de l'émergence de nouvelles techniques de suivi du comportement en ligne des utilisateurs³².

Le 10 février 2021, le Conseil de l'Union européenne a approuvé un texte qui fait entrer le règlement ePrivacy dans une nouvelle phase de négociations en trilogue, d'où une nouvelle loi sur la protection des données pourrait émerger et prendre effet dans toute l'UE. En bref, le projet de règlement ePrivacy 2021³³ couvre toutes les communications électroniques (telles que les textes, les emails, les messages Facebook, SnapChat, etc.) et protège les individus au sein de l'UE contre l'ingérence de tiers dans leurs communications privées, sauf s'ils donnent leur consentement préalable³⁴.

Une directive européenne n'est pas une loi directement applicable et contraignante, les directives doivent en effet être transposées au niveau du droit national. Pour cela, les états se voient alors accorder une période d'adaptation plus ou moins longue. Par contre, un règlement est différent à ce niveau : en effet comme le RGPD, le futur règlement ePrivacy entrera en vigueur immédiatement et sera contraignant pour tous les États membres. Il faudra tenir compte des deux règlements. L'ePrivacy va en effet concrétiser et détailler le RGPD. L'ePrivacy est une *lex specialis*. Cela signifie qu'il a priorité et précisera le RGPD qui est une *lex generalis*. Le RGPD va ainsi être précisé et clarifié par l'ePrivacy sur des points spécifiques avec des règles claires. En effet, le RGPD n'a pas été créé exclusivement pour Internet³⁵.

En ce qui concerne la vie privée, les cookies d'un site web constituent aujourd'hui la technologie la plus utilisée pour la collecte, le traitement et le partage des données personnelles des utilisateurs finaux sur Internet, mais ils doivent recevoir le consentement

³² Conseil de l'UE, Communiqué de presse, Confidentialité des communications électroniques: le Conseil arrête sa position sur des règles en matière de vie privée et de communications électroniques, 10 février 2021 (disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/>).

³³ Le 10 février 2021, les États membres ont approuvé un mandat de négociation en vue de la révision des règles en matière de protection de la vie privée et de la confidentialité dans l'utilisation des services de communications électroniques. Ces règles actualisées "vie privée et communications électroniques" définiront les situations dans lesquelles les fournisseurs de services sont autorisés à traiter des données de communications électroniques ou à avoir accès à des données stockées sur les appareils des utilisateurs finaux.
Projet de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement "vie privée et communications électroniques") - mandat du Conseil : <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>

³⁴ Article 16.1 du projet.

Cookiebot, « RGPD et consentement aux cookies | RGPD et cookies | Mon utilisation des cookies est-elle conforme ? », 28 octobre 2020 (disponible sur : <https://www.cookiebot.com/fr/rgpd-cookies/>).

³⁵ Digital Guide IONOS, « Le règlement ePrivacy : à quoi devez-vous vous attendre ? », 2021 (disponible sur : <https://www.ionos.fr/digitalguide/sites-internet/droit-dinternet/le-reglement-eprivacy-projet-de-lue/>)

explicite des utilisateurs avant d'être activés³⁶. Avec l'entrée en vigueur du RGPD en 2018, les questions relatives à la vie privée sur Internet et aux cookies ont été abordées en plaçant le consentement de l'utilisateur final au cœur même du processus³⁷.

Le consentement reste un élément essentiel du projet de règlement ePrivacy 2021, et les cookies et traceurs similaires sont également la cible du nouveau projet de loi sur la protection des données. Selon le nouveau projet de règlement ePrivacy 2021, le consentement de l'utilisateur final est nécessaire avant de traiter tout type de données provenant des ordinateurs ou des Smartphones des utilisateurs³⁸.

Chapitre 4 : Principes clés du RGPD

Le RGPD énonce, en son chapitre II, plusieurs principes : le consentement, la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité, la confidentialité et la responsabilité³⁹.

Une grande importance est accordée au consentement donné par les personnes concernées par le traitement de leurs données personnelles. Pour être licite, le traitement de données doit avoir été effectué avec le consentement libre, spécifique, éclairé et univoque de la personne concernée. Le consentement doit laisser un véritable choix à la personne concernée : accepter ou refuser, sans conséquence dommageable⁴⁰.

En outre, le texte s'appuie sur deux autres éléments que nous analyserons ici :

- premièrement, la responsabilité des acteurs chargés du traitement des données personnelles, des entreprises et des organismes publics ou privés qui traitent des données ou bien des personnes dont les données personnelles sont traitées ;
- deuxièmement, la transparence à l'égard des personnes dont les données personnelles sont utilisées. L'objectif est de permettre à chacun de pouvoir reprendre le contrôle sur leurs données personnelles.

Les dispositions du RGPD s'articulent ainsi autour de trois principes clés : le consentement, la transparence, et la responsabilité.

³⁶ Sur ce point, Fashion ID a intégré sur son site web le plugin (ou bouton) « j'aime » de Facebook. Ce genre de plugin permet par exemple au visiteur du site web de partager un contenu sur le réseau social. Mais il permet à Facebook de collecter des informations personnelles sur le visiteur (notamment son adresse IP), et ce même si le visiteur n'interagit pas avec le plugin et n'a pas de compte sur le réseau social. Le simple fait que le plugin soit chargé par le navigateur web suffit à envoyer des informations à Facebook.

C.J.U.E., deuxième ch., 29 juillet 2019, *Fashion ID*, C-40/17, EU:C:2019:629.

P. VAN CLEYNENBREUGEL, *Advanced European Law*, cours organisé à l'Université de Liège, 2019-2020.

³⁷ Cookiebot, « Loi sur la vie privée de l'UE | RGPD, ePrivacy... le droit et les cookies », 10 mars 2021 (disponible sur : <https://www.cookiebot.com/fr/loi-vie-privee/>).

³⁸ Cookiebot, « Le règlement ePrivacy et les cookies | Mises à jour du règlement ePrivacy 2021 », 11 mars 2021 (disponible sur : <https://www.cookiebot.com/fr/reglement-e-privacy/>).

³⁹ Ces principes se retrouvent à l'article 5 du RGPD.

⁴⁰ GIAKOUMOPOULOS, G., BUTTARELLI, G., O'FLAHERTY, M., « Manuel de droit européen en matière de protection des données », Luxembourg, 2019, p.126.

En plus de ces principes qui sont applicables aussi bien aux enfants qu'aux adultes, les enfants font l'objet d'une attention et d'une protection additionnelle en raison de leur vulnérabilité particulière que nous analyserons dans la prochaine partie.

A. Le consentement⁴¹

L'article 4, paragraphe 11, du RGPD définit le consentement comme suit : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Le concept fondamental de consentement reste identique à celui de la directive 95/46/CE, et le consentement constitue l'une des bases juridiques sur lesquelles tout traitement de données à caractère personnel doit être fondé conformément à l'article 6 du RGPD.

Le 28 novembre 2017, le dénommé « Groupe de travail Article 29 », en abrégé G29 (l'organe indépendant de conseil et de consultation des Contrôleurs européens de la protection des données), a publié un avis dans lequel est traitée la notion de « *consentement* »⁴². Dans son avis⁴³, le G29 examine ce que ces quatre conditions de validité impliquent précisément.

Cependant, le consentement « *libre, spécifique, éclairé et univoque* » de l'utilisateur, semble peu adapté aux enfants. C'est ce que nous étudierons dans le chapitre suivant dédié à la protection des données personnelles des mineurs.

§1 : Libre

Le consentement doit être libre⁴⁴, c'est-à-dire que la personne concernée a véritablement le choix d'accepter ou de refuser. La personne concernée doit avoir un réel choix et un certain degré de contrôle sur le traitement des données à caractère personnel. Le consentement ne sera, par conséquent, pas valable s'il y a un déséquilibre de force entre le responsable du traitement et la personne concernée.

Le G29 a considéré qu'en général, « *toute pression ou influence inappropriée exercée sur la personne concernée (...) l'empêchant d'exercer sa volonté rendra le consentement non valable* ». Il est considéré comme n'étant pas donné librement quand il existe une

⁴¹ Autorité de protection des données belge, Consentement (disponible sur <https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/bases-juridiques/consentement>).

⁴² Claeys and Engels, Comment faut-il comprendre la notion de 'consentement' dans le RGPD ?, 5 janvier 2018 (disponible sur : <https://www.gdprbelgium.be/fr/nouvelles/comment-faut-il-comprendre-la-notion-de-'consentement'-dans-le-rgpd>).

⁴³ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017.

⁴⁴ Y. POULLET, « Consentement et RGPD:des zones d'ombre ! », 2019, p.6.

« tromperie », « intimidation », « coercition » ou de « conséquences négatives importantes »⁴⁵.

§2 : Spécifique

Le consentement doit être spécifique, c'est-à-dire que, selon le G29, le consentement n'est spécifique que si le responsable du traitement explique le but du traitement, demande un consentement distinct⁴⁶ dans le cas d'un traitement avec plusieurs finalités⁴⁷, et distingue clairement les informations relatives à la réception du consentement à un traitement de données, des informations relatives à d'autres questions.

L'exigence selon laquelle le consentement doit être « spécifique » vise à garantir un certain degré de contrôle utilisateur et de transparence pour la personne concernée.

§3 : Éclairé

Le consentement doit être éclairé⁴⁸, c'est-à-dire que la personne qui donne son consentement doit comprendre ce à quoi elle consent. Ce n'est possible que si le responsable du traitement informe la personne concernée préalablement. Les informations que le responsable de traitement communique doivent être complètes, claires et formulées en des termes compréhensibles de sorte que la personne concernée puisse décider en connaissance de cause. Il faut également veiller à ce que la personne concernée ait ces informations réellement sous les yeux. Le fait qu'elles soient « accessibles » ne suffit pas⁴⁹.

Cependant, selon Kightlinger⁵⁰, l'un des critiques les plus véhéments du consentement dans la législation européenne sur la protection des données, fait valoir qu'en vertu de la protection des données personnelles, le consentement éclairé n'est jamais suffisant pour garantir qu'un

⁴⁵ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p. 8, p. 12.

⁴⁶ Considérant 32 du RGPD.

⁴⁷ Autorité de protection des données belge, Consentement (disponible sur <https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/bases-juridiques/consentement>). Par exemple, un hebdomadaire organise un quiz à titre publicitaire, permettant de gagner un voyage. Les participants mentionnent leurs coordonnées sur le formulaire de participation afin que l'hebdomadaire puisse contacter le gagnant. L'hebdomadaire souhaite transmettre les coordonnées des participants à une série d'éditeurs d'autres hebdomadaires ainsi qu'à des tour-opérateurs afin que ces deux groupes puissent envoyer des publicités aux participants du quiz. Il s'agit ici d'autres traitements qui n'ont rien à voir avec le quiz. Pour que l'hebdomadaire puisse transmettre les données des participants, il doit demander le consentement aussi bien pour la transmission aux éditeurs que pour la transmission aux tour-opérateurs.

⁴⁸ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.14 et s.

⁴⁹ Autorité de protection des données belge, Consentement (disponible sur <https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/bases-juridiques/consentement>)

⁵⁰ M., KIGHTLINGER. 2007–2008. Twilight of the idols? EU internet privacy and the postenlightenment paradigm. *Columbia Journal of European Law* 14:1–62.

opérateur de site Web puisse collecter et utiliser légalement les informations personnellement identifiables de la personne et les transférer vers des pays tiers⁵¹.

§4 : Univoque

Le consentement doit être univoque, c'est-à-dire qu'il requiert un acte positif clair de la personne concernée. Toute imprécision au sujet de la volonté de la personne concernée de donner son consentement est ainsi exclue. Cet acte positif peut être une déclaration écrite ou orale ainsi qu'un acte spécifique comme par exemple un mouvement de glissement dans une certaine direction d'un élément sur un écran⁵².

Le G29 indique également qu'un responsable de traitement doit toujours pouvoir prouver qu'il a reçu le consentement valable de la personne concernée. Il faut donc pouvoir démontrer quand le consentement a été reçu et quelles informations ont été données à la personne concernée. Le Groupe de travail souligne que la personne concernée a toujours la possibilité de retirer son consentement. Il doit être aussi simple pour la personne concernée de retirer son consentement, que de le donner. Si, par exemple, le consentement a été donné par un simple « clic de souris », il doit pouvoir être retiré tout aussi simplement⁵³.

§5 : Explicite - situations particulières

Le G29 examine ensuite la notion de « *consentement explicite* ». Le consentement explicite est requis dans certaines situations où un risque sérieux lié à la protection des données survient, et où un niveau élevé de contrôle sur les données à caractère personnel par la personne concernée est de ce fait jugé approprié⁵⁴.

En effet, dans certaines situations spécifiques (telles que par exemple, le traitement de données à caractère personnel sensibles comme les données relatives à la santé, données desquelles ressort l'origine raciale,...), le consentement doit être « *explicite* ». Selon le G29, il est dans cette hypothèse requis d'avoir une déclaration explicite de consentement, par exemple : une déclaration écrite, un e-mail, un formulaire rempli électroniquement⁵⁵.

B. La transparence

⁵¹ G., ZANFIR, « Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law », in *Reloading Data Protection*, Dordrecht, Springer Netherlands, 2013, pp. 237–257.

⁵² Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.18 et s.

⁵³ Claeys and Engels, Comment faut-il comprendre la notion de ‘consentement’ dans le RGPD ?, 5 janvier 2018 (disponible sur : <https://www.gdprbelgium.be/fr/nouvelles/comment-faut-il-comprendre-la-notion-de-‘consentement’-dans-le-rgpd>).

⁵⁴ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.20 et s.

⁵⁵ Claeys and Engels, Comment faut-il comprendre la notion de ‘consentement’ dans le RGPD ?, 5 janvier 2018 (disponible sur : <https://www.gdprbelgium.be/fr/nouvelles/comment-faut-il-comprendre-la-notion-de-‘consentement’-dans-le-rgpd>).

La transparence est un principe qui se manifeste tout au long du droit de l'Union⁵⁶. Il traverse toute la compréhension du RGPD.

Ce dernier principe s'applique principalement :

- Lorsque le responsable du traitement doit fournir des informations aux personnes concernées à propos de ses activités de traitement. Le responsable devra toujours vérifier la bonne compréhension des informations qu'il fournit et ce en fonction de son public cible ;
- Lorsque le responsable du traitement communique avec les personnes concernées à propos de l'exercice de droits ou d'une violation de données à caractère personnel ;
- Lorsque le responsable du traitement doit faciliter l'exercice par les personnes concernées de leurs droits.

Ce principe fondamental (voire le plus important de toute la matière) permet de donner de la confiance aux personnes concernées en leur permettant de comprendre et d'appréhender convenablement les activités de traitement du responsable du traitement et, s'ils le souhaitent, de demander plus d'informations, de s'y opposer, de retirer leur consentement, etc⁵⁷.

Il s'articule au consentement, dans la mesure où la transparence est la condition de possibilité d'un consentement explicite et éclairé. Les entreprises ont désormais l'obligation, et ce dès la phase de collecte, de fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données seront traitées. Ces informations doivent être fournies de façon concise, compréhensive et accessible par tous. Les traitements doivent être expliqués aux personnes concernées d'une façon aisément accessible garantissant qu'elles comprennent ce qu'il va advenir de leurs données. Cela signifie que la personne concernée doit connaître la finalité spécifique du traitement de données à caractère personnel lors de la collecte des données la concernant⁵⁸.

Ainsi, l'article 12 du RGPD accorde à la personne concernée le droit d'attendre du responsable de traitement que celui-ci prenne des mesures appropriées afin de lui fournir les informations listées aux articles 13 et 14 du RGPD, ainsi que pour procéder à toute communication relative aux autres droits de la personne concernée « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* »⁵⁹.

C. La responsabilité

La question de la responsabilité est loin d'être un effet secondaire du RGPD qui impose aux responsables du traitement une obligation de pouvoir démontrer qu'il se conforme à la réglementation. La terminologie anglaise permet de mieux décrire ce qui est entendu sous le

⁵⁶ Art. 1 TUE, art. 11§2 TUE, art. 15§3 TFUE.

⁵⁷ A. BEELEN, P. LAMBRECHT et F. DECHAMPS, « Guide pratique du RGPD : fiches de guidance », Bruxelles, Bruylant, 2018, p.29.

⁵⁸ Considérant 39 du RGPD.

⁵⁹ T. TOMBAL, *op. cit.*, p.410.

couvert de ce principe. Le terme « *accountability* » renvoie à l'idée de pouvoir « rendre compte de »⁶⁰.

Ce principe anglo-saxon est une obligation pour le responsable du traitement d'assurer la transparence et la traçabilité des traitements de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte afin de pouvoir rendre des comptes aux autorités de contrôle qui lui signaleraient des irrégularités⁶¹.

Le RGPD vise à responsabiliser davantage les entreprises dans leur traitement des données à caractère personnel. Le système de responsabilisation recouvre principalement deux notions⁶² :

- d'une part, la protection des données dès la conception ou « *Privacy by design* » : le responsable de traitement anticipe, dès l'étape de définition d'un projet, toutes les contraintes juridiques en matière de protection des données à caractère personnel ;
- d'autre part, la protection des données par défaut ou « *Privacy by default* » : le responsable de traitement doit s'assurer de ne collecter que les données strictement nécessaires aux finalités poursuivies par le traitement de données à caractère personnel. On parle de principe de minimisation des données⁶³.

Selon l'avis du Groupe de travail « Article 29 »⁶⁴, l'aspect fondamental de la responsabilité est l'obligation du responsable du traitement de :

- mettre en place des mesures qui, dans des circonstances normales, garantissent que les règles de la protection des données sont respectées dans le contexte de traitements ; et
- disposer de documents démontrant aux personnes concernées et aux autorités de traitement quelles mesures ont été prises pour obtenir le respect des règles relatives à la protection des données⁶⁵.

B. Une protection spécifique des enfants

Chapitre 1 : Les raisons d'une telle protection

Pourquoi les enfants auraient-ils besoin d'une protection particulière face aux opérations de traitement de leurs données personnelles ?

⁶⁰ K. ROSIER et A. DELFORGE, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Bruxelles, Larcier, 2018, p.665.

⁶¹ A. BENSOUSSAN, « La protection des données personnelles de A à Z », Bruxelles, Bruylant, 2017, p.140.

⁶² Article 25 du RGPD.

⁶³ S. M'HAMDI, « "RGPD" : quelle protection pour vos données personnelles ? », Institut national de la consommation (INC), 10 octobre 2019 (disponible sur : <https://www.inc-conso.fr/content/rgpd-quelle-protection-pour-vos-donnees-personnelles>)

⁶⁴ Groupe de travail « Article 29 », Avis 3/2010 sur le principe de la responsabilité, WP 173, Bruxelles, 13 juillet 2010.

⁶⁵ GIAKOUMOPOULOS, G., BUTTARELLI, G., O'FLAHERTY, M., « Manuel de droit européen en matière de protection des données », Luxembourg, 2019, p.153.

Les enfants passent de plus en plus de temps *online*. Facebook, Snapchat ou Instagram... Consulter à tout moment de la journée ces réseaux sociaux est aujourd'hui devenu un réflexe pour la plupart des jeunes. Ces outils font partie intégrante de leur réalité et occupent une place centrale⁶⁶.

Lorsque le mineur s'inscrit sur ces réseaux sociaux, il partage, souvent sans s'en rendre compte, de nombreuses données à caractère personnel (coordonnées, photos, données de localisation). Il devient ainsi vulnérable de par le contenu qu'il divulgue lui-même, sans être conscient de la notion de « vie privée » et sans envisager les conséquences dommageables. Son « profil » en ligne reste souvent public, ce qui permet aussi à des personnes malveillantes d'avoir accès à ses photos, son âge, ses centres d'intérêts. Il est également avéré que tant les réseaux sociaux eux-mêmes que des annonceurs tiers, comme les publicitaires, utilisent ces données, notamment à des fins commerciales. C'est dans cet environnement de développement numérique que le RGPD a été adopté et qu'il se veut soucieux de leur situation⁶⁷.

L'enfant n'est pas une personne autonome face à son écran, ayant des connaissances et des capacités qui lui donnent une compréhension suffisante de la question posée et de ses conséquences économiques et juridiques, comme le majeur.

Les chiffres sont frappants : selon des données publiées par l'Unicef, les jeunes (de 15 à 24 ans) constituent la tranche d'âge la plus connectée. À l'échelle mondiale, 71 % d'entre eux utilisent Internet contre 48 % pour la population totale⁶⁸. D'après les estimations, un internaute sur trois dans le monde est un enfant ou un adolescent de moins de 18 ans⁶⁹.

Chapitre 2 : La protection juridique des données des enfants

Malgré les enjeux particuliers posés concernant les données des enfants, il n'existe pas actuellement de texte obligatoire qui régleme spécifiquement la protection des données des enfants⁷⁰.

En revanche, il existe des éléments protecteurs contenus dans les Conventions internationales et régionales. Par ailleurs, au niveau de l'Union européenne alors que la directive du 24

⁶⁶ Média Animation ASBL, *Médias sans frontières – Productions et consommations médiatiques dans une société multiculturelle*, Les dossiers de l'éducation aux médias, 2011, p. 30 (disponible sur <http://www.media-animation.be>)

⁶⁷ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p.7.

⁶⁸ Défense des enfants internationale Belgique, La protection des données des enfants dans le monde numérique, outil pédagogique n°2018-07, Aurélie Carré sous la supervision de Géraldine Mathieu et Benoit Van Keirsbilck, décembre 2018.

⁶⁹ S. LIVINGSTONE, J. CARR et J. BYRNE, « One in three: Internet Governance and Children's Rights », *Global Commission on Internet Governance*, Paper series n° 22, novembre 2015.

⁷⁰ G. MATHIEU et A.-C. RASSON, « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l'environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018, p. 395 et s.

octobre 1995 n'abordait pas la question du consentement des mineurs à des traitements de données à caractère personnel, le RGPD posent des conditions spécifiques applicables au consentement des enfants⁷¹.

1. La protection offerte par les Conventions internationales et régionales

L'instrument principal est la Convention internationale des droits de l'enfant. La CIDE ne contient pas de disposition spécifique à la protection des données des enfants. Cependant, il est tout à fait possible de s'appuyer sur certains de ses principes et droits pour protéger ces données⁷².

De plus, le Comité des droits de l'enfant⁷³, a publié en 2016 des observations générales sur la mise en œuvre des droits de l'enfant durant l'adolescence dans lesquelles les questions du respect de leur vie privée et de la confidentialité de leurs données personnelles sont abordées, notamment dans le contexte de l'environnement numérique⁷⁴.

La CIDE est un texte de droit international contraignant pour les pays. La reconnaissance du droit des enfants à une protection renforcée de leurs données dans le monde numérique a une portée internationale. Ceci s'applique à la Belgique qui a ratifié la CIDE, comme la quasi-totalité des pays dans le monde.

Au niveau de l'Europe, la Convention européenne des droits de l'Homme (CEDH) ne vise pas spécifiquement les enfants, ni la protection des données en tant que telle. Cependant, elle instaure : le droit au respect de la vie privée et familiale, du domicile et de la correspondance

⁷¹ A. BAMDE, « RGPD : le consentement des mineurs », disponible sur www.aurelienbamde.com, 19 décembre 2018.

⁷² Il s'agit en particulier de : la prise en compte, pour toute décision qui le concerne, de l'intérêt supérieur de l'enfant (art. 3 CIDE) ; le droit à la liberté d'expression sans restriction, y compris le droit de rechercher, de recevoir, de répandre l'information librement (art. 13 CIDE) ; le droit à la vie privée (art. 16 CIDE) ; le droit à recevoir de l'information, sous la forme de médias qui soient adaptés aux enfants et diversifiés, ainsi que le droit à la protection contre les contenus nocifs (art. 17 CIDE) ; le droit à la protection contre toute forme de violence (art. 19 CIDE) ; le droit à l'éducation (art. 28 CIDE) ; le droit à la protection contre toute forme d'exploitation économique (art. 32 CIDE) ; le droit d'être protégé contre toute forme d'exploitation (art. 36 CIDE).

⁷³ L'entité chargée au sein des Nations unies de surveiller la bonne application de la Convention internationale des droits de l'enfant par les pays qui l'ont ratifiée.

⁷⁴ A. CARRÉ, sous la supervision de G. MATHIEU et B. VAN KEIRSBILCK
Défense des enfants internationale Belgique, « La protection des données des enfants dans le monde numérique », outil pédagogique n°2018-07, décembre 2018 (disponible sur : <https://www.dei-belgique.be/index.php/component/jdownloads/send/46-la-protection-des-donnees/389-la-protection-des-donnees-des-enfants-dans-la-monde-numerique.html>).

« Les Etats devraient chercher à déterminer, par le dialogue avec les adolescents, les domaines dans lesquels le droit au respect de la vie privée n'est pas respecté, notamment en ce qui concerne les interactions personnelles dans l'environnement numérique et l'utilisation des données par des entreprises commerciales et d'autres entités. Ils devraient aussi prendre toutes les mesures qui s'imposent pour améliorer et garantir le respect de la confidentialité des données et de la vie privée des adolescents, compte tenu du développement de leurs capacités ». Comité des droits de l'enfant des Nations unies, Observation générale n°20(2016) sur la mise en œuvre des droits de l'enfant pendant l'adolescence, décembre 2016, CRC/C/GC/20, p.13

(art. 8 CEDH)⁷⁵ ; l'interdiction de l'abus de droit (art. 17 CEDH) et la limitation de l'usage des restrictions à ces droits qui doit toujours être strictement justifiée et encadrée (art. 18 CEDH), pour tous, et donc aussi pour les enfants⁷⁶.

En outre, le Conseil de l'Europe⁷⁷, a adopté le 4 juillet 2018 des Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique⁷⁸.

2. La protection offerte à l'échelle de l'Union européenne

2.1 La Charte des droits fondamentaux de l'Union européenne

Le droit à la protection des données à caractère personnel a été reconnu comme tel à l'article 8 de la Charte⁷⁹ après 30 ans d'histoire de la réglementation de la protection des données en Europe⁸⁰.

Selon la Charte, la protection des données personnelles est un droit fondamental en tant que tel.

⁷⁵ Cour.eur. D.H., 7 février 2012, *Von Hannover c. Allemagne* (n° 2), n°40660/08 et 60641/08. Cour.eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, n° 59320/00. S. OFFMANN, Journal d'Actualités des Droits européens, « Von Hannover 2 (le retour) : Le droit au respect de la vie privée de la Princesse Caroline au royaume de la liberté de la presse », 6 avril 2012 (disponible sur : <https://revue-jade.eu/article/view/245>).

Dans ces affaires, les membres de la famille princière monégasque ont alimenté, outre la presse à scandale, la jurisprudence de la Cour européenne des droits de l'Homme sur la question récurrente et délicate de la conciliation du droit au respect de la vie privée avec la liberté d'information. Dans l'arrêt Von Hannover du 24 juin 2004, la Cour européenne des droits de l'Homme avait condamné l'Allemagne pour ne pas avoir assuré cet équilibre entre les deux droits fondamentaux dans la mesure où son système juridique n'offrait aucune protection aux personnes publiques se trouvant dans les lieux publics. Dans le second arrêt Von Hannover, la Cour européenne des droits de l'Homme maintient l'exigence pour les articles et les photographies de contribuer « au moins pour partie » à un débat « d'intérêt général » afin que leur publication soit licite. Ainsi, dans cette dernière affaire, les photographies présentaient un caractère d'intérêt général entendu de manière large dans la mesure où elles servent à illustrer un article relatif à la santé du « Prince gouvernant de Monaco et la façon dont les enfants du Prince conciliaient les obligations de solidarité familiale avec les besoins légitimes de leur vie privée dont faisait partie les vacances ». Considérant 49.

⁷⁶ Cour eur. D.H., 23 février 2016, *Y.Y./Russie*, n° 40378/06. La Convention européenne des droits de l'homme a été violée en raison du fait que les données médicales de la requérante et celles de ses enfants ont été transmises sans son consentement par une commission des soins de santé au ministère russe des soins de santé.

⁷⁷ L'organisme qui s'occupe notamment de la bonne mise en œuvre de la CEDH

⁷⁸ Comité des Ministres du Conseil de l'Europe, Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, Recommandation CM/REC(2018)7, <http://rm.coe.int/lignes-directrices-relatives-au-respect-a-la-protection-et-a-la-realisation/16808d881b>.

⁷⁹ Quant à sa relation avec la directive 95/46/CE, la Cour de Justice précise que « les dispositions de la directive 95/46/CE, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux ». C.J.U.E., 20 mai 2003, *Rechnungshof*, aff. jointes C-465/00, C-138/01 et C-139/01.

⁸⁰ ZANFIR, G., « Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law », in *Reloading Data Protection*, Dordrecht, Springer Netherlands, 2013, pp. 237-257.

En effet, en son article 8, la Charte prévoit que :

- « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »⁸¹.

Cet article est très important, la Charte est contraignante pour tous les pays membres de l'Union européenne, y compris la Belgique, mais uniquement dans la mesure où l'Etat membre agit dans le champ d'application du droit de l'Union. En effet, l'article 51 de la Charte stipule que : « *Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en oeuvre le droit de l'Union* »⁸².

Par ailleurs, même si ce n'est pas un texte spécifique pour les enfants, cet article s'applique à tous, y compris aux mineurs d'âge. L'article 8 de la Charte peut donc être utilisé également pour les données personnelles des enfants. Ceux-ci bénéficient ainsi également de son effet protecteur et de son efficacité.

L'article 8 de la Charte est complété par l'article 16 du Traité sur le fonctionnement de l'Union européenne qui est également contraignant. L'article 16 du Traité affirme également que toute personne a droit à la protection de ses données personnelles.

Sur la base de ces deux articles, le Règlement Général sur la Protection des Données a été adopté et celui-ci s'applique aussi bien aux données des enfants qu'à celles des adultes et contient en outre quelques éléments spécifiques pour les enfants⁸³.

⁸¹ Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 à Nice, article 8.

⁸²A. LENNE, EU-Logos Athéna, « L'édification de « notre » Charte des droits fondamentaux », 16 mai 2014 (disponible sur : <https://www.eu-logos.org/2014/05/16/ledification-de-notre-charte-des-droits-fondamentaux/>). C.J.U.E., gde ch., 26 février 2013, *Aklagaren contre Hans Akerberg Fransson*, C-617/10, EU:C:2013:105. La rédaction de l'article 51 de la Charte émerge dans l'arrêt Wachauf dans lequel la Cour affirme que la protection des droits fondamentaux lie les Etats membres « *lorsqu'ils mettent en œuvre une réglementation communautaire* ». Dans cet arrêt, la Cour de justice demande un strict rapport d'exécution du droit de l'Union européenne pour que les Etats membres soient liés par les droits fondamentaux dans le cadre de l'Union européenne. Mais finalement, la jurisprudence ambitieuse et évolutive de la Cour de justice continue d'interpréter l'ambiguïté qui entoure l'article 51 de la Charte. L'arrêt qui a fait le plus de retentissements est sans hésitation l'arrêt *Aklagaren contre Hans Akerberg Fransson* de 2013. En l'espèce, il s'agissait de dispositions internes, transposant une directive européenne et donc, ne répondaient pas à la condition de mise en œuvre du droit de l'Union européenne. Toutefois, la Cour étend sa jurisprudence antérieure relative à la protection des droits fondamentaux et affirme que lorsqu'une réglementation nationale entre dans le champ d'application du droit de l'Union européenne alors, la Charte trouve à s'appliquer. La Cour affirme la portée ambitieuse du champ d'application de la Charte des droits fondamentaux et donne une interprétation plus large de l'article 51 de la Charte.

⁸³ En Belgique, le RGPD a été complété par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

2.2 Le RGPD

Le RGPD a renforcé sur certains plans la protection des données à caractère personnel des individus, mais ce dernier se veut soucieux du cas des mineurs sur internet, et plus particulièrement de leurs données à caractère personnel⁸⁴. Ce n'était pas tellement le cas, sous l'empire de la directive 95/46, qui n'appréhendait pas leur situation particulière.

L'article 6 du RGPD énumère les différentes bases légales rendant licite le traitement d'une donnée à caractère personnel. À priori, le traitement des données d'un mineur devrait remplir les mêmes conditions que pour tout traitement, comme le traitement d'un adulte non protégé. Cependant, sur les six bases légales prévues par le RGPD, deux connaissent des aménagements lorsque la donnée traitée concerne un mineur⁸⁵ :

- le point f) de l'article 6 1. du RGPD prévoit que le traitement 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* ». Par conséquent, la vulnérabilité des mineurs suppose, lorsqu'une mise en balance est faite entre leurs intérêts et les intérêts légitimes du responsable de traitement, que ce soit toujours les intérêts des mineurs qui priment.

- Par ailleurs, des conditions particulières sont prévues s'agissant du consentement des mineurs.

L'article 8 du RGPD détermine des conditions particulières en ce qui concerne le consentement du mineur dans le cadre de traitements de données par des services de la société de l'information, et uniquement pour ces traitements. Sont ici visés les plateformes internet, les réseaux sociaux ou encore les newsletters⁸⁶.

Il ressort clairement de ce qui précède que l'article 8 s'appliquera donc uniquement lorsque les conditions suivantes sont remplies :

- Le traitement est lié à l'offre directe de services de la société de l'information à un enfant ;
- Le traitement est fondé sur le consentement.

a. Les services de la société de l'information

⁸⁴ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p.7.

⁸⁵ G. MATHIEU et A.-C. RASSON, « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l'environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018, p. 420.

⁸⁶ Grande Bibliothèque du Droit, La protection des données personnelles des mineurs (fr), 3 avril 2020 (disponible sur : [https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_\(fr\)](https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_(fr)))

Il existe un consentement particulier applicable aux enfants en ce qui concerne les services de la société de l'information, fondé principalement sur l'autorité parentale⁸⁷.

Par conséquent, dans le droit de l'UE, lorsque des fournisseurs de services de la société de l'information traitent des données à caractère personnel d'enfants de moins de 16 ans sur la base d'un consentement, 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* »⁸⁸.

Afin de déterminer la portée du terme « *service de la société de l'information* » dans le RGPD, l'article 4, paragraphe 25, du RGPD fait référence à la directive 2015/1535⁸⁹.

Pour ce faire, le G29 se réfère également à la jurisprudence de la CJUE. La CJUE a estimé que les services de la société de l'information couvrent les contrats et autres services conclus ou transmis en ligne⁹⁰. Le Groupe de Travail indique que lorsqu'un service a deux éléments

⁸⁷ A. BENSOUSSAN, C. AVIGNON, V. BENSOUSSAN-BRULÉ, F. FORSTER, C. TORRES, et I. FALQUE-PIERROTIN, « Règlement européen sur la protection des données : textes, commentaires et orientations pratiques », 2e éd., Bruxelles, Bruylant, 2017, p.14.

⁸⁸ Art. 8, para. 1, premier alinéa du RGPD.

⁸⁹ Selon l'article 4, paragraphe 25 du RGPD, un service de la société de l'information est un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535: «b) "service", tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Aux fins de la présente définition, on entend par: i) "à distance", un service fourni sans que les parties soient simultanément présentes; ii) "par voie électronique", un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques; iii) "à la demande individuelle d'un destinataire de services", un service fourni par transmission de données sur demande individuelle.»

⁹⁰ C.J.U.E., troisième ch., 2 décembre 2010, *Ker-Optika bt contre ÁNTSZ Dél-dunántúli Regionális Intézet*, C-108/09, EU:C:2010:725, paragraphes 22 et 28.

Par rapport aux « *services composites* », le G29 se réfère également à l'affaire C-434/15 (*Asociación Profesional Elite Taxi contre Uber Systems Spain SL*), paragraphe 40, qui stipule qu'« *un service de la société de l'information faisant partie intégrante d'un service global dont l'élément principal n'est pas un service de la société de l'information (dans le cas d'espèce, un service de transport) ne répond pas à la qualification de « service de la société de l'information ».*

économiquement indépendants⁹¹, l'un d'entre eux étant un élément en ligne, par exemple l'offre ou l'acceptation d'une offre dans le cadre de la conclusion d'un contrat, ou les informations liées aux produits ou services, y compris les activités de marketing, cet élément est considéré comme un service de la société de l'information, tandis que l'autre élément, qui serait la livraison ou la distribution physique de marchandises, n'est pas couvert par la notion de service de la société de l'information. La fourniture d'un service en ligne relèverait également du champ d'application du terme service de la société de l'information au sens de l'article 8 du RGPD⁹².

b. La notion d' « enfant »

Bien que le Règlement prévoie un régime spécifique pour les enfants, celui-ci ne définit pas la notion d'enfant, celle-ci étant préférée par le législateur européen au concept de « *mineur* ».

Le G29⁹³ indique clairement dans ses lignes directrices sur le consentement que l'enfant est entendu au sens de la Convention des Nations unies relative aux droits de l'enfant, « (...) *un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable* »⁹⁴. C'est la définition retenue par la Convention internationale des droits de l'enfant (CIDE), adoptée par les Nations unies et ratifiée par tous les pays du monde, sauf les Etats-Unis.

Un adolescent est donc aussi un enfant jusqu'à son 18^{ème} anniversaire.

c. La vulnérabilité de l'enfant

⁹¹ C.J.U.E., 19 décembre 2019, *Airbnb Ireland*, C-390/18, EU:C:2019:1112.

La lettre de la DAJ, « La CJUE juge qu'Airbnb est un « service de la société de l'information » et non un agent immobilier », 16 janvier 2020 (disponible sur : <https://kiosque.bercy.gouv.fr/alyas/msite/view/lettre-daj/13245>). Cette demande est intervenue dans le cadre d'une procédure pénale introduite en France contre la société Airbnb Ireland. Dans sa plainte, l'Association pour un hébergement et un tourisme professionnels (AHTOP) soutenait que l'activité d'Airbnb ne se limitait pas à la mise en relation de locataires potentiels avec des loueurs d'hébergements de courte durée via sa plateforme, mais qu'elle exerçait une activité d'agent immobilier sans détenir de carte professionnelle comme l'exige la loi dite Hoguet (Loi n° 70-9 du 2 janvier 1970 réglementant les conditions d'exercice des activités relatives à certaines opérations portant sur les immeubles et les fonds de commerce). La CJUE estime que le service d'intermédiation fourni par Airbnb satisfait aux critères fixés par la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), et constitue par conséquent un « service de la société de l'information ». La CJUE considère que l'activité d'Airbnb consiste essentiellement à mettre à disposition « *un instrument de présentation et de recherche des logements mis à la location et facilitant la conclusion de futurs contrats de location* », et ne tend pas à la réalisation immédiate d'une prestation d'hébergement ni n'est indispensable à l'exécution d'une telle prestation.

⁹² Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.29 et s.

⁹³ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.28 et s.

⁹⁴ Cf. Nations unies, résolution 44/25 du 20 novembre 1989 (Convention relative aux droits de l'enfant).

Le mineur est généralement perçu comme une personne vulnérable⁹⁵.

Dans plusieurs de ses considérants, le règlement général sur la protection des données énonce que les enfants doivent bénéficier d'une protection spécifique de leurs données à caractère personnel parce qu'ils sont moins conscients des risques, des conséquences et de leurs droits liés au traitement des données à caractère personnel⁹⁶.

En effet, le considérant 38 du RGPD met en exergue la vulnérabilité des « enfants », terme utilisé au sein du règlement, et considère qu'ils « *méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences, des garanties concernées et de leurs droits liés au traitement des données à caractère personnel (...)* »⁹⁷.

Le RGPD continue et stipule que : « *Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre* »⁹⁸.

Le RGPD énonce encore que : « *Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier (...) lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants* »⁹⁹.

Lorsque le jeune s'inscrit sur les réseaux sociaux comme Facebook, Instagram, Snapchat, il partage, souvent sans s'en rendre compte, de nombreuses données à caractère personnel. Il devient ainsi vulnérable de par le contenu qu'il divulgue lui-même, sans être conscient de la notion de « vie privée » et sans envisager les conséquences dommageables potentielles.

d. Le consentement comme base de traitement des données à caractère personnel

Lorsqu'un mineur s'inscrit sur un réseau social, il fournit de nombreuses données à caractère personnel évidentes, comme son nom, son prénom, sa date de naissance, ainsi que des données personnelles plus intrusives, comme les photos qui se trouvent sur son GSM, le contenu de ses messages, ses données de géolocalisation, celles concernant ses centres d'intérêt, etc. En collectant, utilisant, conservant et diffusant ces données, le fournisseur d'un

⁹⁵ F. GEORGE et J.-B. HUBIN, « La protection de la personne en situation de vulnérabilité par le droit des obligations et des contrats dans l'environnement numérique », in *La protection de la personne en situation de vulnérabilité par le droit des obligations et des contrats dans l'environnement numérique*, s.l., Larcier, 2018.

⁹⁶ A. BENSOUSSAN, « E » in *La protection des données personnelles de A à Z*, 1e édition, Bruxelles, Bruylant, 2017, p. 109-114

⁹⁷ Considérant 38 du Règlement.

⁹⁸ Considérant 58 du Règlement.

⁹⁹ Considérant 75 du Règlement.

service de réseau social opère des traitements de données, à plusieurs fins, et devient dès lors un responsable de traitement¹⁰⁰, au sens du RGPD¹⁰¹.

Or, lorsque le responsable de traitement traite ce type de données, il doit pouvoir fonder son traitement sur l'une des bases légales édictées à l'article 6 du RGPD, comme le consentement de la personne concernée, l'exécution d'un contrat, le respect d'une obligation légale ou encore ses intérêts légitimes.

e. L'âge du consentement

L'article 8 du RGPD prévoit qu' « *en ce qui concerne l'offre directe de services de la société de l'information aux enfants, 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.* »

A cet égard, cette disposition opère une distinction entre d'une part, les enfants âgés de plus de 16 ans qui sont présumés être en mesure de consentir seuls, soit sans l'intervention de leurs représentants légaux, à un traitement de données à caractère personnel et, d'autre part, les enfants âgés de moins de 16 ans qui, pour consentir à un traitement de données à caractère personnel, doivent obtenir l'autorisation de leurs représentants légaux.

Le RGPD souligne cependant que les Etats membres peuvent prévoir par le biais de dispositions légales nationales un âge différent permettant à un enfant mineur de donner un consentement sans l'autorisation des parents, à la condition que cet âge ne soit pas inférieur à 13 ans¹⁰².

L'Autorité de protection de données belge soutient le choix du législateur belge d'abaisser à 13 ans l'âge pour le consentement parental en vertu du Règlement général sur la protection des données. Cet âge correspond mieux à la réalité quotidienne de très nombreux jeunes qui surfent déjà sur Internet à un jeune âge. Nous ne pouvons pas les priver d'opportunités de s'épanouir numériquement. Mais vu que les enfants doivent aussi prendre conscience de leur vie privée, le choix de 13 ans doit s'accompagner d'efforts supplémentaires pour leur apprendre dès l'enfance à adopter une attitude réfléchie à l'égard des médias¹⁰³.

À titre indicatif, l'âge de consentement est de 15 ans en France, en Grèce, en République Tchèque et en Slovaquie, contre 14 ans en Italie, en Autriche, à Chypre et en Bulgarie. Celui-ci

¹⁰⁰ Pour rappel, le responsable de traitement est défini à l'article 4 .7) du RGPD comme : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens de traitement* ».

¹⁰¹ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p. 8.

¹⁰² Grande Bibliothèque du Droit, La protection des données personnelles des mineurs (fr), 3 avril 2020 (disponible sur : [https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_\(fr\)](https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_(fr)))

¹⁰³ Autorité de protection des données, Communiqué de presse, RGPD: "la limite d'âge de 13 ans correspond à la pratique numérique", 13 février 2018

descend également à 13 ans en Estonie, au Danemark, en Irlande, en Finlande, en Pologne, en Lettonie, en Espagne, au Portugal, au Royaume-Uni et en Suède.

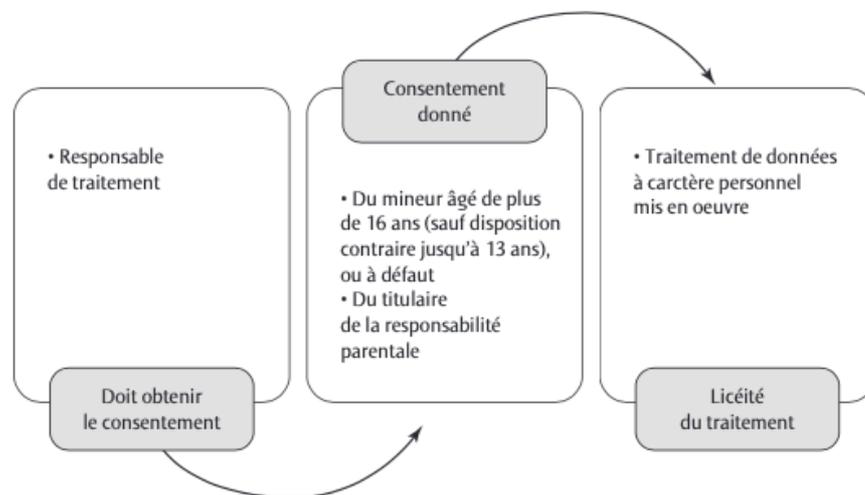
f. La responsabilité parentale

Lors de l'entrée en vigueur du RGPD, tant les médias que certaines autorités ont affirmé que les enfants ne pourraient plus, sous un certain âge, avoir accès aux réseaux sociaux sans autorisation de leurs parents¹⁰⁴.

À cet égard, un communiqué de presse de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen du 17 décembre 2015¹⁰⁵ indiquait que le RGPD en devenir allait instaurer des règles concernant la présence des enfants sur les médias sociaux : « *Les enfants en dessous d'un certain âge devront obtenir la permission de leurs parents (« consentement parental ») pour ouvrir un compte sur les médias sociaux tels que Facebook, Snapchat, comme c'est déjà le cas dans la plupart des pays de l'UE aujourd'hui* »¹⁰⁶.

L'article 8 n'est, cependant, pas une disposition encadrant l'inscription des enfants sur les réseaux sociaux. L'accès est en effet à dissocier de la question des données personnelles, qui est la seule réglementée par le RGPD¹⁰⁷.

En effet, il est bien possible qu'un jeune soit tout à fait légalement capable de s'inscrire seul sur un réseau social, mais n'ait pas l'âge fixé par le RGPD pour se prononcer seul sur le sort de ses données personnelles.¹⁰⁸



¹⁰⁴ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p. 5.

¹⁰⁵ Communiqué de presse disponible à l'adresse: <http://www.europarl.europa.eu/news/fr/press-room/20151217IPR08112/protection-des-donnees-les-citoyens-aux-commandes>.

¹⁰⁶ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p. 6.

¹⁰⁷ J. MONT, « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p. 5.

¹⁰⁸ A. BENSOUSSAN, « E » in La protection des données personnelles de A à Z, 1e édition, Bruxelles, Bruylant, 2017, p. 109-114

g. Le principe de la transparence

Le principe de transparence susmentionné se voit renforcé lorsque les informations à fournir sont destinées spécifiquement à un enfant¹⁰⁹.

Le Règlement prévoit des obligations accrues en matière de transparence vis à vis des enfants : les informations destinées aux enfants doivent être rédigées dans des termes qui soient adaptés à leur niveau de compréhension et à leurs capacités.

Dès lors, toute information ou communication relative à un traitement qui les concerne devra être rédigée en des termes clairs, simples et aisément compréhensibles pour ces enfants¹¹⁰. Ainsi, le vocabulaire, le ton et le style de langage employé devront être adaptés à ce public spécifique¹¹¹.

Le Groupe 29 précise également que les enfants conservent leur droit à recevoir ces informations conformément au principe de transparence renforcée, quand bien même leurs parents auraient-ils consentis au traitement, en application de l'article 8 du RGPD¹¹².

h. Le principe de responsabilité de l'enfant - une faiblesse du RGPD

Bien entendu, les atteintes à la vie privée des enfants sur la Toile ne sont pas uniquement le fait de parents ou d'adultes. Les enfants et les jeunes sont également responsables des contenus qu'ils diffusent et doivent donc être informés et accompagnés à propos de leurs droits et obligations en la matière¹¹³.

La faiblesse du RGPD réside dans la responsabilisation de la personne concernée, à qui le pouvoir décisionnel revient face au traitement de leurs données, à savoir le mineur. Il semble difficile, voire inopportun, de baser un système de protection à leur égard sur une telle responsabilisation¹¹⁴.

Les garde-fous posés par le RGPD sont très partiels et essentiellement limités à la substitution de l'accord parental ou équivalent à celui de l'enfant.

¹⁰⁹ Considérant 38 du Règlement.

¹¹⁰ Considérant 58 du Règlement.

¹¹¹ Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 10.

¹¹² T. TOMBAL, *op. cit.*, p.415.

¹¹³ G. MATHIEU et A.-C. RASSON, « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l'environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018, p.428.

¹¹⁴ A. CARRÉ, sous la supervision de G. MATHIEU et B. VAN KEIRSBILCK, *op. cit.*, p.30. (disponible sur : <https://www.dei-belgique.be/index.php/component/jdownloads/send/46-la-protection-des-donnees/389-la-protection-des-donnees-des-enfants-dans-la-monde-numerique.html>)

Comment vérifier que l'utilisateur a atteint la majorité digitale ? Le Groupe 29 suggère ainsi de demander à l'utilisateur son année de naissance. Rien ne garantit cependant que l'utilisateur ne persiste pas dans son mensonge à propos de son âge. Le G29 évoque également la possibilité de demander le paiement de 0,01 € par carte de crédit¹¹⁵. Parmi les suggestions évoqués par le Groupe de travail, ne figure pas l'utilisation d'un document officiel, comme une carte d'identité électronique¹¹⁶.

Ce sont là les maigres solutions proposées par le Comité européen de la protection des données. Sur ce point, les autorités de contrôle nationales sont tout à la fois pragmatiques et perplexes quant aux moyens à mettre en œuvre.

Chapitre 3 : Enquêtes en Europe : le réseau social « Tik Tok ».

Les enquêtes contre TikTok, application mobile de partage de vidéos et de réseau social lancée en septembre 2016, se multiplient.

L'application TikTok a encore une fois été épinglée pour manquement à ses obligations, dont la protection des données et de la vie privée des mineurs. Une enquête est également en cours au sein de l'Union Européenne.

Après les États-Unis, c'est au tour de l'Europe d'enquêter sur l'application chinoise TikTok. Une nouvelle fois, ce sont les pratiques de collecte de données à caractère personnel de cette application très populaire auprès des jeunes qui créent la polémique. L'European Data Protection Board (EDPB) vient de mettre en place une « *task force* » pour enquêter sur le traitement et la protection des données de TikTok par le propriétaire de l'application¹¹⁷.

Dans un communiqué de presse datant du 22 décembre 2020¹¹⁸, l'Autorité de protection des données personnelles italienne a annoncé qu'elle allait prendre des « mesures officielles » contre TikTok. Celle-ci a précisé également ses inquiétudes concernant la protection des données. L'autorité cite dans sa lettre « *le peu d'importance accordée à la protection des mineurs, le fait que l'interdiction de l'application aux moins de 13 ans soit facilement contournable, le peu de transparence, le manque d'informations pour les utilisateurs et les réglages par défaut ne respectant pas la vie privée* » pour justifier sa décision.

Les problèmes concernant les questions de vie privée et de protection des données sont d'autant plus importants puisque la majorité des utilisateurs de l'application est mineure. Les inquiétudes de l'Italie sont suffisamment sérieuses pour qu'elle n'attende pas les résultats de l'enquête actuellement en cours au niveau européen. En France, la CNIL (Commission

¹¹⁵ Groupe 29, Guidelines on Consent under Regulation 2016/679, 2017, p.30.

¹¹⁶ MONT, J., « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019, p.20 (disponible sur : <http://www.crid.be/pdf/public/8550.pdf>).

¹¹⁷ L. BASTIEN, « Le Big Data, RGPD : l'Union européenne ouvre une enquête sur l'application TikTok », 12 juin 2020 (disponible sur <https://www.lebigdata.fr/rgpd-tiktok>).

¹¹⁸ Disponible en version anglaise sur : <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9508923>.

nationale de l'informatique et des libertés) a lancé au mois d'août 2020 une enquête sur l'application, qui porte également sur la protection des données et des mineurs¹¹⁹.

Chapitre 4 : Tableau récapitulatif : majeur / mineur - RGPD¹²⁰

¹¹⁹ A. GAYTE, « L'Italie juge que TikTok ne protège pas assez les données de ses utilisateurs », Numerama, 22 décembre 2020 (disponible sur :<https://www.numerama.com/politique/678061-litalie-juge-que-tiktok-ne-protege-pas-assez-les-donnees-de-ses-utilisateurs.html>).

¹²⁰ A. BENSOUSSAN, C. AVIGNON, V. BENSOUSSAN-BRULÉ, F. FORSTER, C. TORRES, et I. FALQUE-PIERROTIN, *op. cit.*, p.21.

ADULTE

Consentement :

Un consentement libre, spécifique, éclairé et univoque par lequel la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Transparence :

La transparence est la condition de possibilité d'un consentement explicite et éclairé. Les entreprises ont l'obligation, et ce dès la phase de collecte, de fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données seront traitées. Ces informations doivent être fournies de façon concise, compréhensive et accessible par tous.

Responsabilité :

Il demeure qu'en cas de manquement aux obligations, la responsabilité du responsable du traitement pourra être engagée. Il s'agit d'assumer les conséquences du non-respect de ces obligations.

ENFANT

Les enfants doivent faire l'objet d'une protection renforcée.

Consentement :

Le consentement « libre, spécifique, éclairé et univoque » semble peu adapté aux enfants.

En la matière, les règles du consentement sont les suivantes pour l'offre directe de services en ligne à des enfants âgés de :

- moins de 13 ans : absence de consentement valide ;
- entre 13 et 16 ans : autorisation parentale avec possibilité pour les États d'abaisser la limite de 16 ans pour autant que cet âge ne soit pas inférieur à 13 ans ;
- 16 ans et plus : licéité du consentement sous réserve de la prise en compte d'un éventuel déséquilibre.

Pour vérifier l'expression de l'autorité parentale, le responsable de traitement doit mettre en place les moyens techniques raisonnables afin de s'assurer de l'existence d'une telle expression.

Transparence :

Le principe de transparence se voit renforcé lorsque les informations à fournir sont destinées spécifiquement à un enfant.

Toute information ou communication relative à un traitement qui les concerne devra être rédigée en des termes clairs, simples et aisément compréhensibles pour ces enfants.

Responsabilité :

Le consentement doit être accordé par une personne pouvant exercer ce qu'on appelle la « responsabilité parentale ». Le responsable de traitement est également tenu de faire tous les « efforts raisonnables » pour prouver que la personne qui fournit ce consentement dispose réellement de cette figure parentale. La vérification de la personne qui se trouve derrière l'écran incombe aussi à l'entreprise qui collecte ces données, en prenant en compte les moyens technologiques disponibles dont elle a accès.

C. Les droits subjectifs

Le RGPD instaure par ailleurs un ensemble de droits fondamentaux pour les personnes dont les données personnelles sont utilisées :

- le droit à l'information est renforcé dès le moment où les données personnelles sont collectées et à toutes les étapes du traitement des données¹²¹ ;
- le droit d'accès aux données collectées¹²² ;
- le droit à la rectification¹²³, à l'effacement des données¹²⁴ (c'est le droit à l'oubli si important pour les enfants et leur vie future) et à la limitation du traitement¹²⁵ ;
- le droit à la portabilité des données¹²⁶, c'est-à-dire le fait pour une personne d'obtenir que les informations détenues par un tiers puissent être transmises à un autre tiers ;
- le droit de s'opposer au traitement de ses données personnelles¹²⁷.

Le droit à l'oubli mérite, dans le cadre de ce travail, un exposé plus détaillé concernant les enfants.

L'article 8 du RGPD protège en amont les mineurs sur les réseaux sociaux ; tandis que l'article 17 du RGPD les protègerait en aval grâce à un droit à l'oubli numérique.

L'article 17 du RGPD, stipule explicitement que chaque personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant dans les meilleurs délais et sans retard injustifié. Ce droit n'est pas inconditionnel, car seules les données qui ne sont plus nécessaires ou qui sont illégalement collectées peuvent faire l'objet d'une telle demande. En outre, dans la mesure où le traitement est nécessaire dans l'intérêt public, le droit ne peut pas être invoqué¹²⁸.

¹²¹ Article 13 et 14 du RGPD.

¹²² Article 15 du RGPD. C.J.U.E., troisième ch., 1er octobre 2015, *Smaranda Bara et autres c. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*, C-201/14, EU:C:2015:638. Cette affaire concernait la transmission de données fiscales relatives aux revenus de travailleurs indépendants par l'administration fiscale nationale au fonds national roumain d'assurance maladie. Sur base de ces données, le paiement d'arriérés de contributions au régime d'assurance maladie a été exigé. La CJUE était invitée à déterminer si la personne concernée aurait dû être informée au préalable de l'identité du responsable du traitement et de la finalité de la transmission des données avant que celles-ci ne soient traitées par le fonds national d'assurance maladie. La CJUE a conclu que lorsqu'une administration publique d'un État membre transmet des données à caractère personnel à une autre administration publique qui traite ultérieurement ces données, les personnes concernées doivent être informées de la transmission ou du traitement.

¹²³ Article 16 du RGPD.

¹²⁴ Article 17 du RGPD.

¹²⁵ Article 18 du RGPD.

¹²⁶ Article 20 du RGPD.

¹²⁷ Article 21 du RGPD.

¹²⁸ P. VAN CLEYNENBREUGEL, « What should be forgotten? Time to make sense of Article 17 GDPR from the point of view of data controllers », 2017 (disponible sur : <https://blogdroiteuropeen.com/2017/05/25/what-should-be-forgotten-time-to-make-sense-of-article-17-gdpr-from-the-point-of-view-of-data-controllers-by-pieter-van-cleyenbreugel/>)

Le droit à l'oubli numérique a une origine prétorienne. C'est une décision de la Cour de justice de l'Union européenne qui l'a consacré : l'arrêt *Google Spain* du 13 mai 2014. Dans cette affaire, Monsieur Mario Costeja González, un ressortissant espagnol, se plaint de l'apparition de son nom sur le site Web du quotidien *La Vanguardia* lorsqu'il effectue une recherche le concernant sur le moteur de recherche Google¹²⁹.

Chapitre 1 : La notion d'oubli

Il est impératif de bien comprendre ce qui est réellement entendu par « droit à l'oubli ». L'idée n'est pas de permettre à quelqu'un de réécrire le passé et d'effacer les traces non plaisantes de son passage sur terre. L'idée est de veiller à ce que le présent d'un individu ne soit pas encombré par son passé¹³⁰. Le passé est le passé, il ne devrait pas remonter à la surface.

Le RGPD représente la première intégration du concept de « droit à l'oubli » en droit positif. Est affirmé, pour la première fois, un « droit à l'effacement » dont bénéficient les personnes concernées par les traitements de données à caractère personnel. C'est sous cette expression de « droit à l'effacement » qu'est inscrit, au rang de règlement européen, le concept de droit à l'oubli¹³¹.

Malgré sa reconnaissance explicite, la portée exacte du droit à l'oubli ne peut être déduite clairement du libellé de l'article 17 du RGPD. En effet, même une lecture superficielle de cette disposition permet d'emblée de distinguer deux interprétations différentes de ce droit. D'une part, un droit à l'oubli pourrait être lu uniquement pour incorporer un droit à un simple « effacement », c'est-à-dire la simple radiation technique des données de leur affichage dans les résultats de recherche ou les bases de données. D'autre part, une obligation plus fondamentale d'assurer la suppression permanente de ses données, une approche dite d'« oubli » pourrait également être envisagée dans ce contexte. Tout au long du RGPD, les références aux deux approches peuvent être détectées simultanément¹³².

Sandrine Carneroli, avocate au barreau de Bruxelles et spécialisée en droit des médias préfère parler d'« effacement » plutôt que d'« oubli », dès lors que ce droit n'est pas soumis au temps qui passe. Il peut être actionné dès que les données sont traitées, sans devoir attendre l'écoulement d'un laps de temps, et ce, même si le temps qui passe est pris en compte dans la décision d'accéder à la demande de déréférencement¹³³.

¹²⁹ C. BERNARD-GLANZ, « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », *C.D.R.*, 2014/3, pp. 685-717.

¹³⁰ C. DE TERWANGNE, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ? », in *Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ?*, s.l., Larcier, 2015, p.24.

¹³¹ M. RANQUET, « Le droit à l'oubli : vers un nouveau droit fondamental de l'individu ? », *Communications (Paris)*, 2019, vol. 104, n° 1, pp. 149-159.

¹³² P. VAN CLEYNENBREUGEL, *op. cit.*

¹³³ S. CARNEROLI, « Le droit à l'oubli : du devoir de mémoire au droit à l'oubli », Bruxelles, Larcier, 2016, p.72.

Le droit à l'oubli numérique renvoie au droit de demander le retrait ou l'effacement de ses données personnelles d'internet. Le but du RGPD vise non pas la protection de l'intimité de la vie privée mais bien « l'auto-détermination sur l'information »¹³⁴.

Chapitre 2 : L'infailibilité de la mémoire d'Internet

« Dieu pardonne et oublie, mais le Web jamais ! ». Cette déclaration de la Commissaire à la justice Viviane Reding résume la constatation qu'Internet conserve toutes les informations sans limite dans le temps¹³⁵.

Chez l'être humain, la mémoire est sélective. Elle oublie d'elle-même ce qui n'est pas important, à la différence d'internet qui conserve définitivement les traces de notre histoire¹³⁶.

Il y a quelques années encore, les informations susceptibles de porter atteinte à la réputation n'étaient pas diffusées à large échelle. La révolution technologique a profondément modifié ce paradigme. Grâce aux smartphones, tablettes et ordinateurs portables, il n'a jamais été aussi simple de capturer ou de créer de l'information et de la diffuser immédiatement. Les archives sont digitalisées, classées et rendues massivement accessibles. L'information est copiée, sauvegardée et transférée à une vitesse qui dépasse l'entendement humain. Le tout est indexé par des moteurs de recherche toujours plus performants qui associent contenus et personnes avec une impitoyable efficacité¹³⁷.

« Enfin, la mémoire numérique est eidétique. Elle n'oublie jamais. Rien. »¹³⁸.

Chapitre 3 : La protection spécifique des mineurs d'âge

L'article 17, paragraphe 1er, f), du RGPD consacre le droit de demander l'effacement des données à caractère personnel collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants. Dans cette hypothèse, la personne concernée pourra, à tout moment, et sans qu'aucune justification ne doive être fournie, demander que les données en cause soit effacées, nonobstant le fait qu'elle n'est plus un enfant¹³⁹.

¹³⁴ S. CARNEROLI, *ibid.*, p.8.

¹³⁵ C. DE TERWANGNE, *op. cit.*, p.26.

¹³⁶ S. CARNEROLI, *op. cit.*, p.7.

¹³⁷ A. CASSART et J.-F. HENROTTE, « E-réputation : vers une amnésie sélective ? », in *Pas de droit sans technologie* (sous la dir. de J.-F. HENROTTE et F. JONGEN), Bruxelles, Larcier, 2015, p. 10.

¹³⁸ A. CASSART et J.-F. HENROTTE, *ibid.*

¹³⁹ TOMBAL, T., « Les droits de la personne concernée dans le RGPD », in *Les droits de la personne concernée dans le RGPD*, s.l., Larcier, 2018, p.415, p.557.

Le considérant 65 du RGPD précise que ce droit à l’effacement est pertinent¹⁴⁰ lorsque la personne concernée a donné son consentement à l’époque où elle était enfant et n’était pas pleinement consciente des risques inhérents au traitement, et qu’elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l’internet¹⁴¹.

TITRE 2 : Directive 2018/1808 du 2 octobre 2018 relative à la fourniture de services de médias audiovisuels (Directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché

Chapitre 1 : Définitions et objectif

Le paysage audiovisuel a considérablement évolué en moins d'une décennie. Au lieu d'être assis devant le poste de télévision familial, des millions d'Européens, notamment les jeunes, regardent des contenus en ligne, à la demande et sur différents appareils mobiles¹⁴².

La Commission européenne a présenté le 25 mai 2016 une proposition de révision de la Directive sur les services de médias audiovisuels (Directive SMA)¹⁴³. La publication de cette proposition, qui a fait l’objet d’un premier examen par le Conseil des Ministres le 31 mai 2016 et a du être examiné dans les mois à venir par le Parlement européen, puis transposée en droit national par les Etats membres, constitue un moment important dans l’évolution de la réglementation européenne, à l’heure où les offres de service à la demande sont arrivées à maturité et où les pratiques des consommateurs, en particulier des jeunes, évoluent très rapidement¹⁴⁴.

C’est alors au début du mois de juin 2018 que le projet de révision de la directive Service de Médias audiovisuels (SMA) a fait l’objet d’un accord entre les trois principales branches du pouvoir législatif européen. Cet accord permettra de moderniser le cadre juridique du secteur

¹⁴⁰ G. MATHIEU et A.-C. RASSON, « Les droits de l’enfant dans l’environnement numérique : à la recherche d’un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l’environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018, p. 423.

¹⁴¹ A. BAMDE, « RGPD: Le droit à l’effacement ou le “droit à l’oubli” », disponible sur www.aurelienbamde.com, 2 janvier 2019

¹⁴² Commission européenne, fiche d’information, Marché unique numérique - la commission met à jour la réglementation de l’UE dans le domaine de l’audiovisuel et présente une approche ciblée ds plateformes en ligne, 25 mai 2016 (disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_16_1895).

¹⁴³ Sous la Directive 2010/13/UE, la Cour de justice de l’Union européenne a eu l’occasion, dans un arrêt rendu le 21 octobre 2015, de définir la notion de « service de médias audiovisuels » et de poser des critères permettant l’application uniforme de cette notion par les juridictions des Etats membres. C.J.U.E., 21 octobre 2015, *New Media Online GmbH c/ Bundeskommunikationssenat*, aff. C-347/14, EU:C:2015:434.

¹⁴⁴ A. LANGE-MÉDART, « Vers une révision a minima de la directive SMA », *Enjeux de l’information et de la communication*, 2016, vol. 17-, vol. 2, n° 2, pp. 91-112.

audiovisuel européen avec, pour objectif, celui d'assurer un meilleur équilibre entre les différents acteurs du secteur audiovisuel¹⁴⁵.

« SMA » signifie Service¹⁴⁶ de Médias Audiovisuels¹⁴⁷. On distingue deux types de services de médias audiovisuels :

- les services linéaires de télévision ;
- les services non-linéaires, qui désignent les services de contenus audiovisuels à la demande, où le contenu comme le moment de son visionnage est choisi par l'utilisateur. Il s'agit par exemple de Netflix¹⁴⁸.

En son article 1er, ladite directive qualifie de « *service de médias audiovisuels* » celui qui « *relève de la responsabilité éditoriale d'un fournisseur de services de médias et dont l'objet principal est la fourniture de programmes dans le but d'informer, de divertir ou d'éduquer le grand public, par des réseaux de communication électroniques* ». Elle y indique qu'« *un service de médias audiovisuels est soit une émission télévisée [...] soit un service de médias audiovisuels à la demande* »¹⁴⁹.

En outre, la nouvelle directive SMA intégrera dans son champ, aux côtés des Services de Médias Audiovisuels, les plateformes de partage de vidéos, les réseaux sociaux et les plateformes de vidéos de direct.

La nouvelle directive va entraîner d'importantes modifications sur cette matière¹⁵⁰. En 10 ans, l'offre s'est transformée. Il était temps de réviser et de s'adapter aux nouveaux modes de « *consommation* » des contenus culturels¹⁵¹.

¹⁴⁵ Conseil de l'UE, communiqué de presse, Services de médias audiovisuels: accord sur une directive visant à protéger les mineurs, stimuler la compétitivité et promouvoir les contenus européens, 2018 (disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2018/06/13/audiovisual-media-services-agreement-on-a-new-directive-to-boost-competitiveness-and-promote-european-content/>)

¹⁴⁶ La notion de « service » a déjà été énoncée dans la RGPD. Nous ferons une brève analyse de comparaison entre les deux instruments européens au Titre 3.

¹⁴⁷ Selon la Cour de justice de l'Union européenne, en son arrêt du 21 février 2018, la notion de « service de médias audiovisuels » ne couvre ni une chaîne de vidéos, telle que mise en ligne sur YouTube, « *sur laquelle les utilisateurs d'Internet peuvent consulter de courtes vidéos promotionnelles* », ni encore moins « *une seule de ces vidéos prise isolément* ». C.J.U.E., 21 février, *Peugeot Deutschland GmbH contre Deutsche Umwelthilfe eV*, aff. C-132/17, EU:C:2018:85.

¹⁴⁸ Conseil Supérieur de l'Audiovisuel, « Régulation audiovisuelle de l'UE : La nouvelle directive SMA en 5 questions », 9 mai 2018 (disponible sur : <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Regulation-audiovisuelle-de-l-UE-La-nouvelle-directive-SMA-en-5-questions>).

¹⁴⁹ E. DERIEUX, « Vidéos en ligne : « service de médias audiovisuels » ou « documentation promotionnelle » ? », La revue européenne des médias et du numérique, n°46-47 printemps-été 2018 (disponible sur : <https://la-rem.eu/2018/09/videos-en-ligne-service-de-medias-audiovisuels-ou-documentation-promotionnelle/>).

¹⁵⁰ G. THIRY, Régulation, « La protection des mineurs sur les plateformes de partage vidéo : les prémisses d'un grand chantier ! », 2020 (disponible sur <https://regulation.be/2020/03/05/la-protection-des-mineurs-sur-les-plateformes-de-partage-video%E2%80%AF-les-premisses-dun-grand-chantier%E2%80%AF/>)

¹⁵¹ M. COCK, Droit & Technologies, « La directive « médias audiovisuels » sur le point d'être réformée », 2018 (disponible sur <https://www.droit-technologie.org/actualites/directive-medias-audiovisuels-point-detre-reformee/>)

Le changement qui nous intéressera dans le cadre de cette étude est la protection renforcée des mineurs, notamment en matière de publicité, de placement de produit et de l'usage fait de leur données, que nous analyserons au chapitre 2.

La directive SMA vise à créer un marché unique des services de médias audiovisuels dans l'Union européenne et à en assurer le bon fonctionnement, tout en contribuant à la promotion de la diversité culturelle et en garantissant un niveau adéquat de protection des consommateurs et des enfants.

Le considérant 4 de la directive (UE) 2018/1808 reconnaît que « les services de plateformes de partage de vidéos fournissent un contenu audiovisuel qui est de plus en plus consulté par le grand public, en particulier les jeunes. Cela vaut également pour les services de médias sociaux, qui sont devenus un vecteur important de partage de l'information, de divertissement et d'éducation, notamment en fournissant un accès à des programmes et à des vidéos créées par l'utilisateur¹⁵².

Par conséquent, afin de protéger les mineurs des contenus préjudiciables et de mettre l'ensemble des citoyens à l'abri des contenus incitant à la haine, à la violence et au terrorisme, ces services devraient répondre à la définition d'un « service de plateformes de partage de vidéos »¹⁵³.

Par conséquent, il est clair que certains services de médias sociaux relèvent du champ d'application des nouvelles règles relatives aux plateformes de partage de vidéos lorsqu'ils répondent à certains critères.

Selon le texte initial de la Commission, un service de plateforme de partage de vidéos « *consiste à stocker une grande quantité de programmes ou de vidéos créées par les utilisateurs, qui ne relèvent pas de la responsabilité éditoriale du fournisseur de la plateforme de partage de vidéos* ».

Jusqu'alors écartées de la directive SMA, les plateformes de partages vidéo sont désormais concernées par certaines obligations. Les médias sociaux sont également intégrés lorsque la fourniture de programmes audiovisuels ou de vidéos générées par les utilisateurs constituent une fonctionnalité essentielle de ceux-ci. Le projet initial de la directive prévoyait de limiter ces obligations à la protection des mineurs.

La directive SMA vise à renforcer la protection des utilisateurs, en particulier les mineurs, contre certaines formes de contenu audiovisuel en ligne illégal et préjudiciable. C'est la raison pour laquelle le champ d'application de la directive SMA a été élargi afin d'imposer certaines obligations aux fournisseurs de plateformes de partage de vidéos¹⁵⁴.

¹⁵² Lignes directrices pour l'application pratique du critère relatif à la fonctionnalité essentielle figurant dans la définition d'un «service de plateformes de partage de vidéos» établie par la directive «Service de médias audiovisuels», 2020.

¹⁵³ Considérant 4 de la Directive SMA.

¹⁵⁴ Lignes directrices pour l'application pratique du critère relatif à la fonctionnalité essentielle figurant dans la définition d'un «service de plateformes de partage de vidéos» établie par la directive «Service de médias audiovisuels», 2020.

Chapitre 2 : La priorité de la nouvelle Directive : la protection des mineurs

Les pays de l'UE doivent prendre des mesures appropriées pour garantir que les programmes susceptibles de « nuire à l'épanouissement physique, mental ou moral des mineurs » ne soient mis à disposition que dans des conditions telles que les mineurs ne puissent normalement pas les entendre ni les voir, notamment à travers le choix de l'heure de l'émission, l'utilisation d'outils permettant de vérifier l'âge ou d'autres mesures techniques proportionnées au préjudice que pourrait causer le programme.

Les contenus les plus préjudiciables, tels que la pornographie et la violence gratuite, font l'objet des mesures les plus strictes. Les mineurs bénéficient également d'un niveau plus élevé de protection en ligne : les plateformes de partage de vidéos doivent ainsi mettre en place des mesures pour les protéger des contenus préjudiciables. Le placement de produit est également interdit dans les émissions destinées aux enfants. Concernant la publicité à destination des enfants promouvant, inopportunément, des aliments et boissons à forte teneur en matières grasses, en sel et en sucres, les pays de l'UE doivent, au moyen de codes de conduite, encourager l'utilisation de l'autorégulation et de la corégulation¹⁵⁵.

Les enfants délaissent de plus en plus la télévision au profit des vidéos à la demande et en ligne. Or l'ancienne directive SMA les protégeait davantage lorsqu'ils regardaient la télévision que dans l'environnement en ligne. Cette incohérence a été désormais corrigée¹⁵⁶.

Comme développé ci-avant, le champ d'application de la Directive est élargi aux plateformes de partage vidéo en ce qui concerne la protection des mineurs. Les plateformes qui organisent une grande quantité de vidéos devront protéger les mineurs des contenus préjudiciables. Parmi les mesures détaillées figurent des systèmes de contrôle parental ou des outils qui permettent aux utilisateurs d'indiquer et de signaler les contenus préjudiciables ou qui concernent la vérification de l'âge¹⁵⁷.

En résumé, pour la protection des mineurs *stricto sensu*, les évolutions portent principalement sur trois points :

- Premièrement, les contenus « les plus préjudiciables » (pornographie et violence gratuite) seront soumis aux mesures les plus strictes¹⁵⁸ ;
- Deuxièmement, les éditeurs devront fournir une information sur la nature du contenu qui justifie une signalétique relative à l'âge : sexe, violence,...¹⁵⁹ ;

¹⁵⁵ Synthèse du document : Directive 2018/1808 du 2 octobre 2018 relative à la fourniture de services de médias audiovisuels (Directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché.

¹⁵⁶ Commission européenne, fiche d'information, *op. cit.*

¹⁵⁷ A. LANGE-MÉDART, *op. cit.*, pp. 91-112.

¹⁵⁸ Article 6 *bis* de la Directive.

¹⁵⁹ Article 28 *ter*, d) de la Directive.

- Et troisièmement, les données personnelles des mineurs acquises par les entreprises via les systèmes de protection mis en place ne peuvent être utilisées à des fins commerciales¹⁶⁰.

Pour s'assurer que ces mesures résistent à l'épreuve du temps et sont efficaces, la Commission invitera toutes les plateformes de partage de vidéos à coopérer au sein de l'Alliance¹⁶¹ pour une meilleure protection des mineurs en ligne, en vue d'élaborer un code déontologique pour l'industrie¹⁶².

TITRE 3 : Un manque de cohérence entre d'une part, le RGPD et d'autre part, la Directive SMA ?

Nous nous tâcherons d'établir une conclusion quant à la réponse à apporter à la question suivante : « *Y a-t-il un manque de cohérence entre d'une part, le Règlement Général sur la Protection des Données et d'autre part, la Directive Services de médias audiovisuels ?* »

Chapitre 1 : Les objectifs

La Directive SMA s'inscrit dans la mouvance du RGPD, et dans une volonté assumée d'imposer un standard européen normatif aux géants du numérique. La Directive SMA met l'accent sur la protection des mineurs, particulièrement exposés aux risques inhérents au visionnage des médias audiovisuels. Ainsi, dans la lignée du RGPD, elle exclut toute exploitation des données personnelles des mineurs à des fins commerciales¹⁶³.

Le considérant 21 de la Directive SMA affirme que : « *Le règlement (UE) 2016/679 du Parlement européen et du Conseil affirme que les enfants méritent une protection spécifique en ce qui concerne le traitement de leurs données à caractère personnel. La mise en place, par les fournisseurs de services de médias, de mécanismes de protection des enfants entraîne inévitablement le traitement de données à caractère personnel de mineurs. Étant donné que de tels mécanismes visent à protéger les enfants, les données à caractère personnel de mineurs traitées dans le cadre de ces mesures techniques de protection des enfants ne devraient pas être utilisées à des fins commerciales.* »

Le Parlement européen a obtenu qu'un mécanisme de protection des données personnelles pour les enfants soit introduit dans la Directive SMA. Il prévoit : « *des mesures garantissant que les données collectées par les fournisseurs de médias audiovisuels ne seront pas*

¹⁶⁰ Articles 6 bis, 7 ter, et 28 ter de la Directive

¹⁶¹ « *L'Alliance pour une meilleure protection des mineurs en ligne* » (ci-après « *l'Alliance* »). L'Alliance, officiellement lancée en 2017, est une plateforme multi-acteurs qui permet aux entreprises membres de prendre une série d'engagements visant à faire face aux nouveaux risques auxquels les mineurs s'exposent en ligne. Commission européenne, Evaluation de la mise en œuvre de l'alliance pour une meilleure protection des mineurs en ligne, 2019 (disponible sur : <https://op.europa.eu/fr/publication-detail/-/publication/66a6685b-2378-11e9-8d04-01aa75ed71a1/language-fr/format-PDF/source-93323895>).

¹⁶² A. LANGE-MÉDART, *op. cit.*, pp. 91–112.

¹⁶³ E. PIERRAT et L. KRUGER, « La transposition en droit français de la directive SMA », Issue (disponible sur : https://issuu.com/ecrantotal/docs/eth_1318/s/11825348)

exploitées pour un usage commercial, notamment pour le profilage¹⁶⁴ ou la publicité ciblée sur le comportement »¹⁶⁵.

Chapitre 2 : Le règlement ou la directive

L'Union européenne peut prendre des décisions juridiques de plusieurs manières, les deux plus courantes étant les règlements et les directives :

- Les règlements sont des lois de l'UE qui s'appliquent automatiquement et uniformément à tous les pays de l'UE sans qu'il soit nécessaire d'interpréter et de mettre en œuvre au niveau national. Tout ce qui est adopté en vertu d'un règlement sera contraignant et immédiatement applicable dans toute l'Europe.
- Les directives, en revanche, sont des actes juridiques de l'UE que chaque pays doit adopter et mettre en œuvre à sa manière au niveau national.

Après validation de la directive SMA¹⁶⁶ par les institutions européennes, les États membres peuvent choisir de transposer dans leur droit national cette directive en l'état, ou d'adopter des règles plus strictes dans les cas où la directive ne l'interdit pas expressément. La directive SMA permet donc d'établir un socle minimal de règles communes qui ménage tout de même les particularismes nationaux¹⁶⁷.

Les États membres ont été tenus de transposer la directive SMA révisée pour le 19 septembre 2020 au plus tard, y compris les nouvelles règles relatives aux plateformes de partage de vidéos et aux œuvres européennes. À compter de cette date, la Commission suivra les progrès accomplis par les États membres dans la transposition et la mise en œuvre de la directive pour veiller au respect des nouvelles règles¹⁶⁸.

Le choix d'opter pour un règlement concernant le RGPD et non pour une directive n'est pas sans raison. Tandis qu'une directive doit être transposée dans chacune des législations nationales des États membres, un règlement jouit d'une applicabilité directe¹⁶⁹, il s'applique

¹⁶⁴ C'est une opération particulière de traitement des données personnelles qui consiste à analyser l'ensemble des données d'une personne et à les classer selon un profil type. L'utilisation du profilage répond souvent à des fins de marketing direct ou indirect. Il permet de cibler les personnes susceptibles d'acheter tel ou tel produit ou service pour les encourager à « passer à l'acte » en les informant de l'existence de produits ou services qui leur correspondent.

¹⁶⁵ M. REES, « Audiovisuel : YouTube, Facebook, Netflix, cibles de choix de la future directive SMA », 2018 (disponible sur <https://www.nextinpact.com/article/28335/106528-audiovisuel-youtube-facebook-netflix-cibles-choix-future-directive-sma>)

¹⁶⁶ Commission européenne, Lignes directrices sur la directive «Services de médias audiovisuels» révisée - Questions et réponses, 2 juillet 2020, Bruxelles (disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1208).

¹⁶⁷ Conseil Supérieur de l'Audiovisuel, « Régulation audiovisuelle de l'UE : La nouvelle directive SMA en 5 questions », 9 mai 2018 (disponible sur : <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Regulation-audiovisuelle-de-l-UE-La-nouvelle-directive-SMA-en-5-questions>).

¹⁶⁸ Commission européenne, Lignes directrices sur la directive «Services de médias audiovisuels» révisée - Questions et réponses, 2 juillet 2020, Bruxelles (disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1208).

¹⁶⁹ Art. 288 du Traité sur le fonctionnement de l'Union européenne.

sans transposition dans la législation nationale. Ce règlement européen permet donc une harmonisation des règles de l'Union européenne concernant la protection des données personnelles, ce que ne permettrait pas une directive, qui amènerait à des incohérences compte tenu des différentes manières de transposer les règles dans les États membres. Le RGPD a une portée générale, il s'applique de la même manière à tout le territoire de l'Union européenne. Il garantit une sécurité juridique en évitant des divergences.

Le but est donc de lutter contre la disparité des règles sur la protection des données à caractère personnel pouvant exister entre plusieurs pays européens, du fait de leur transposition. Même si, il est vrai que sur certains points, le règlement offre la possibilité aux États d'adapter leur législation nationale aux usages propres en matière de protection des données à caractère personnel¹⁷⁰.

La vulnérabilité des mineurs suppose une protection accrue de leurs données, notamment à l'ère de leur surexposition sur internet. Cependant, l'applicabilité des règles issues du RGPD, questionne¹⁷¹.

D'une part, le RGPD, en laissant la possibilité aux États membres de fixer comme seuil l'âge de leur choix compris entre 13 ans et 16 ans, fait naître des disparités entre états qui sont susceptibles de complexifier les actions des services de la société d'information. Ainsi, ces différences doivent être prises en compte et intégrées dans les conditions générales d'utilisation ou conditions générales de vente de la société, et ce pour chaque Etat.

D'autre part, comment garantir l'âge effectif des mineurs ou encore la collecte du consentement du titulaire de l'autorité parentale ? C'est ce que nous avons évoqué dans l'exposé concernant le principe de responsabilité qui est une faiblesse du Règlement, quand il s'agit d'un enfant. La conciliation des procédés de vérification de l'identité des utilisateurs avec la réglementation sur la protection des données personnelles pose aujourd'hui problème, notamment s'agissant du principe de minimisation de la collecte des données¹⁷².

Quoi qu'il en soit, le RGPD est un règlement contraignant dans tous les États membres de l'UE depuis mai 2018. Il a un champ d'application beaucoup plus large qu'une directive.

En effet, le règlement porte sur la protection des données indépendamment du type de données (pas seulement les informations numériques des utilisateurs) et la manière dont les sociétés doivent garantir la transparence et documenter le consentement des utilisateurs.

Cependant, la directive SMA est un instrument européen qui traite principalement des plateformes offrant de l'audiovisuel. Cette directive est basée essentiellement sur un certain type de responsable de traitement, un responsable de traitement distribuant de l'audiovisuel.

¹⁷⁰ S. CARNEROLI, *op.cit.*, p.71.

¹⁷¹ Grande Bibliothèque du Droit, La protection des données personnelles des mineurs (fr), 3 avril 2020 (disponible sur : [https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_\(fr\)](https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_(fr)))

¹⁷² Grande Bibliothèque du Droit, *ibid.*

Chapitre 3 : Une complémentarité

L'article 8 du RGPD consacré à la protection spécifique des données personnelles des enfants, s'applique uniquement lorsque le traitement est lié à l'offre directe de « services de la société de l'information » à un enfant.

Comme exposé ci-avant, la notion de « services de la société de l'information » est définie à l'article 4, paragraphe 25, du RGPD.

Cet article nous énonce que le « service de la société de l'information » est un service au sens de l'article 1^{er}, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil¹⁷³ : « *« service », tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Aux fins de la présente définition, on entend par:*

- *« à distance », un service fourni sans que les parties soient simultanément présentes;*
- *« par voie électronique », un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques;*
- *« à la demande individuelle d'un destinataire de services », un service fourni par transmission de données sur demande individuelle. »*

En outre, le règlement s'applique sans préjudice de l'application de la directive 2000/31/CE du Parlement européen et du Conseil¹⁷⁴, et notamment du régime de responsabilité des prestataires de services intermédiaires prévu dans ses articles 12 à 15. Cette directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

Cependant dans la directive SMA, il est également question de « service ». Dans cette dernière, il est question de « fournisseurs de plateformes de partage de vidéos ». Ceux-ci fournissent des services de la société de l'information également au sens de la directive 2000/31/CE.

La directive 2000/31 prévoit des règles applicables aux services de la société de l'information, que sont les services de médias audiovisuels à la demande, mais pas les SMA linéaires¹⁷⁵.

¹⁷³ Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, L 241/1, 17 septembre 2015.

¹⁷⁴ Directive (UE) 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.C.E.*, L 178, 17 juillet 2000.

¹⁷⁵ Considérant 18 de la directive 2000/31 : « *Les services de télévision au sens de la directive 89/552/CEE et de radiodiffusion ne sont pas des services de la société de l'information car ils ne sont pas fournis sur demande individuelle. En revanche, les services transmis de point à point, tels que les services de vidéo à la demande ou la fourniture de communications commerciales par courrier électronique constituent des services de la société de l'information.* » Cela a été dernièrement confirmé par le considérant 44 de la directive 2018/1808.

A noter que les règles de l'article 28 *ter* de la directive SMA s'appliquent « sans préjudice des articles 12 à 15 de la directive 2000/31/CE », comme le relève le considérant 48, 1^{ère} phrase, de la directive 2018/1808 révisant la directive SMA¹⁷⁶.

Il semble qu'ils ne permettent pas d'établir, une réelle incohérence entre ces deux instruments, mais plutôt une complémentarité.

Cependant, peut-être, l'Union européenne aurait dû non pas voter une directive SMA, mais aurait-il été préférable de voter un Règlement « obligatoire dans tous ses éléments » et « directement applicable dans tout État membre »¹⁷⁷ de l'Union européenne afin d'éviter une disparité de législations nationales et un soucis de mise en oeuvre des instruments.

Mieux encore, la dangerosité des mineurs sur les plateformes audiovisuelles et sur les réseaux sociaux grandissant, l'Union européenne pourrait réfléchir à un Règlement ne concernant que la protection spécifique des mineurs en ce qui concerne, tant leurs données personnelles, que leur protection sur du contenu audiovisuel. Ne serait-il pas mieux d'avoir un cadre juridique européen plus cohérent consacré explicitement et uniquement aux mineurs d'âge en droit numérique de l'Union européenne ?

Dans le cadre de ce travail, nous avons étudié les risques de la violation du droit à la vie privée des enfants en ligne, la protection de leurs données personnelles, ainsi que les risques des contenus audiovisuels. D'autres risques peuvent être abordés. Nous songeons, notamment, à l'exposition à des contenus inappropriés, à la pédopornographie et à la sollicitation à caractère sexuel ou encore au cyber-harcèlement. Le sujet est énorme concernant la protection des enfants. C'est pourquoi, un instrument européen regroupant tous les aspects de la protection de l'enfance est nécessaire.

Chapitre 4 : Un avenir numérique pour l'Europe

Lors de la réunion extraordinaire du Conseil européen qui s'est tenue les 1^{er} et 2 octobre 2020¹⁷⁸, les dirigeants de l'UE ont invité la Commission à présenter une « *boussole numérique* » globale présentant les ambitions numériques concrètes de l'UE à l'horizon 2030. La Commission a présenté sa proposition en mars¹⁷⁹ de cette année¹⁸⁰.

¹⁷⁶ Conseil Supérieur de l'Audiovisuel, « Note d'orientation du CSA sur la lutte contre certaines formes de contenus illicites sur Internet, en particulier le discours de haine », 2020 (disponible sur : https://www.csa.be/wp-content/uploads/2020/02/Note-dorientation-contenus-illicites_février-2020.pdf).

¹⁷⁷ Article 288 TFUE.

¹⁷⁸ Conseil de l'UE, Vidéoconférence des ministres des télécommunications, 7 décembre 2020 (disponible sur : <https://www.consilium.europa.eu/fr/meetings/tte/2020/12/07/>).

¹⁷⁹ Conseil européen, Vidéoconférence des membres du Conseil européen, 25 mars 2021 (disponible sur : <https://www.consilium.europa.eu/fr/meetings/european-council/2021/03/25/>).

¹⁸⁰ Conseil européen et Conseil de l'UE, « Un avenir numérique pour l'Europe », 2021 (disponible sur : <https://www.consilium.europa.eu/fr/policies/a-digital-future-for-europe/>).

Les technologies numériques modifient non seulement la façon dont les gens communiquent, mais aussi, plus généralement, leur façon de vivre et de travailler. La situation créée par la pandémie de la COVID-19 a incité l'UE à travailler à accélérer la transition technologique.

En effet, la pandémie de la COVID-19 a rendu encore plus pressante la nécessité d'accélérer la transition numérique en Europe¹⁸¹.

Parmi les sujets abordés dans cette proposition, plusieurs nous intéressent dans le cadre de ce travail¹⁸².

L'Union européenne vise à protéger et à renforcer sa souveraineté numérique tout en promouvant les valeurs communes de l'UE et en respectant les libertés fondamentales, y compris la protection des données et de la vie privée, la sûreté et la sécurité¹⁸³.

Les plateformes en ligne constituent un élément important du marché et de l'économie numériques de l'UE. Les États membres de l'UE reconnaissent la nécessité de renforcer, de moderniser et de clarifier les règles applicables aux services numériques afin d'assurer la sécurité des utilisateurs en ligne¹⁸⁴.

Dans l'environnement numérique, les risques de porter atteinte à la vie privée des enfants sont importants¹⁸⁵.

En outre, le 29 avril 2021, un accord informel avec le Parlement européen a eu lieu touchant la lutte contre les abus commis contre des enfants en ligne¹⁸⁶. « *La protection des enfants contre toute forme de violence ou d'abus est primordiale pour l'UE* » a dit Pedro Siza Vieira, ministre d'État portugais à l'économie et à la transition numérique, président du Conseil.

L'accord prévoit une dérogation aux articles 5, paragraphe 1, et 6, paragraphe 1, de la directive sur la vie privée en ligne¹⁸⁷, afin de permettre aux fournisseurs de continuer à

¹⁸¹ Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions empty, « 2030 Digital Compass: the European way for the Digital Decade », 9 mars 2021 (disponible sur : <https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX%3A52021DC0118>).

¹⁸² Conseil européen et Conseil de l'UE, *op. cit.*

¹⁸³ Communication de la commission, du parlement européen, du conseil, au économique économique et social européen et au comité des régions, « Une stratégie européenne pour les données », 19 février 2020 (disponible sur : <https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>).

¹⁸⁴ Proposal for a regulation of the european parliament and of the council on contestable and fair markets in the digital sector (Digital Markets Act), 15 décembre 2020 (disponible sur : https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf).

¹⁸⁵ G. MATHIEU et A.-C. RASSON, « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l'environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018, p.424.

¹⁸⁶ Conseil de l'UE, Communiqué de presse, « Combating child abuse online – informal deal with European Parliament on temporary rules », 29 avril 2021.

¹⁸⁷ Directive (UE) 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »), *J.O.U.E.*, L 201, 31 juillet 2002.

détecter, supprimer et signaler le matériel d'abus sexuel d'enfants. La Charte des droits fondamentaux et le RGPD continueront de s'appliquer de toute façon, et un certain nombre de garanties supplémentaires garantiront le respect de la vie privée en ligne. La Commission a annoncé qu'elle proposera une législation globale pour lutter contre les abus sexuels sur enfants en ligne d'ici le deuxième trimestre de 2021. Cette législation visera à fournir une solution à long terme pour remplacer cette mesure temporaire.

Conclusion générale

Echanger, enregistrer, trier ou traiter les données personnelles acquises par une personne sont des activités anciennes essentielles sur lesquelles nos sociétés et leur développement reposent. C'était la fonction dévolue aux Scribes de l'époque égyptienne ou encore aux moines copistes dans l'Europe du Moyen-âge. Un exemple de traitement de données traditionnel est celui du recensement de la population.

Et puis Internet est né et en permettant des échanges libres d'informations sans précédent, cet outil est devenu un instrument d'émancipation, y compris pour les enfants.

Internet est un outil mythique qui nous ouvre les portes du savoir, de la connaissance et de l'information comme jamais auparavant. Qui aurait pu prédire il y a dix ans que la plupart des enfants seraient capables d'envoyer des photos à des personnes à l'autre bout de la planète avec un simple téléphone ?

En réalité, nos sociétés ne peuvent pas fonctionner sans l'échange de données personnelles. Aristote disait déjà : « *L'homme est un animal social* ». Ces échanges forgent l'identité et la personnalité de nos enfants, ils les protègent et sont indispensables à leur vie quotidienne : inscription à l'école, achat en ligne, apprentissage, sport, partage avec les ami(e)s, contacts avec la famille, et liens de contact malgré la distance, en particulier durant cette période de crise sanitaire due à la COVID-19.

En réalité, protéger les données personnelles des enfants et protéger ceux-ci de contenus dangereux audiovisuels, implique une véritable éducation des enfants au monde numérique, qui fait défaut dans la plupart des programmes scolaires, et qui ne se limiterait pas à un exposé des dangers réels ou supposés mais qui porterait bel et bien sur le contenu du monde numérique, sur son modèle de fonctionnement économique et sur les enjeux qu'il pose notamment en terme de droits et libertés fondamentaux¹⁸⁸.

Et même si des instruments internationaux, européens et nationaux protègent nos enfants contre leurs imprudences d'une part, concernant leurs données personnelles et, d'autre part, sur du contenu audiovisuel, le Conseil de l'Europe rappelle que : « *Les enfants doivent avant tout être soutenus et accompagnés dans la découverte et l'utilisation de l'environnement numérique afin d'apprendre à se protéger eux-mêmes. Et l'environnement numérique devrait vraiment être adapté à leurs besoins spécifiques, surtout pour les plus jeunes* »¹⁸⁹.

¹⁸⁸ A. CARRÉ, sous la supervision de G. MATHIEU et B. VAN KEIRSBILCK, *op. cit.*, p.30. (disponible sur : <https://www.dei-belgique.be/index.php/component/jdownloads/send/46-la-protection-des-donnees/389-la-protection-des-donnees-des-enfants-dans-la-monde-numerique.html>)

¹⁸⁹ Conseil de l'Europe, Recommandation du Comité des Ministres aux États membres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, adoptée par le Comité des Ministres, le 4 juillet 2018 (disponible sur : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c153b).

Bibliographie

Législation

a) Internationale

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi 13 mai 1955, *M.B.*, 19 août 1955.

Convention relative aux droits de l'enfant, adoptée à New York le 20 novembre 1989, approuvée par la loi du 25 novembre 1991, *M.B.*, 17 janvier 1992.

b) Européenne

Convention européenne des Droits de l'Homme.

Traité sur le fonctionnement de l'Union européenne (version consolidée), *J.O.U.E.*, 26 octobre 2012, C 326.

Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C 326.

Directive (UE) 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, *J.O.C.E.*, L 281, 23 novembre 1995.

Directive (UE) 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.C.E.*, L 178, 17 juillet 2000.

Directive (UE) 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »), *J.O.U.E.*, L 201, 31 juillet 2002.

Directive 2010/13/UE du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels, *J.O.U.E.*, L 95, 15 avril 2010.

Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, L 241/1, 17 septembre 2015.

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), *J.O.U.E.*, L 119, du 4 mai 2016.

Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels»), compte tenu de l'évolution des réalités du marché, *J.O.U.E.*, L 303, 28 novembre 2018.

[Projet de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE \(règlement "vie privée et communications électroniques"\) - mandat du Conseil.](#)

c) Soft law

Recommandation du Parlement européen et du Conseil du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne.

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), Bruxelles, 2012.

Groupe de l'article 29, « Avis n°3/2010 sur le principe de la responsabilité », WP 173.

Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous- traitant », WP 169.

Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01.

Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01.

Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187.

Groupe de l'article 29, « Avis n° 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel », WP 48.

Communiqué de presse, De nouvelles règles sur la protection des données placent les citoyens aux commandes, 17 décembre 2015 (disponible sur : <https://www.europarl.europa.eu/news/fr/press-room/20151217IPR08112/protection-des-donnees-les-citoyens-aux-commandes>).

Commission européenne, fiche d'information, Marché unique numérique - la commission met à jour la réglementation de l'UE dans le domaine de l'audiovisuel et présente une approche ciblée ds plateformes en ligne, 25 mai 2016 (disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_16_1895).

Conseil de l'UE, communiqué de presse, Services de médias audiovisuels: accord sur une directive visant à protéger les mineurs, stimuler la compétitivité et promouvoir les contenus européens, 2018 (disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2018/06/13/audiovisual-media-services-agreement-on-a-new-directive-to-boost-competitiveness-and-promote-european-content/>)

Conseil de l'Europe, Recommandation du Comité des Ministres aux États membres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, adoptée par le Comité des Ministres, le 4 juillet 2018 (disponible sur : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c153b).

Conseil de l'UE, Vidéoconférence des ministres des télécommunications, 7 décembre 2020 (disponible sur : <https://www.consilium.europa.eu/fr/meetings/tte/2020/12/07/>).

Comité des Ministres du Conseil de l'Europe, Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, Recommandation CM/REC(2018)7 (disponible sur : <http://rm.coe.int/lignes-directrices-relatives-au-respect-a-la-protection-et-a-la-realisation/16808d881b>).

Communiqué de presse, Garante per la protezione dei dati personali, Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network (disponible sur : <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9508923>).

Commission européenne, Evaluation de la mise en œuvre de l'alliance pour une meilleure protection des mineurs en ligne, 2019 (disponible sur : <https://op.europa.eu/fr/publication-detail/-/publication/66a6685b-2378-11e9-8d04-01aa75ed71a1/language-fr/format-PDF/source-93323895>).

Autorité de protection des données belge, Consentement (disponible sur <https://www.autoriteprotectiondonnees.be/professionnel/rgpd/bases-juridiques/consentement>).

Lignes directrices pour l'application pratique du critère relatif à la fonctionnalité essentielle figurant dans la définition d'un «service de plateformes de partage de vidéos» établie par la directive « Service de médias audiovisuels », 2020.

Commission européenne, Lignes directrices sur la directive «Services de médias audiovisuels» révisée - Questions et réponses, 2 juillet 2020, Bruxelles (disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1208).

Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions empty, « 2030 Digital Compass: the European way for the Digital Decade », 9 mars 2021 (disponible sur : <https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX%3A52021DC0118>).

Communication de la commission, du parlement européen, du conseil, au économique économique et social européen et au comité des régions, « Une stratégie européenne pour les données », 19 février 2020 (disponible sur : <https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>).

Conseil de l'UE, Communiqué de presse, Confidentialité des communications électroniques: le Conseil arrête sa position sur des règles en matière de vie privée et de communications électroniques, 10 février 2021 (disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-privacy-rules/>).

Conseil européen et Conseil de l'UE, « Un avenir numérique pour l'Europe », 2021 (disponible sur : <https://www.consilium.europa.eu/fr/policies/a-digital-future-for-europe/>).

Conseil de l'UE, Communiqué de presse, « Combating child abuse online – informal deal with European Parliament on temporary rules », 29 avril 2021.

Jurisprudence

a) Cour de justice de l'Union européenne

C.J.U.E., troisième ch., 13 juillet 1989, *Hubert Wachauf contre Bundesamt für Ernährung und Forstwirtschaft*, aff. C-5/88, EU:C:1989:321.

C.J.U.E., 20 mai 2003, *Rechnungshof*, aff. jointes C-465/00, C-138/01 et C-139/01, EU:C:2003:294.

C.J.U.E., troisième ch., 2 décembre 2010, *Ker-Optika bt contre ÁNTSZ Dél-dunántúli Regionális Intézete*, aff. C-108/09, EU:C:2010:725.

C.J.U.E., gde ch., 26 février 2013, *Aklagaren contre Hans Akerberg Fransson*, aff. C-617/10, EU:C:2013:105.

C.J.U.E., gde ch., 13 mai 2014, *Google Spain v AEPD and Mario Costeja González*, aff. C-131/12, EU:C:2014:317.

C.J.U.E., troisième ch., 1er octobre 2015, *Smaranda Bara et autres c. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*, aff. C-201/14, EU:C:2015:638.

C.J.U.E., gde ch., 6 octobre 2015, *Schrems*, aff. C-362/14, EU:C:2015:650.

C.J.U.E., 21 octobre 2015, *New Media Online GmbH c/ Bundeskommunikationssenat*, aff. C-347/14, EU:C:2015:434.

C.J.U.E., deuxième ch., 19 octobre 2016, *Breyer*, aff. C-582/14, EU:C:2016:779.

C.J.U.E., gde ch., 20 décembre 2017, *Asociación Profesional Elite Taxi / Uber Systems Spain SL*, aff. C-434/15, EU:C:2017:981.

C.J.U.E., 21 février, *Peugeot Deutschland GmbH contre Deutsche Umwelthilfe eV*, aff. C-132/17, EU:C:2018:85.

C.J.U.E., gde ch., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, EU:C:2018:388.

C.J.U.E., deuxième ch., 29 juillet 2019, *Fashion ID*, aff. C-40/17, EU:C:2019:629.

C.J.U.E., gde ch., 19 décembre 2019, *Airbnb Ireland*, aff. C-390/18, EU:C:2019:1112.

b) Cour européenne des droits de l’homme

Cour.eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, n°59320/00.

Cour.eur. D.H., 7 février 2012, *Von Hannover c. Allemagne (n° 2)*, n°40660/08 et 60641/08.

Cour eur. D.H., 23 février 2016, *Y.Y./ Russie*, n°40378/06.

Doctrine

a) Ouvrages

BARREAU, C., « Le marché unique numérique et la régulation des données personnelles », *Réalités industrielles*, 2016, n° 3.

BEELEN, A., LAMBRECHT, P. et DECHAMPS, F., « Guide pratique du RGPD : fiches de guidance », Bruxelles, Bruylant, 2018.

BENSOUSSAN, A., « La protection des données personnelles de A à Z », Bruxelles, Bruylant, 2017.

BENSOUSSAN, A., AVIGNON, C., BENSOUSSAN-BRULÉ, V., FORSTER, F., TORRES, C., & FALQUE-PIERROTIN, I., « Règlement européen sur la protection des données : textes, commentaires et orientations pratiques » (2e édition.), Bruxelles, Bruylant, 2017.

BERNARD-GLANZ, C., « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », *C.D.R.*, 2014/3.

CARNEROLI, S., *Le droit à l’oubli : du devoir de mémoire au droit à l’oubli*, Bruxelles, Larcier, 2016.

CASSART, A. et HENROTTE, J.-F., « E-réputation : vers une amnésie sélective ? », in *Pas de droit sans technologie* (sous la dir. de J.-F. HENROTTE et F. JONGEN), Bruxelles, Larcier, 2015.

CASTETS-RENARD, C., STROWEL, A. et LAMBERTERIE, I. DE, *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015.

DE TERWANGNE, C., « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ? », in *Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ?*, s.l., Larcier, 2015.

FÉRAL-SCHUHL, C., « Comment les droits de la personne concernée sont-ils renforcés ? », in *Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2015.

GALLARDO MESEGUER M., « Aperçu de la dimension internationale du règlement général sur la protection des données à caractère personnel », in *Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2015.

GEORGE, F. et HUBIN, J.-B., « La protection de la personne en situation de vulnérabilité par le droit des obligations et des contrats dans l'environnement numérique », in *La protection de la personne en situation de vulnérabilité par le droit des obligations et des contrats dans l'environnement numérique*, s.l., Larcier, 2018.

HERVEG, J. et VAN GYSEGHEM, J.-M., « La protection des données à caractère personnel en droit européen - Chronique de jurisprudence (2018): Personal data protection in European law - Column of case-law (2018) », 2019.

KIGHTLINGER, Mark F. 2007–2008. Twilight of the idols? EU internet privacy and the postenlightenment paradigm. *Columbia Journal of European Law* 14:1–62.

LANGE-MÉDART, A., « Vers une révision a minima de la directive SMA », *Enjeux de l'information et de la communication*, 2016, vol. 17–, vol. 2, n° 2.

LIVINGSTONE, S., CARR, J., et BYRNE, J., « One in three: Internet Governance and Children's Rights », *Global Commission on Internet Governance*, Paper series n° 22, novembre 2015.

MATHIEU, G. et RASSON, A.-C., « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilité et droit dans l'environnement numérique*, Bruxelles, Ed. Larcier, oct. 2018.

NOTTET, A., « Le consommateur mineur », *R.G.D.C.* , 2014.

PAILLER, L., et MARCHADIER, F., « Les réseaux sociaux sur Internet et le droit au respect de la vie privée », Bruxelles, Larcier, 2012.

PEYROU, S., « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », *Revue des Affaires européennes/ Law European & Affairs*, 2016.

POULLET, Y., « La vie privée à l'heure de la société du numérique », Bruxelles, Larcier, 2019.

POULLET, Y., « Consentement et RGPD: des zones d'ombre ! », 2019.

GIAKOUMOPOULOS, G., BUTTARELLI, G., O'FLAHERTY, M., « Manuel de droit européen en matière de protection des données », Luxembourg, 2019.

RANQUET, M., « Le droit à l'oubli : vers un nouveau droit fondamental de l'individu ? », *Communications (Paris)*, 2019, vol. 104, n° 1.

ROSIER, K., et DELFORGE, A., « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Bruxelles, Larcier, 2018.

TOMBAL, T., « Les droits de la personne concernée dans le RGPD », in *Les droits de la personne concernée dans le RGPD*, s.l., Larcier, 2018.

VAN ALSENOY, B., « Data protection law in the EU : roles, responsibilities and liability », Cambridge, Intersentia, 2019.

VLASSIS, A., « The review of the Audiovisual Media Services Directive », *Politique européenne*, 2017, vol. 56, n° 2.

b) Articles

BAMDE, A., « RGPD : le consentement des mineurs », 19 décembre 2018 (disponible sur www.aurelienbamde.com).

BAMDE, A., « RGPD: Le droit à l'effacement ou le "droit à l'oubli" », 2 janvier 2019 (disponible sur : www.aurelienbamde.com).

BASTIEN L., « Le Big Data, RGPD : l'Union européenne ouvre une enquête sur l'application TikTok », 12 juin 2020 (disponible sur <https://www.lebigdata.fr/rgpd-tiktok>).

CARRÉ A. sous la supervision de G. MATHIEU et B. VAN KEIRSBILCK
Défense des enfants internationale Belgique, « La protection des données des enfants dans le monde numérique », outil pédagogique n°2018-07, décembre 2018 (disponible sur : <https://www.dei-belgique.be/index.php/component/jdownloads/send/46-la-protection-des-donnees/389-la-protection-des-donnees-des-enfants-dans-la-monde-numerique.html>).

Claeys and Engels, « Comment faut-il comprendre la notion de 'consentement' dans le RGPD ? », 5 janvier 2018 (disponible sur : <https://www.gdprbelgium.be/fr/nouvelles/comment-faut-il-comprendre-la-notion-de-'consentement'-dans-le-rgpd>).

COCK, M., Droit & Technologies, « La directive « médias audiovisuels » sur le point d'être réformée », 2018 (disponible sur <https://www.droit-technologie.org/actualites/directive-medias-audiovisuels-point-detre-reformee/>).

Cookiebot, RGPD et consentement aux cookies | RGPD et cookies | Mon utilisation des cookies est-elle conforme ?, 28 octobre 2020 (disponible sur : <https://www.cookiebot.com/fr/rgpd-cookies/>).

Cookiebot, Le règlement ePrivacy et les cookies | Mises à jour du règlement ePrivacy 2021, 11 mars 2021 (disponible sur : <https://www.cookiebot.com/fr/reglement-e-privacy/>).

Cookiebot, Loi sur la vie privée de l'UE | RGPD, ePrivacy... le droit et les cookies, 10 mars 2021 (disponible sur : <https://www.cookiebot.com/fr/loi-vie-privee/>).

Conseil Supérieur de l'Audiovisuel, « Régulation audiovisuelle de l'UE : La nouvelle directive SMA en 5 questions », 9 mai 2018 (disponible sur : <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Regulation-audiovisuelle-de-l-UE-La-nouvelle-directive-SMA-en-5-questions>).

Conseil Supérieur de l'Audiovisuel, « Note d'orientation du CSA sur la lutte contre certaines formes de contenus illicites sur Internet, en particulier le discours de haine », 2020 (disponible sur : https://www.csa.be/wp-content/uploads/2020/02/Note-dorientation-contenus-illicites_fevrier-2020.pdf).

Digital Guide IONOS, « Le règlement ePrivacy : à quoi devez-vous vous attendre ? », 2021 (disponible sur : <https://www.ionos.fr/digitalguide/sites-internet/droit-dinternet/le-reglement-eprivacy-projet-de-lue/>)

DERIEUX, E., « Vidéos en ligne : « service de médias audiovisuels » ou « documentation promotionnelle » ? », La revue européenne des médias et du numérique, n°46-47 printemps-été 2018 (disponible sur : <https://la-rem.eu/2018/09/videos-en-ligne-service-de-medias-audiovisuels-ou-documentation-promotionnelle/>).

GAYTE, A., « L'Italie juge que TikTok ne protège pas assez les données de ses utilisateurs », Numerama, 22 décembre 2020 (disponible sur : <https://www.numerama.com/politique/678061-litalie-juge-que-tiktok-ne-protège-pas-assez-les-donnees-de-ses-utilisateurs.html>).

Grande Bibliothèque du Droit, « La protection des données personnelles des mineurs (fr) », 3 avril 2020 (disponible sur : [https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_\(fr\)](https://www.lagbd.org/index.php/La_protection_des_donnees_personnelles_des_mineurs_(fr))).

La lettre de la DAJ, « La CJUE juge qu'Airbnb est un « service de la société de l'information » et non un agent immobilier », 2020 (disponible sur : <https://kiosque.bercy.gouv.fr/alyas/msite/view/lettre-daj/13245>).

LENNE, A., EU-Logos Athéna, « L'édification de « notre » Charte des droits fondamentaux », 16 mai 2014 (disponible sur : <https://www.eu-logos.org/2014/05/16/ledification-de-notre-charte-des-droits-fondamentaux/>)

M'HAMDI, S., « "RGPD" : quelle protection pour vos données personnelles ? », Institut national de la consommation (INC), 10 octobre 2019 (disponible sur <https://www.inc-conso.fr/content/rgpd-quelle-protection-pour-vos-donnees-personnelles>).

MADELEINE, N., « Données personnelles d'enfants : enquête sur Instagram en Europe », Echos (Paris, France), 2020.

Média Animation ASBL, Médias sans frontières – Productions et consommations médiatiques dans une société multiculturelle, Les dossiers de l'éducation aux médias, 2011 (disponible sur <http://www.media-animation.be>).

MONT, J., « R.G.P.D.:quelles nouvelles règles pour les enfants sur Facebook? », 2019 (disponible sur : <http://www.crid.be/pdf/public/8550.pdf>).

OFFMANN, S., Journal d'Actualités des Droits européens, « Von Hannover 2 (le retour) : Le droit au respect de la vie privée de la Princesse Caroline au royaume de la liberté de la presse », 6 avril 2012 (disponible sur : <https://revue-jade.eu/article/view/245>).

PIERRAT, E. et KRUGER L., « La transposition en droit français de la directive SMA », Issue (disponible sur https://issuu.com/ecrantotal/docs/eth_1318/s/11825348).

REES, M., « Audiovisuel : YouTube, Facebook, Netflix, cibles de choix de la future directive SMA », 2018 (disponible sur <https://www.nextinpact.com/article/28335/106528-audiovisuel-youtube-facebook-netflix-cibles-choix-future-directive-sma>).

THIRY, G., Regulation, « La protection des mineurs sur les plateformes de partage vidéo : les prémises d'un grand chantier ! », 2020 (disponible sur : <https://regulation.be/2020/03/05/la-protection-des-mineurs-sur-les-plateformes-de-partage-video%E2%80%AF-les-premises-dun-grand-chantier%E2%80%AF/>).

UNICEF, La situation des enfants dans le monde 2017. Les enfants dans un monde numérique, Fonds des Nations Unies pour l'enfance, décembre 2017 (disponible sur : https://www.unicef.org/french/publications/index_101992.html).

VAN CLEYNENBREUGEL, P.,« What should be forgotten? Time to make sense of Article 17 GDPR from the point of view of data controllers », 2017 (disponible sur : <https://blogdroiteuropeen.com/2017/05/25/what-should-be-forgotten-time-to-make-sense-of-article-17-gdpr-from-the-point-of-view-of-data-controllers-by-pieter-van-cleynenbreugel/>).

ZANFIR, G., « Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law », in *Reloading Data Protection*, Dordrecht, Springer Netherlands, 2013, (disponible sur : https://link.springer.com/chapter/10.1007%2F978-94-007-7540-4_12#Fn32).

c) Cours Universitaires

VAN CLEYNENBREUGEL P., Advanced European Law, cours organisé à l'Université de Liège, 2019-2020.

PUYRAIMOND J.-F., Droit de la protection des données personnelles, cours organisé à l'Université de Liège, 2020-2021.