

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

R.G.P.D.

MONT, JULIE

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2019

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):
MONT, JULIE 2019, 'R.G.P.D. quelles nouvelles règles pour les enfants sur Facebook?', *Revue du Droit des Technologies de l'information*, vol. 2019, numéro 2, pp. 5-25.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

DOCTRINE

R.G.P.D. : quelles nouvelles règles pour les enfants sur Facebook ?

Julie Mont¹

Lors de l'émergence et ensuite de l'entrée en vigueur du R.G.P.D., 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 parents. Si le R.G.P.D. a effectivement instauré une nouvelle règle concernant l'enfant mineur, il s'agit d'une disposition régissant le traitement de ses données à caractère personnel, lorsqu'il est fondé sur son consentement. Nous verrons que l'article 8 du R.G.P.D. n'a pas vocation à encadrer l'accès des mineurs aux médias sociaux, cette question étant à notre sens soumise au droit des contrats, et que, dès lors, cette restriction d'accès n'est pas opportune. En tout état de cause, l'exemple choisi qu'est Facebook nous montrera que tant les règles annoncées que les règles existantes, supposées protéger les enfants lors de leur expérience sur les médias sociaux, n'apportent à ce stade pas suffisamment de garanties d'efficacité.



With the emergence and subsequent entry into force of the G.D.P.R., both the media and some authorities have stated that children under a certain age could no longer have access to social networks without their parents' permission. While the G.D.P.R. has indeed introduced a new rule concerning minors, it is a provision governing the processing of their personal data, where it is based on their consent. We will see that Article 8 of the G.D.P.R. is not intended to regulate minors' access to social media, as we believe this issue is subject to contract law, and that, therefore, this restriction of access is not appropriate. In any case, the example chosen, Facebook, will show us that both the rules announced and the existing rules, which are supposed to protect children during their experience on social media, do not provide sufficient guarantees of effectiveness at this stage.

1. Le Règlement européen relatif à la protection des données à caractère personnel² (ci-après le «R.G.P.D.»), entré en vigueur en

mai 2016 et applicable depuis mai 2018, était annoncé depuis plusieurs années comme novateur pour la protection des données à caractère personnel des citoyens. Si cet instrument a principalement réaffirmé et renforcé les principes contenus dans la directive 95/46³, il

¹ Assistante à la faculté de droit de l'UNamur et avocate au barreau de Namur. L'auteure remercie Élise Degrave pour sa relecture attentive.

² 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 de données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règle-

ment général sur la protection des données), *J.O.U.E.*, 4 mai 2016. Ci-après référencé comme suit : «R.G.P.D.».

³ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection

a également instauré de nouvelles dispositions légales, au rang desquelles l'une est dédiée à l'exploitation de données personnelles appartenant à des mineurs.

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 2015 indiquait que le règlement en devenir allait instaurer des règles concernant la présence des enfants sur les médias sociaux⁴ : « 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. Les nouvelles règles flexibles assurent que les États membres puissent fixer leurs propres limites à condition qu'elles ne soient pas inférieures à 13 ans ou supérieures à 16 ans, leur donnant ainsi la liberté de conserver celles qui s'appliquent déjà »⁵.

Lorsque le R.G.P.D. est devenu applicable, trois années plus tard, les médias ont également annoncé que les mineurs devraient dorénavant, sous un certain âge, obtenir l'accord de leurs parents pour se créer un compte sur les réseaux sociaux. Les titres clamaient : « 13 ans devient l'âge minimum pour aller sur les médias sociaux »⁶ ; « La Belgique fixe l'âge minimal pour

s'inscrire sur les réseaux sociaux »⁷ ; « Pour s'inscrire à Facebook, les ados français devront avoir l'autorisation des parents »⁸ ; « Réseaux sociaux : les députés fixent à 15 ans l'âge minimum pour s'inscrire sans accord parental »⁹. Le commissariat aux Droits de l'enfant de la Communauté flamande, consulté lors de la phase d'élaboration de la loi belge exécutant le R.G.P.D., a également annoncé « le Règlement prévoit que les jeunes de moins de 16 ans devront obtenir l'accord de leurs parents pour accéder aux services de la société de l'information comme les médias sociaux »¹⁰.

2. En réalité, nous verrons dans les lignes qui suivent qu'une disposition nouvelle a effectivement vu le jour sous l'ère du R.G.P.D., s'agissant des données personnelles des mineurs, soit l'article 8 du règlement. Toutefois, il ne s'agit à notre sens pas d'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 R.G.P.D. Il est possible qu'un jeune soit également capable de s'inscrire seul sur un réseau social, mais n'ait pas l'âge fixé par le règlement pour se prononcer seul sur le sort de ses données personnelles.

des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, 23 novembre 1995 (abrogée).

⁴ Communiqué de presse disponible à l'adresse : <http://www.europarl.europa.eu/news/fr/press-room/20151217IPR08112/protection-des-donnees-les-citoyens-aux-commandes>.

⁵ Communiqué de presse disponible à l'adresse : <http://www.europarl.europa.eu/news/fr/press-room/20151217IPR08112/protection-des-donnees-les-citoyens-aux-commandes>.

⁶ Article disponible à l'adresse : https://www.rtbfb.be/info/belgique/detail_13-ans-devient-l-age-minimum-pour-aller-sur-les-medias-sociaux?id=9868525.

⁷ Article disponible à l'adresse : <https://www.rtl.be/info/belgique/societe/la-belgique-fixe-l-age-minimum-pour-s-inscrire-sur-les-reseaux-sociaux-1005497.aspx>.

⁸ Article disponible à l'adresse : <http://www.lefigaro.fr/secteur/high-tech/2017/12/13/32001-201712-13ARTFIG00293-pour-s-inscrire-a-facebook-les-ados-francais-devront-avoir-l-autorisation-des-parents.php>.

⁹ Article disponible à l'adresse : <https://bfmbusiness.bfmtv.com/entreprise/reseaux-sociaux-les-deputes-fixent-a-15-ans-l-age-minimum-pour-s-inscrire-sans-accord-parental-1369173.html>.

¹⁰ Commissariat aux Droits de l'enfant de la Communauté flamande, avis du 22 avril 2016, n° 2015-2016/09, disponible à l'adresse : https://www.kinderrechtencommissariaat.be/sites/default/files/bestanden/2015_2016_09_advies_eu_dataprotectie_sociale_media_vanaf_13jaar_def.pdf.

Cette contribution fera le point sur la nouveauté instaurée par le règlement et les contours exacts de celle-ci. Nous présenterons dans un premier point les grandes lignes de l'article 8 du R.G.P.D. Nous verrons ensuite, au travers de l'exemple concret de Facebook, pourquoi, selon nous, cette disposition ne vise nullement les conditions d'inscription sur un réseau social et pourquoi une restriction des conditions d'inscription ne serait pas opportune. Enfin, nous verrons que, pour respecter l'article 8 du R.G.P.D., les responsables de traitement doivent mettre en place plusieurs vérifications qui ne sont pour l'heure pas appliquées, ce qui affaiblit la protection recherchée. Les disparités entre les lois applicables dans les États membres en la matière seront également pointées du doigt.

I. LES CONTOURS DE L'ARTICLE 8 DU R.G.P.D.

A. Les raisons d'être – La vulnérabilité du mineur sur les réseaux

3. Le R.G.P.D., qui a renforcé sur certains plans la protection des données à caractère personnel des individus, se veut soucieux du cas des mineurs sur internet, et plus particulièrement de leurs données à caractère personnel. Ce n'était pas le cas, en tous cas pas directement, sous l'empire de la directive 95/46, qui n'appréhendait pas leur situation particulière. Les raisons pour lesquelles une disposition spécifique a été édictée ne sont pas développées dans les travaux préparatoires ayant abouti à l'adoption du règlement. Quelques considérants du R.G.P.D. évoquent tout de même celles-ci en ces termes: «les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences, des garanties concernées et de leurs droits liés au traitement

des données à caractère personnel (...)»¹¹; «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»¹².

4. 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 autres¹³. Cette vulnérabilité se renforce dans l'environnement numérique. En effet, le mineur est généralement à l'aise avec les nouvelles technologies et dispose le plus souvent d'un *smartphone* facilitant l'accès à internet. Or, les dangers d'internet pour les plus jeunes sont très souvent mis en avant. Le harcèlement sur les réseaux sociaux est notamment – malheureusement – relayé de manière fréquente dans l'actualité.

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 (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 potentielles. Son profil 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 notoire que tant les réseaux sociaux eux-mêmes que des annonceurs tiers, comme les publicitaires, utilisent ces données, notamment à des fins

¹¹ R.G.P.D., considérant 38.

¹² R.G.P.D., considérant 58.

¹³ A. NOTTET, «Le consommateur mineur», *R.G.D.C.*, 2014, p. 40.

commerciales. C'est dans cet environnement de développement numérique toujours grandissant et de numérisation de plus en plus large des contenus accessibles aux enfants que le règlement européen a été adopté et qu'il se veut soucieux de leur situation.

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

5. Lorsqu'un mineur s'inscrit sur un réseau social, il fournit, on l'a dit, de nombreuses données à caractère personnel, allant des plus évidentes, comme son nom, son prénom, sa date de naissance, à d'autres encore 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 service de réseau social opère des traitements de données, à plusieurs fins, et devient dès lors un responsable de traitement, au sens du R.G.P.D.¹⁴. Les informations personnelles susmentionnées sont enregistrées et organisées sur les serveurs de Facebook, diffusées aux autres utilisateurs du réseau, voire à des tiers, consultées à des fins de publicité ciblée et exportées vers d'autres sites web conçus et offerts par Facebook¹⁵. 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 R.G.P.D., comme le consentement de la personne concernée, l'exécution d'un contrat,

le respect d'une obligation légale ou encore ses intérêts légitimes.

6. Dans sa politique d'utilisation des données, Facebook détaille les informations qui sont recueillies, comment elles sont utilisées et partagées et sur quel fondement juridique le réseau s'appuie pour les traiter¹⁶. À la lecture des bases légales de traitement utilisées, on se rend compte que le réseau social se fonde sur toutes celles qui sont prévues à l'article 6 du R.G.P.D.¹⁷. La base légale de traitement la plus largement utilisée par Facebook est le contrat conclu avec l'utilisateur¹⁸. Le réseau social envisage toutefois le cas d'une personne qui n'est pas juridiquement habilitée à passer un contrat, comme le mineur, en déplaçant alors la base légale de traitement vers ses intérêts légitimes ou ceux d'un tiers¹⁹. Nous reviendrons sur ce point *infra*.

À côté de ces bases légales de traitement largement employées que sont l'exécution d'un contrat et les intérêts légitimes du responsable de traitement, le consentement de l'utilisateur à propos du traitement envisagé est quant à lui assez peu utilisé par le réseau social. Il l'est

¹⁶ Politique d'utilisation des données Facebook, disponible à l'adresse: <https://www.facebook.com/about/privacy/update>.

¹⁷ Un hyperlien à partir de la politique de traitement renvoie vers une page pour « en savoir plus » sur les bases de traitement: https://www.facebook.com/about/privacy/legal_bases.

¹⁸ Extrait de la page précitée: « Pour toutes les personnes juridiquement habilitées à passer un contrat exécutoire, nous traitons les données de la manière nécessaire pour exécuter les contrats qui nous lient à vous (les Conditions d'utilisation de Facebook) ».

¹⁹ Extrait de la page précitée « Pour les personnes qui n'ont pas atteint l'âge de la majorité (moins de 18 ans dans la plupart des pays européens) et qui ne sont pas entièrement habilitées à conclure un contrat exécutoire, il est possible que nous ne puissions pas traiter les données personnelles sur la base de la nécessité contractuelle. Toutefois, lorsqu'une telle personne utilise nos Services, les points suivants sont dans nos intérêts légitimes (...) ».

¹⁴ Le responsable de traitement est défini à l'article 4.7) du R.G.P.D. 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 ».

¹⁵ J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010, n° 2, p. 243.

pour les données bénéficiant d'une protection spéciale (croyances religieuses, opinions politiques, santé) si elles sont partagées, la technologie de la reconnaissance faciale, les données que les annonceurs et partenaires communiquent au sujet de l'activité de l'utilisateur en dehors de Facebook, le partage avec les annonceurs, les données qui identifient personnellement l'utilisateur (comme son nom ou son adresse e-mail) et pour collecter les informations via les paramètres de l'appareil utilisé, comme les coordonnées GPS ou l'appareil photo du *smartphone* par exemple²⁰.

7. C'est à ces opérations, ces traitements, que l'article 8 du R.G.P.D. s'applique puisqu'il régit spécifiquement le cas où le responsable de traitement de données entendra fonder celui-ci sur le *consentement de la personne concernée* (i) par lesdites données et que ces dernières *concernent un mineur* (ii)²¹.

Cette disposition fixe l'âge à partir duquel un mineur peut autoriser le responsable de traitement à user de ses données person-

nelles sur base de son consentement. Si le mineur a moins de 16 ans, le traitement de données qui serait fondé sur le consentement ne pourra avoir lieu que si le responsable de l'autorité parentale (généralement le parent) a donné son accord. Par contre, si le mineur a plus de 16 ans, il est considéré comme « apte à consentir » ou en âge du « consentement numérique » et le traitement de données autorisé qu'il autorise lui-même est légal.

L'article 8 du R.G.P.D. s'applique uniquement aux services de la société de l'information qui sont directement offerts aux enfants. Le service de la société de l'information est « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services »²². Un service presté à distance signifie qu'il est fourni sans que les parties soient simultanément présentes. La Cour de justice de l'Union européenne estime que les services de la société de l'information couvrent les contrats et autres services conclus ou transmis en ligne, ainsi que la fourniture d'un service en ligne²³. Les services offerts par Facebook correspondent aux éléments constitutifs d'un service de la société de l'information. L'activité du réseau social est en effet considérée comme « prestée normalement contre rémunération » car elle constitue une activité économique, peu importe qu'elle soit rémunérée ou non par l'utilisateur²⁴. Par ailleurs, ces services doivent

²⁰ *Ibid.*

²¹ L'article 8 du R.G.P.D. dispose : « 1. Lorsque l'article 6, paragraphe 1, point a) s'applique [lorsque le traitement est fondé sur le consentement de la personne concernée], 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. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en dessous de 13 ans. 2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles. 3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant ».

²² Directive (UE) 2015-1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant un procédé d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.E.U.*, 17 septembre 2015, article 1^{er} § 1^{er}, b), auquel renvoie l'article 4.25 du R.G.P.D.

²³ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices sur le consentement au sens du règlement 2016/679, version révisée et adoptée le 10 avril 2018, pp. 28-29.

²⁴ J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données »,

être offerts directement aux enfants, ce qui signifie que si le prestataire indique clairement aux utilisateurs potentiels qu'il ne propose ses services qu'à des personnes âgées de 18 ans ou plus, et que cette affirmation n'est pas contredite par d'autres éléments comme le contenu du site, les services qu'il preste ne seront pas considérés comme étant « directement proposés » à un enfant mineur et l'article 8 du règlement ne s'appliquera pas²⁵.

8. Il est également à noter que le premier paragraphe de cet article 8 laisse la possibilité aux États membres de prévoir un âge inférieur à 16 ans à partir duquel ils estiment que le mineur est apte à consentir seul au traitement de ses données, sans que cet âge puisse être inférieur à 13 ans. Initialement, les négociateurs au Parlement européen souhaitaient une limite d'âge à l'échelle européenne de 13 ans, mais les États membres ne sont pas parvenus à dégager un consensus sur cet âge, raison pour laquelle cette flexibilité a été instaurée²⁶. Ceux-ci sont donc libres de fixer l'âge du « consentement numérique », calqué sur la notion de « majorité numérique », étant l'âge à partir duquel les autorités nationales considèrent que le mineur est propriétaire de ses données et est en mesure de comprendre que des tiers, comme un réseau social, sont susceptibles d'y avoir accès, de les collecter et de les traiter, notamment à des fins commerciales.

La Belgique a usé de la faculté offerte par le R.G.P.D. puisque l'article 7 de la loi du 30 juillet 2018²⁷ prévoit que le traitement des données

personnelles d'un mineur, fondé sur le consentement de celui-ci, est licite si le mineur a plus de 13 ans²⁸. Le législateur a donc opté pour un abaissement du seuil auquel le mineur peut autoriser un responsable de traitement à utiliser ses données, ce après avoir tout de même reconnu que « les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel »²⁹. L'Autorité belge de protection des données a validé le choix du législateur, considérant que « cet âge correspond mieux à la réalité quotidienne de très nombreux jeunes qui surfent déjà sur Internet à un jeune âge » et qu'il ne faut pas « les priver d'opportunités de s'épanouir numériquement et socialement »³⁰. Il a été considéré que les enfants doivent pouvoir utiliser les applications et chatter librement sans devoir toujours demander l'accord de leurs parents. L'Autorité a toutefois relevé qu'au vu du choix du seuil de 13 ans, celui-ci devait être accompagné d'efforts supplémentaires pour leur apprendre dès l'enfance à adopter une « attitude réfléchie

op. cit., p. 240.

²⁵ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 29.

²⁶ Voy. le résumé de l'analyse de l'article au niveau européen sur le site: <https://www.gdpr-expert.eu/article.html?id=8#eu-regulation>.

²⁷ Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

²⁸ L'article 7 de la loi dispose: « En exécution de l'article 8.1. du Règlement, le traitement des données à caractère personnel relatif aux enfants en ce qui concerne l'offre directe de services de la société de l'information aux enfants, est licite lorsque le consentement a été donné par des enfants âgés de 13 ans ou plus. Lorsque ce traitement porte sur des données à caractère personnel de l'enfant âgé de moins de 13 ans, il n'est licite que si le consentement est donné par le représentant légal de cet enfant ».

²⁹ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 11 juin 2018, Exposé des motifs, *Doc., Ch.*, 2017-2018, n° 3126/001, p. 18.

³⁰ Autorité belge de protection des données, « R.G.P.D.: la limite d'âge de 13 ans correspond à la pratique numérique », Communiqué de presse du 13 février 2018, disponible à l'adresse: <https://www.autoriteprotectiondonnees.be/news/rgpd-la-limite-dage-de-13-ans-correspond-a-la-pratique-numerique>.

à l'égard des médias» pour qu'ils perçoivent les risques d'un comportement de «partages multiples»³¹.

9. En France, l'âge du consentement numérique a été fixé à 15 ans. Si le mineur a moins de 15 ans, il ne pourra consentir seul à un traitement et une intervention du ou des titulaire(s) de l'autorité parentale sera nécessaire³². Pour ce qui concerne les autres États membres qui ont adopté une loi consacrant les règles issues du R.G.P.D., on peut relever que l'âge du consentement numérique a été fixé à 14 ans en Autriche, 16 ans en Croatie, 14 ans à Chypre, 13 ans au Danemark, 13 ans en Finlande, 16 ans en Allemagne, 16 ans en Hongrie, 14 ans en Italie, 13 ans en Lettonie, 14 ans en Lituanie, 16 ans au Luxembourg, 13 ans à Malte, 16 ans aux Pays-Bas, 16 ans en Pologne, 16 ans en Roumanie, 16 ans en Slovaquie, 14 ans en Espagne, 13 ans en Suède, 16 ans en Suisse et 13 ans en Norvège³³. Nous verrons *infra* que cette disparité entre les lois nationales engendre des conflits de loi applicable.

II. LA RESTRICTION D'ACCÈS AUX RÉSEAUX SOCIAUX N'EST PAS OPPORTUNE

10. Comme exposé dans les propos introductifs, lorsque le R.G.P.D. a été adopté et qu'ensuite, les États membres ont légiféré en la matière, le principe selon lequel les enfants ne pourraient plus s'inscrire sous un certain âge sur les réseaux sociaux sans l'accord de leurs parents a été clamé. Il s'agit d'un raccourci provenant nécessairement de l'âge du «consentement numérique» fixé en droit européen et par les droits nationaux («Si un enfant de 15 ans est considéré par la législation sur la protection des données comme n'étant pas apte à consentir seul au traitement de ses données, alors il n'a pas l'âge de s'inscrire seul sur le réseau social»). Il a probablement été imaginé que l'encadrement de l'inscription sur les médias sociaux permettrait d'assurer que le responsable de traitement recueille dans tous les cas un consentement valide lui permettant de traiter les données sur cette base. Ainsi, l'inscription d'un enfant (avec ou sans l'intervention des parents) rendrait tout consentement légal puisque forcément donné, dès l'inscription, par la bonne personne (soit l'enfant s'il a pu s'inscrire seul, soit les parents).

En réalité, et même si on ne retrouve pas de trace de ces annonces médiatiques en pratique, le raccourci qu'elles sous-tendent n'est pas exact. Il faut en effet distinguer l'inscription ou l'accès au réseau et le consentement éventuellement demandé ensuite pour légitimer le traitement de données. L'inscription sur le réseau s'apparente à notre sens à la conclusion d'un contrat et est régie par le droit des contrats, qui impose un consentement valable dans le chef de la personne qui s'engage. Le consentement ultérieur qui serait éventuellement demandé par le responsable de traitement lors de l'exécution du contrat, pour traiter certaines données personnelles est quant à lui différent

³¹ *Ibid.*

³² Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *J.O.F.R.*, 13 décembre 2018, article 45.

³³ Résultats de l'étude réalisée par l'Université de Gand, «A children's rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth», disponible à l'adresse: https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.

et, à notre avis, le seul envisagé par le R.G.P.D. Le règlement indique d'ailleurs spécifiquement au paragraphe 3 de son article 8 que : « le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant ». F. Coton expose à ce propos : « Cette "minorité digitale" ne concerne que le traitement des données de l'enfant utilisateur du service, et pas l'achat du service. La capacité juridique nécessaire pour commander le service en lui-même reste inchangée. De même, la seule utilisation des coordonnées de l'enfant et de son mot de passe pour se connecter au service en ligne ne requiert pas son consentement, puisque ce traitement de données est nécessaire à l'exécution du contrat »³⁴.

Il est donc possible, comme nous le verrons ci-après, qu'un jeune soit capable de s'inscrire seul sur le réseau social, en vertu du droit des contrats, mais ne soit pas en âge de consentir seul au traitement de ses données personnelles. Et inversement.

A. Le consentement au contrat *versus* le consentement au traitement

11. Sous l'ère « *ante* » R.G.P.D., l'obtention du consentement pour traiter les données de la personne concernée passait par l'acceptation des conditions générales du contrat, dans lesquelles était contenue une clause « vie privée »³⁵. Dorénavant, pour Th. Léonard, il y a lieu de considérer le consentement au sens du R.G.P.D., c'est-à-dire le consentement utilisé comme base légale d'un traitement de

données, comme un acte unilatéral à distinguer du contrat, acte juridique bilatéral³⁶. Selon lui, il existe effectivement deux types de consentements, de natures différentes, soit le consentement qui légitime le traitement de données et celui qui conditionne la conclusion d'un contrat³⁷. Le premier consiste en l'exécution d'un devoir légal qui s'impose au responsable de traitement, par l'effet de la loi, au titre de protection des personnes concernées³⁸. En ce sens, ce consentement ne permet pas, au contraire du consentement en droit des contrats, de créer une relation contractuelle avec le responsable de traitement mais consiste uniquement en un effet de la loi. Le consentement prévu par l'article 6 du R.G.P.D. permet ainsi uniquement au responsable de mettre les traitements en œuvre, en étant « un acte juridique unilatéral permettant de poser toute une série d'actes sur les traitements en cause dans le respect du GDPR »³⁹.

Pour d'autres auteurs, le consentement ne se distingue pas du contrat, mais il y a lieu de distinguer plusieurs types de consentements au sein d'un même contrat et en tout cas de dissocier le consentement particulier qui doit être sollicité dès que la cause de licéité excède les besoins stricts du contrat ou l'intérêt légitime, du consentement « global » au contrat⁴⁰. D'après Y. Pouillet, la nature contractuelle du consentement devrait être reconnue car elle répond mieux que la qualification d'acte unilatéral à la réalité des opérations effectuées sur un réseau⁴¹.

12. Outre la nature de ces consentements (acte juridique unilatéral ou contrat), dont

³⁴ F. COTON, « Minorité digitale: votre entreprise est-elle prête? », article disponible à l'adresse: <https://lexing.be/minorite-digitale-votre-entreprise-est-elle-prete/>.

³⁵ Th. LÉONARD, « Yves, si tu exploitais tes données? », *Law, Norms and Freedoms in Cyberspace, Liber Amicorum Yves Pouillet, E. DEGRAVE et al.* (éd.), coll. du CRIDS, Bruxelles, Larcier, n° 43, 2018, p. 665.

³⁶ Y. POUILLET, « Consentement et R.G.P.D.: des zones d'ombre! », *D.C.C.R.*, n° 122-123, 2019, p. 12.

³⁷ Th. LÉONARD, *op. cit.*, p. 666.

³⁸ *Ibid.*, p. 667.

³⁹ *Ibid.*, p. 668.

⁴⁰ Y. POUILLET, *op. cit.*, p. 13.

⁴¹ *Ibid.*, p. 21.

on voit qu'elle oppose les auteurs, il convient selon nous d'insister plus particulièrement sur la nécessité de dissocier le consentement au contrat dans son ensemble du consentement au traitement de données. Le second paragraphe de l'article 7 du R.G.P.D. dispose d'ailleurs que si le consentement de la personne concernée est requis dans le contexte d'une déclaration écrite qui concerne également d'autres questions, la demande relative au consentement doit être présentée sous une forme qui la distingue clairement des autres questions, d'une façon compréhensible et facilement accessible, en des termes clairs et simples. Selon Th. Léonard, on peut « inférer de cette règle de forme que le consentement au traitement ne peut plus nécessairement s'exprimer par le consentement relatif au contrat. L'implication de cette règle de forme revient à sortir du contrat à conclure avec le responsable de traitement/prestataire le consentement spécifique imposé par le GDPR »⁴². Cela rejoint la thèse de Y. Pouillet selon laquelle le consentement nécessaire pour fonder la licéité du traitement doit être « dissocié » de celui donné aux conditions générales du contrat⁴³.

Partageant l'avis de ces auteurs, il convient, selon nous, de conditionner la question de l'inscription sur le réseau social au respect du droit des contrats, et non de la relier à l'âge du « consentement numérique » issu du R.G.P.D.

B. L'accès au réseau social régi par le droit des contrats

13. Le consentement au sens du droit des contrats s'entend comme la volonté de contracter d'une partie⁴⁴, c'est-à-dire de s'engager dans une relation contractuelle avec son co-contractant, et constitue une condition

de validité de la convention⁴⁵. L'enfant mineur n'est, en principe, pas en mesure de s'engager en droit, étant considéré comme « incapable » au sens du droit civil. Ce dernier ne peut donc poser valablement d'actes juridiques et ne peut conclure de conventions sans l'intervention de ses parents⁴⁶. Il ne peut dès lors en principe pas exprimer de consentement valable.

Il est toutefois admis que l'enfant dispose d'une « capacité de discernement », dite capacité « résiduelle », située entre 12 et 14 ans. Ainsi, il peut accomplir seul les actes de la vie courante, les actes conservatoires et les actes à caractère purement personnel⁴⁷, pourvu que ceux-ci ne soient pas lésionnaires. La catégorie des actes que le mineur est susceptible d'accomplir seul sous le couvert de cette capacité « résiduelle » reste toutefois floue et il appartient au juge d'apprécier, au cas par cas, si le mineur en dispose, notamment compte tenu de son âge, sa maturité, son éducation, la nature de l'acte...

14. Pour s'inscrire sur Facebook, il est demandé d'encoder un prénom, un nom, un numéro de GSM ou une adresse e-mail, un mot de passe, son sexe et une date de naissance. Une clause stipule, juste avant le bouton « inscription » : « en cliquant sur inscription, vous acceptez nos conditions générales. Découvrez comment nous recueillons, utilisons et partageons vos données en lisant notre Politique d'utilisation des données et comment nous utilisons les cookies et autres technologies similaires en consultant notre Politique d'utilisation des cookies. Vous rece-

⁴⁵ Article 1108 du Code civil.

⁴⁶ F. GEORGE, J.-B. HUBIN, « La protection de la personne en situation de vulnérabilité par le droit des obligations et des contrats dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, H. JACQUEMIN, M. NIHOUL (dir.), coll. Faculté de droit de l'UNamur, Bruxelles, Larcier, 2018, p. 52.

⁴⁷ *Ibid.*, p. 54.

⁴² Th. LÉONARD, *op. cit.*, p. 665.

⁴³ Y. POUILLET, *op. cit.*, p. 16 et p. 21.

⁴⁴ P. WÉRY, *Droit des obligations, Volume 1: Théorie générale du contrat*, 2^e éd., Bruxelles, Larcier, 2011, p. 223.

DOCTRINE

vrez peut-être des notifications par texto de notre part et vous pouvez à tout moment vous désabonner». Les termes « conditions générales », « politique d'utilisation des données » et « politique d'utilisation des cookies » sont des hyperliens donnant accès auxdits documents.

Inscription

C'est rapide et facile.

Prénom Nom de famille

Numéro de mobile ou e-mail

Nouveau mot de passe

Date de naissance

18 oct 1994

Genre

Femme Homme Personnalisé

En cliquant sur Inscription, vous acceptez nos Conditions générales. Découvrez comment nous recueillons, utilisons et partageons vos données en lisant notre Politique d'utilisation des données et comment nous utilisons les cookies et autres technologies similaires en consultant notre Politique d'utilisation des cookies. Vous recevrez peut-être des notifications par texto de notre part et vous pouvez à tout moment vous désabonner.

Inscription

1. La conclusion d'un contrat utilisateur

15. En cliquant sur « inscription » après avoir rempli les champs demandés, on conclut un contrat avec le réseau social. Le droit américain, et plus particulièrement le droit californien, distingue le « *clickwrap* » *agreement* du « *browsewrap* » *agreement*. Le premier nécessite que l'utilisateur marque son consentement aux termes de l'engagement, par un clic sur un bouton « J'accepte » « Je consens » adjacent à une mention stipulant le consentement aux conditions d'utilisation et à la politique d'utilisation ou par le fait de cocher une case, avant

de pouvoir utiliser le service⁴⁸. Le second résulte de la seule utilisation du site, manifestant ainsi l'acceptation, que les conditions aient été lues ou non⁴⁹. Selon J.-P. Moiny, Facebook propose un « *browsewrap* » *agreement* puisqu'il suffit de cliquer sur le bouton « inscription » pour utiliser le réseau social, sans devoir exprimer littéralement un consentement aux conditions et politiques légales⁵⁰.

Lorsqu'une personne s'inscrit sur Facebook, le renvoi par les hyperliens vers les pages contenant la politique de confidentialité et les conditions d'utilisation tendent à inclure ces documents contractuels dans le champ du consentement de l'internaute au contrat qu'il conclut. Les conditions d'utilisation ou conditions générales sont considérées comme faisant partie de l'objet du contrat⁵¹. Dès lors, c'est à l'occasion de son inscription sur le réseau social que l'utilisateur consent à ce que les données le concernant soient traitées conformément à la politique de confidentialité⁵² (mais sans encore manifester son consentement pour un traitement particulier fondé sur cette base – *cf* points 11 et 12). Cette acceptation des conditions d'utilisation et de la politique de confidentialité est donc concomitante au comportement supposé manifester le consentement nécessaire à la formation du contrat⁵³.

Cette pratique, que l'on peut qualifier de conclusion d'un « contrat d'adhésion », n'est pas propre aux réseaux sociaux et a déjà fait

⁴⁸ J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée. Quelques réflexions en droit belge et américain », *Rev. Dr. ULiège*, 2010/2, p. 184.

⁴⁹ L. PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Bruxelles, Larcier, 2012, p. 38.

⁵⁰ J.-P. MOINY, « Contracter dans les réseaux sociaux... », *op. cit.*, p. 184.

⁵¹ *Ibid.*, p. 186.

⁵² *Ibid.*, p. 165.

⁵³ *Ibid.*, p. 165.

couler beaucoup d'encre, notamment en droit de la consommation. Sans nous appesantir sur ces règles spécifiques qui sortent du cadre de la présente contribution, relevons que ce type de contrat est constitué de dispositions contractuelles standards, imposées au cocontractant, ce qui annihile la phase de négociation précontractuelle⁵⁴. Or, selon la législation belge, le cocontractant doit avoir la possibilité de prendre connaissance, effectivement, des conditions générales applicables au contrat, avant la conclusion de celui-ci, et doit les avoir acceptées. On l'a vu, dans le cas de Facebook, l'acceptation des conditions générales est présumée par l'utilisation du site après la phase d'inscription («*browsewrap*» *agreement*). Les *browsewrap contracts* sont toutefois reconnus par la jurisprudence américaine comme permettant l'expression du consentement valable de l'internaute⁵⁵. Les droits belge et américain semblent proches s'agissant du processus de formation du contrat et du contenu du champ contractuel, en reconnaissant notamment les *browsewrap contracts* comme des contrats valables, même s'ils ne sont pas à l'abri de tout reproche⁵⁶.

2. Par un mineur

16. Il reste encore à déterminer si l'inscription d'un mineur sur Facebook, qui constitue donc la conclusion d'un contrat, est un acte juridique valable. Sa validité peut être analysée, pour le mineur belge, au regard du droit belge puisque les conditions générales de Facebook contiennent une clause fixant le droit applicable comme pouvant être celui du pays du consommateur⁵⁷.

La lecture des conditions générales (ou conditions d'utilisation ou politique d'utilisation) Facebook nous apprend qu'en réalité, le réseau social est interdit aux enfants de moins de 13 ans (14 ans en Espagne et en Corée du Nord)⁵⁸. Cette interdiction provient du *Children's Online Privacy Protection Act* de 1998, qui n'autorise la collecte de données personnelles sans le consentement parental que pour les mineurs de plus de 13 ans. Facebook a donc calqué l'âge pour s'inscrire sur le réseau à ce seuil, lié à la protection des données⁵⁹. On retrouve ici la même démarche que celle que nous critiquons.

Facebook, qui autorise les mineurs de plus de 13 ans à utiliser ses services et donc indirectement à conclure un contrat avec le réseau, reconnaît, pour rappel, la possibilité que ce type d'utilisateur ne soit pas «entièrement» habilité à passer un contrat exécutoire: «Pour les personnes qui n'ont pas atteint l'âge de la majorité (moins de 18 ans dans la plupart des pays européens) et qui ne sont pas *entièrement habilitées*⁶⁰ à conclure un contrat exécutoire, il est possible que nous ne puissions pas traiter les données personnelles sur la base de la nécessité contractuelle».

L'Autorité de protection des données, lorsqu'elle a conforté le choix d'abaisser le seuil du «consentement numérique» à 13 ans en Belgique, a fait ce parallèle avec l'application du droit des contrats puisqu'elle a déclaré que «les dispositions du droit des contrats restent également inchangées à l'égard des enfants. En Belgique, cet âge est toujours fixé à

⁵⁴ F. GEORGE, J.-B. HUBIN, *op. cit.*, p. 68.

⁵⁵ J.-P. MOINY, «Contracter dans les réseaux sociaux ...», *op. cit.*, p. 211.

⁵⁶ *Ibid.*, p. 212.

⁵⁷ Conditions générales de Facebook (version au 31.07.2019), disponibles à l'adresse: https://www.facebook.com/legal/terms/update_2019: «Si vous êtes un

consommateur et que vous résidez habituellement dans un État membre de l'Union européenne, les lois de cet État membre s'appliqueront à toute réclamation, à toute cause d'action ou à tout litige à notre rencontre».

⁵⁸ *Ibid.*

⁵⁹ L. PAILLER, *op. cit.*, p. 39.

⁶⁰ Souligné par nous.

18 ans»⁶¹. L'Autorité de contrôle a ainsi rappelé qu'en principe, le mineur ne peut rien faire seul sous l'âge des 18 ans, mais dans le même temps validé le seuil de l'âge du consentement numérique à 13 ans, en se référant à la capacité de discernement, fixée entre 12 et 14 ans.

17. Pour ceux qui ont entre 13 et 18 ans, si Facebook les autorise à s'inscrire, rappelons qu'ils n'ont en principe pas la capacité de s'engager dans les liens d'un contrat. Sur le fait de savoir si l'inscription sur un réseau social est un acte de la vie courante qui ressort de la capacité résiduelle du mineur, F. George et J.-B. Hubin sont d'avis que: «l'évolution des habitudes et mœurs sur internet ainsi que l'éventuel coût d'une telle inscription joueront sans aucun doute un rôle dans l'appréciation du juge»⁶². Compte tenu de la nature évolutive de la notion d'acte de la vie courante et de l'utilisation massive d'internet par les jeunes, il nous semble que l'inscription d'un mineur doté de la capacité de discernement (âgé généralement de 12, 13 ou 14 ans) sur Facebook pourrait être considérée comme un tel acte.

À ce jour, la jurisprudence belge ne s'est pas prononcée sur le fait de savoir si un tel contrat d'utilisation d'un réseau social pouvait être valablement conclu avec un mineur. Il est à supposer qu'en cas de problème⁶³, les responsables du mineur se tournent rarement vers un tel moyen de défense, probablement car la mise en cause du réseau social effraie. Ceux-ci pourraient toutefois arguer, si l'enfant n'est pas doté de la capacité de discernement (incapacité totale ou absolue), que le contrat est

frappé d'une cause de nullité relative, la simple déclaration mensongère du mineur quant à son âge n'empêchant pas l'action en nullité, sauf si cette dissimulation est frauduleuse⁶⁴. Encore la conclusion de ce contrat serait-elle considérée comme valide dans le chef de l'enfant (notamment si le juge devait considérer qu'il a la capacité de discernement suffisante), un moyen tiré du droit de la consommation pour contester le contrat d'utilisateur et éventuellement mettre en cause la responsabilité de Facebook présente des chances de succès puisque cette convention s'apparente à un contrat d'adhésion, au vu des conditions contractuelles qui sont imposées à l'utilisateur, qui n'a d'autre choix que de les accepter pour accéder au service: «l'individu ne peut négocier, il est contraint à une simple alternative: soit il agréé inconditionnellement les termes proposés, soit il renonce à accéder au réseau social»⁶⁵.

18. Il découle de ce qui précède qu'il n'est pas opportun de cadenacer l'accès à Facebook suite à l'entrée en vigueur du R.G.P.D. fixant l'âge du «consentement numérique», l'inscription étant régie par le droit des contrats uniquement. Si, en Belgique, l'âge minimum autorisé par Facebook pour s'inscrire correspond à l'âge du consentement numérique fixé par la loi du 30 juillet 2018, ces deux seuils d'âges ne doivent à notre sens pas forcément être calqués l'un sur l'autre. Un enfant allemand de 14 ans devrait en effet, si l'on en croit les médias (*cf supra*) être interdit d'accès à Facebook pour l'unique raison que l'âge du consentement numérique a été fixé à 15 ans en Allemagne, en application de l'article 8 du R.G.P.D., ce alors qu'il dispose vraisemblablement de la capacité de discernement et que le média social l'autorise à créer un compte.

⁶¹ Autorité belge de protection des données, «R.G.P.D.: la limite d'âge de 13 ans correspond à la pratique numérique», Communiqué de presse du 13 février 2018, précité.

⁶² *Ibid.*, p. 57.

⁶³ On pourrait songer à un mineur victime de harcèlement sur le réseau social et dont les parents entendent mettre en cause la responsabilité de Facebook pour avoir contracté illégalement avec leur enfant.

⁶⁴ F. GEORGE, J.-B. HUBIN, *op. cit.*, p. 54.

⁶⁵ J.-P. MOINY, «Contracter dans les réseaux sociaux ...», *op. cit.*, p. 193.

C. Le consentement au traitement de données doit être caractérisé

19. Outre le fait qu'il est erroné de penser que les traitements de données effectués sur la base du consentement seront forcément conformes au R.G.P.D. si l'inscription n'est autorisée qu'aux mineurs ayant atteint l'âge du consentement numérique, il faut également relever que le consentement donné lors de l'inscription ne serait pas suffisamment « caractérisé » pour permettre au responsable de traitement de baser les traitements sur celui-ci.

En effet, en matière de protection des données, il ne suffit pas de simplement manifester un simple accord : que ce soit le mineur qui puisse consentir seul ou que ce soit son représentant légal, le responsable de traitement doit veiller à recueillir un consentement « caractérisé », c'est-à-dire répondant aux exigences prévues par le R.G.P.D. L'article 4. 11) du texte définit en effet le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que les données à caractère personnel la concernant fassent l'objet d'un traitement ».

20. Si ces conditions de validité du consentement appellent des observations applicables à toutes les personnes concernées⁶⁶, c'est surtout l'exigence du consentement « éclairé » qui pose question pour les mineurs. Cette exigence est un corollaire du principe de transparence qui gouverne, entre autres, la collecte et le traitement de données à caractère personnel. Pour que le consentement soit éclairé, le Groupe 29 est d'avis que différentes informations doivent, au minimum, être fournies à la personne

concernée, comme l'identité du responsable de traitement, la/les finalité(s) de traitement pour la/lesquelle(s) le consentement est requis, le type de donnée qui va être collecté, le droit pour elle de retirer son consentement à tout moment, etc.⁶⁷. Le responsable de traitement doit, en résumé, veiller à ce que le consentement de la personne concernée soit donné sur la base d'informations qui permettent à celle-ci de savoir exactement à quoi elle consent. S'agissant de la forme que doit prendre la communication de ces informations, elle peut être diverse (écrite, orale, audio, vidéo, ...) pour autant que le message soit facilement compréhensible pour toute personne, c'est-à-dire qu'elle ne peut consister en des clauses longues et inintelligibles ou rédigées en termes juridiques.

Si l'obtention d'un tel consentement éclairé n'est déjà pas simple pour un public adulte, le Groupe 29 insiste sur le fait que si le public cible comprend des mineurs « il convient que le responsable du traitement s'assure que les informations soient compréhensibles pour ceux-ci »⁶⁸. Cette obligation est également contenue au considérant 58 du R.G.P.D. qui dispose « les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne devraient être rédigées en de termes clairs et simples que l'enfant peut aisément comprendre ».

L'Autorité de contrôle indiquait déjà il y a plusieurs années que le responsable doit utiliser un style direct et s'adresser directement à l'enfant, en se présentant, renseignant son adresse et la façon dont le mineur peut obtenir plus d'informations le concernant et expliquer au mineur pourquoi il lui est nécessaire d'obtenir certaines informations person-

⁶⁶ Voy. notamment C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, C. DE TERWANGNE, K. ROSIER (dir.), coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 120 à 126.

⁶⁷ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 15.

⁶⁸ *Ibid.*, p. 16.

nelles. L'Autorité recommande par ailleurs au responsable de traitement d'encourager le mineur à informer ses parents de ses activités en ligne, à les faire participer à ces activités et à leur demander leur avis avant de fournir ses données. L'exemple d'un encart destiné aux parents placé sur la première page du site où les données sont collectées, pour les informer de la politique en matière de traitement de données à caractère personnel, est donné⁶⁹. L'exposé des motifs de la loi belge ayant implémenté le R.G.P.D. insiste également sur l'importance de la communication: «il est primordial que le responsable de traitement mette en œuvre une information claire et adaptée au jeune public en l'informant de tous les droits que le jeune détient ainsi que de toutes les conséquences que comporte l'utilisation de ce service de société de l'information sur sa vie privée et ses données à caractère personnel»⁷⁰.

21. Comme indiqué *supra*, Facebook se base par exemple sur le consentement de l'utilisateur pour utiliser la technologie de la reconnaissance faciale⁷¹. Via les paramètres du compte, il est possible d'accéder à un onglet «reconnaissance faciale». En cliquant sur «en savoir plus», on accède à des illustrations qui expliquent ce qu'est la reconnaissance faciale et pourquoi elle est utilisée⁷². Il convient ensuite de répondre à la question «voulez-vous que Facebook

puisse reconnaître si vous apparaissez dans des photos et vidéos?» par «oui» ou «non».



Sélectionnez **Oui** si vous souhaitez que Facebook vous reconnaisse sur des photos ou dans des vidéos.

Pour cet exemple particulier, il semble qu'on puisse déterminer la portée du consentement que l'on donne, les explications étant *user-friendly*. Il faut toutefois rétrécir quelque peu la perspective et se placer du point de vue de l'enfant de 13, 14 ans, qui n'entreprendra vraisemblablement pas la démarche d'aller consulter ces différentes pages et qui cochera sans doute la case «oui» sans se renseigner plus avant...

22. En conclusion, recueillir un consentement conforme aux exigences du R.G.P.D. ne semble pas chose aisée, et ce davantage lorsque la personne concernée est un enfant. Il s'en déduit que conditionner la possibilité de s'inscrire sur les réseaux au fait d'avoir l'âge du consentement numérique ne suffira en tout état de cause pas pour s'assurer que la personne qui s'inscrit, que ce soit l'enfant seul ou l'enfant par l'intervention de ses parents, exprime un consentement parfaitement conforme au règlement européen, outre le fait qu'il doit s'agir d'un acte distinct à celui posé lors de l'inscription.

⁶⁹ Autorité de protection des données, avis n° 38/2002 du 16 septembre 2002, n.réf.: 10/A/2002/029.

⁷⁰ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 11 juin 2018, exposé des motifs, *op. cit.*, p. 18.

⁷¹ Outil qui analyse les photos et vidéos de l'utilisateur et les compare avec celles dans lesquelles il est identifié, à plusieurs fins comme par exemple l'identifier rapidement dès qu'une photo de lui est publiée, sans démarche de sa part.

⁷² Page disponible à l'adresse: <https://www.facebook.com/about/basics/manage-your-privacy/face-recognition#2>.

III. LA RESTRICTION D'ACCÈS AUX RÉSEAUX SOCIAUX N'EST PAS EFFICACE

23. Au travers de ce dernier point, nous verrons que tant l'éventualité d'une restriction de l'inscription sur les réseaux que la fixation de l'âge du consentement numérique ne sont pas exemptes de critiques et que pour l'heure, elles manquent encore leur but de protection des plus jeunes.

A. L'inscription sur un réseau social : la fraude à l'âge

24. Si les médias ont annoncé une restriction des possibilités d'inscription des plus jeunes sur Facebook, on n'en retrouve aucune trace en pratique, excepté sous la barre des 13 ans, ce qui est la politique de Facebook. Aucun texte ne prévoit cette interdiction, qui, en plus de n'être ni opportune, ni suffisante pour garantir que le consentement requis pour traiter des données personnelles est légal, ne serait nullement efficace.

Si l'on crée un profil en encodant une date de naissance qui manifeste un âge inférieur à 13 ans, Facebook refuse l'inscription. Par contre, la critique à formuler contre ce dispositif supposé «filtrer les inscriptions», est qu'il n'y a pas de contrôle de l'âge et qu'il est tout à fait possible de mentir. La seule vérification demandée au moment de l'inscription est de confirmer le compte via un lien reçu par e-mail. Les conditions générales de Facebook prévoient que si l'utilisateur enfreint les conditions générales, le compte pourra être suspendu ou désactivé définitivement. C'est donc par cette sanction *a posteriori* que Facebook entend faire respecter, notamment, la condition d'inscription liée à l'âge de l'utilisateur. Celle-ci engendrerait la suppression journalière de 20.000 comptes au motif qu'ils

ont été créés par des mineurs de moins de 13 ans⁷³.

Pour l'heure, il est donc tout à fait possible pour des enfants de moins de 13 ans d'accéder au réseau social et de «sortir des radars». Une enquête menée en 2014 démontrait d'ailleurs que 35% des enfants flamands entre 9 et 12 ans avaient un profil Facebook⁷⁴. Dès lors, lorsqu'on affirme que, suite à l'entrée en vigueur du R.G.P.D., les enfants en dessous d'un certain âge ne pourront s'inscrire seuls sur les réseaux sociaux, force est de constater que cette limitation n'est nullement appliquée ou en tous cas qu'aucun procédé n'est mis en œuvre pour la rendre effective.

B. Les vérifications liées à l'âge et l'identité du parent affaiblissent le consentement au traitement de données

25. Ensuite, si déjà au moment de l'inscription, une faille se révèle compte tenu de la non-vérification de l'âge des enfants, force est de constater que l'article 8 du R.G.P.D. n'est, en lui-même, pas à l'abri de tout reproche, notamment compte tenu des vérifications auxquelles doit procéder, au stade de l'obtention du consentement, le responsable de traitement.

Facebook doit, s'il utilise le consentement comme base légale de traitement et que cela concerne un mineur, faire la distinction entre d'une part les enfants qui peuvent consentir seuls au traitement et ceux pour lesquels le consentement du représentant de l'autorité parentale est requis. Le règlement dispose que: «le responsable de traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technolo-

⁷³ L. PAILLER, *op. cit.*, p. 39.

⁷⁴ Commissariat aux Droits de l'enfant de la Communauté flamande, avis du 22 avril 2016, précité.

giques disponibles»⁷⁵. Deux obligations pèsent donc sur le responsable de traitement : vérifier que le mineur ne ment pas sur son âge pour éviter de devoir recourir à l'intervention de ses parents/représentants (1) et que ce sont bien ces derniers qui ont donné leur consentement et non l'enfant (2).

1. La vérification de l'âge de l'enfant

26. Tout comme au stade de l'inscription, il est fastidieux pour le responsable de traitement de mettre en place un procédé qui lui permette de vérifier que le mineur, lorsqu'il l'autorise à traiter certaines données, ne ment pas sur son âge.

Lors de l'élaboration de la loi belge du 30 juillet 2018, il a été suggéré de vérifier l'âge de l'enfant en exigeant une lecture de la carte d'identité. Si une telle vérification semble envisageable dans un contexte « extra-numérique », il peut sembler lourd d'exiger d'un adolescent de 13 ans (qui, en Belgique, a pour rappel atteint l'âge du « consentement numérique ») d'introduire sa carte d'identité dans un lecteur dès qu'il doit confirmer son accord au traitement de ses données.

Le Groupe 29 estime que si l'utilisateur indique qu'il a l'âge minimum du consentement numérique, le responsable de traitement peut effectuer des vérifications raisonnables pour s'assurer que cette affirmation est vraie. La nécessité de déployer ces efforts raisonnables est sous-entendue dans le R.G.P.D., dès lors que si enfant donne son consentement sans avoir l'âge requis pour le donner, le traitement de données sera illicite⁷⁶. Le Groupe 29 précise toutefois que la vérification liée à l'âge de la personne concernée ne doit pas non plus entraîner un traitement de données excessif et

qu'il faut évaluer les risques liés au traitement envisagé⁷⁷. Lorsque le risque est faible, il pourrait être suffisant de demander à un nouvel abonné à un service de révéler son année de naissance. En cas de doute, le Groupe 29 recommande au responsable de traitement de « réviser ses mécanismes de vérification de l'âge dans un cas donné et évaluer si des méthodes de vérification alternatives sont nécessaires »⁷⁸. Le commissariat aux Droits de l'enfant de la Communauté flamande encourage, au même titre que ce qu'avait suggéré le Comité général aux droits de l'enfant des Nations Unies, les fournisseurs de réseaux sociaux à mettre en place des mesures techniques permettant de différencier les âges selon l'usage qui est fait des réseaux, par exemple via des paramètres « vie privée » renforcés. Ce comité avait en effet préconisé : « que les États s'assurent que tous les enfants aient accès à une information compréhensible et *child-friendly* sur la manière dont leurs données sont collectées, conservées, utilisées et potentiellement partagées. À cet égard, les États doivent veiller à assurer que des paramètres vie privée adaptés à l'âge et des informations et avertissements clairs soient disponibles pour les enfants qui utilisent des médias digitaux et des technologies de l'information »⁷⁹.

27. Pratiquement, pour ce qui concerne les permissions qui sont demandées à l'utilisateur de Facebook pour traiter certaines données (ex. opinion politique de l'utilisateur), aucune vérification complémentaire n'a lieu suivant l'expérience que nous avons pu faire. Or, Facebook devrait, au moment de demander un consentement particulier pour activer une

⁷⁵ *Ibid.*, p. 30.

⁷⁶ *Ibid.*, p. 30.

⁷⁹ *Committee on the rights of the child, Report of the 2014 day of general discussion "Digital media and children's rights"*, § 103, disponible à l'adresse : https://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf. Traduction libre.

⁷⁵ R.G.P.D., article 8.2.

⁷⁶ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 29.

option comme la reconnaissance faciale, révérier l'âge de l'utilisateur, sans se baser sur celui qui a été encodé lors de l'inscription qui peut être faux ou inférieur à l'âge fixé en application de l'article 8 du R.G.P.D. Un tel contrôle semble à ce stade insurmontable, d'autant qu'il ne peut constituer une atteinte supplémentaire aux règles protégeant les données personnelles. Tel serait le cas si le réseau social exigeait de l'utilisateur qu'il exprime son consentement aux traitements visés au moyen de sa carte d'identité électronique.

28. Si ce contrôle – qui n'est donc pas garanti pour l'heure – aboutit au constat que le mineur n'a pas l'âge de consentir, encore faut-il que le réseau obtienne la permission de la part de son responsable parental.

2. La vérification de l'origine parentale du consentement

29. Si la première vérification décrite ci-avant révèle que le mineur ne peut consentir seul au traitement de ses données, le responsable de traitement pourra accepter cet état de fait mais devra s'efforcer, raisonnablement, de s'assurer que le consentement est donné par le responsable de l'autorité parentale et donc de vérifier l'origine parentale du consentement. Au vu de la formulation du règlement⁸⁰, on peut supposer que l'obligation qui pèse sur le responsable de traitement est une obligation de moyens, et non de résultat. Il n'en reste pas moins qu'en vertu du principe d'*accountability* prévu par le règlement, le responsable de traitement doit pouvoir démontrer qu'il a mis en œuvre les moyens nécessaires pour s'assurer de ce que le consentement recueilli émane du responsable du mineur.

Le Groupe 29 a toutefois souligné que « ces efforts devraient être proportionnels à la nature

des activités de traitement et aux risques qui y sont liés », conformément au principe de minimisation des données, qui exige d'opter pour une approche proportionnée dans la collecte des données⁸¹. Sous le couvert d'une approche proportionnée, le responsable de traitement pourrait donc uniquement veiller à obtenir une faible quantité d'informations, comme par exemple les coordonnées d'un parent ou d'un tuteur⁸².

Comme pour la vérification liée à l'âge de l'enfant, le Groupe 29 recommande que le responsable de traitement adopte une approche fondée sur les risques liés au traitement pour vérifier l'identité du titulaire de l'autorité parentale. Si le traitement présente un risque faible, la vérification de la responsabilité parentale par e-mail peut être suffisante. Si le traitement présente des risques plus élevés pour la protection des données personnelles, le responsable de traitement devra récolter davantage de preuves pour démontrer l'obtention du consentement du responsable de l'autorité⁸³. Le responsable de traitement pourrait par exemple suivre ces étapes : demander au client mineur s'il a l'âge du consentement numérique (16 ans ou moins en fonction de l'État membre) (i), si ce n'est pas le cas, informer le client mineur que son parent ou tuteur doit donner son consentement et lui demander de fournir l'adresse e-mail d'un de son parent/tuteur (ii), contacter par e-mail le parent/tuteur, obtenir son consentement et adopter des mesures raisonnables pour vérifier que l'adulte est bien responsable de l'autorité parentale (iii)⁸⁴. Le texte du *Children's Online Privacy Protection Act* américain (COPPA) fournit également des indications sur les méthodes

⁸¹ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 21.

⁸² *Ibid.*, p. 30.

⁸³ *Ibid.*, p. 30.

⁸⁴ *Ibid.*, p. 31.

⁸⁰ R.G.P.D., article 8.2.

qu'il est possible d'utiliser pour vérifier l'origine parentale du consentement: un formulaire à signer par le parent et à renvoyer (par courrier postal ou *scan*) au responsable de traitement, l'utilisation, par le parent, d'une carte de crédit ou autre méthode de paiement en ligne, un appel téléphonique ou une vidéo-conférence avec le parent...⁸⁵

Le Groupe 29 reconnaît que les vérifications développées ci-dessus peuvent s'avérer ardues, notamment si le mineur qui est en âge de consentir au traitement n'a pas encore établi une « empreinte identitaire » ou lorsque la responsabilité parentale n'est pas facilement vérifiable, auxquels cas ces difficultés seront prises en compte au moment de décider si le responsable de traitement a fourni des « efforts raisonnables »⁸⁶.

30. Sur le fondement même de l'approche du législateur européen, d'aucuns doutent également du fait que l'autorisation des parents soit une garantie contre les atteintes à la vie privée de leurs enfants. En effet, il n'est pas certain que les parents soient eux-mêmes bien conscients des enjeux en matière de vie privée sur les réseaux. Le cas du *sharenting* est souvent cité comme désignant: « le partage par des parents ou des grands-parents de photographies et de vidéos de leurs enfants ou petits-enfants sur les médias sociaux ». Les chiffres de cette pratique ne trompent pas puisqu'une enquête réalisée il y a près de dix ans démontrait déjà que « 81 % des enfants de moins de deux ans dans dix pays à revenu élevé (Allemagne, Australie, Canada, Espagne, États-Unis, France, Italie, Japon, Nouvelle-Zélande et Royaume-

Uni) avaient une empreinte numérique, ce qui signifie qu'ils avaient un profil personnel ou des photographies d'eux en ligne »⁸⁷.

L'Unicef critique également la fixation d'un âge par le règlement, notamment compte tenu du fait qu'il limite la liberté d'expression des enfants, leur accès à l'information et leur habileté numérique⁸⁸. Il est aussi prôné par le commissariat aux Droits de l'enfant de la Communauté flamande qu'il est préférable de fournir une meilleure éducation aux médias et de privilégier le dialogue parents-enfants, plutôt que soumettre l'accès aux réseaux sociaux à l'accord des parents⁸⁹.

Il apparaît en tout cas que l'article 8 du R.G.P.D., critiqué pour partie, n'a pas encore atteint ses objectifs, puisque la protection qu'il est supposé garantir est largement lettre morte, en tous cas dans le cadre de Facebook. En effet, une rapide expérience sur ce réseau nous a montré qu'aucune vérification n'était faite, ni pour s'assurer que l'utilisateur mineur a bien l'âge du consentement numérique, ni *a fortiori* pour voir si son référent autorise les traitements pour lesquels son autorisation est requise.

C. La disparité des législations nationales

31. Outre les problèmes précités qui affaiblissent la protection des plus jeunes compte tenu des vérifications auxquelles doit s'adonner le responsable de traitement, celui-ci doit par

⁸⁵ Children's online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505, disponible à l'adresse: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>.

⁸⁶ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 31.

⁸⁷ G. MATHIEU, A.C. RASSON, « Les droits de l'enfant dans l'environnement numérique: à la recherche d'un subtil équilibre entre protection et autonomie », in *Vulnérabilités et droits dans l'environnement numérique*, op. cit., p. 425.

⁸⁸ Unicef, La situation des enfants dans le monde 2017. Les enfants dans un monde numérique, résumé du rapport, p. 32, disponible à l'adresse: https://www.unicef.org/french/publications/files/SOWC_2017_Summary_Fr_WEB.pdf.

⁸⁹ Commissariat aux Droits de l'enfant de la Communauté flamande, avis du 22 avril 2016 précité.

ailleurs examiner scrupuleusement les différentes législations susceptibles de s'appliquer à ses services. En effet, le législateur européen a laissé le choix aux États membres de fixer à 16, 15, 14 ou 13 ans l'âge à partir duquel le mineur était considéré comme apte à consentir seul au traitement de ses données. Il en résulte que si le service proposé est un service transfrontalier, le prestataire ne pourra se contenter de respecter uniquement la législation de l'État membre dans lequel il est principalement établi, mais peut être contraint de respecter les législations nationales respectives de tous les États membres vers lesquels il dirige ses services⁹⁰. Les États membres peuvent en effet définir comme loi applicable celle du pays dans lequel le responsable de traitement a son établissement principal ou celle de l'État dans lequel la personne concernée réside⁹¹.

Par exemple, la loi belge du 30 juillet 2018 prévoit qu'elle s'applique lorsque le responsable de traitement est établi sur le territoire belge et, à certaines conditions, lorsque la personne concernée est domiciliée sur le territoire belge⁹². Lors de l'élaboration de cette législation, il a été relevé que « malheureusement, la marge de manœuvre laissée aux États membres sur l'âge de l'enfant crée une discordance de la loi applicable au sein même de l'Union européenne »⁹³. Le Conseil d'État, dans son avis sur l'avant-projet de loi belge, a quant à lui soulevé que : « compte tenu des critères de rattachement territoriaux de l'article 4, la disposition ne sera pas applicable aux traitements de données à caractère personnel d'enfants par des responsables de traitement

établis dans d'autres États membres de l'Union européenne »⁹⁴. Selon la doctrine, « cette latitude étant offerte au niveau national, il se peut que, sur ce point, on retrouve une hétérogénéité qu'on avait voulu éviter en optant pour un règlement plutôt qu'une directive »⁹⁵.

32. En conséquence, le R.G.P.D., qui laisse une marge de manœuvre aux États membres, engendre des conflits de loi puisque l'application de deux lois nationales exécutant le règlement peut amener à des solutions divergentes s'agissant du droit applicable⁹⁶. Sans rentrer dans une analyse fouillée des règles de droit international privé régissant la matière, qui devrait faire l'objet d'une contribution à part entière⁹⁷, prenons un exemple concret pour le cas qui nous occupe.

On l'a dit, l'âge du consentement numérique a été fixé à 13 ans en Belgique et à 15 ans en France. Un opérateur dont le seul établissement se situe en Belgique et qui collecte, dans le cadre d'un service de la société de l'information, des données relatives à un enfant de moins de 15 ans résidant en France, sur la base du consentement de ce dernier, est dans une

⁹⁴ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 11 juin 2018, avis du Conseil d'État, section de législation, n° 63.192/2 du 19 avril 2018, p. 412.

⁹⁵ C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », *op. cit.*, p. 130.

⁹⁶ N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *R.D.C.*, 2019/1, p. 77.

⁹⁷ Voy. notamment à ce sujet: N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, pp. 52-78; N. MICHAIL, « Entre le RGPD et le règlement Bruxelles Ibis: quel juge pour protéger nos données personnelles ? », *D.C.C.R.*, 2019/1-2, nos 122-123, pp. 175-200; J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 235-271.

⁹⁰ Groupe de travail « Article 29 » sur la protection des données, Lignes directrices précitées, p. 29.

⁹¹ *Ibid.*, p. 29.

⁹² Loi du 30 juillet 2018 précitée, article 4.

⁹³ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 11 juin 2018, exposé des motifs, *op. cit.*, p. 20.

situation délicate⁹⁸. En effet, en vertu du droit français, applicable dès lors que la personne concernée réside en France, ce traitement est illicite si le parent du mineur n'a pas consenti, puisque l'enfant a moins de 15 ans. Par contre, en vertu du droit belge, également applicable en vertu du critère de rattachement lié à l'établissement sur le territoire belge, ce traitement est licite puisqu'en vertu de la loi belge, le consentement du parent n'est plus nécessaire si l'enfant a plus de 13 ans.

33. Si ces divergences de contenus entre les lois applicables rendent la tâche des responsables de traitement ardue, notons que cette question se pose également dans le chef de parents qui voudraient agir, par exemple, contre un réseau social qui aurait collecté, de manière illégale, certaines données relatives à leur enfant, en se basant sur un consentement obtenu sans respecter l'article 8 du R.G.P.D. Ceux-ci devront également veiller à se fonder sur le droit applicable au litige, qui ne sera pas forcément le R.G.P.D.⁹⁹ ni leur loi nationale, et agir devant le juge compétent.

Facebook leur facilite la tâche puisqu'il prévoit que l'action en réclamation d'un consommateur résidant dans un pays de l'Union européenne à l'encontre du réseau sera régie par le droit de cet État et jugée par les juges de cet État¹⁰⁰. Les parents d'un mineur belge pour-

raient donc se prévaloir de la loi du 30 juillet 2018 et agir devant une juridiction belge pour faire valoir leurs droits à l'encontre de Facebook. Ce réseau social, de par son ampleur, reste toutefois une exception. Il y a en effet fort à parier que les responsables de traitement tentent, tant que faire se peut, d'être soumis à des règles moins contraignantes s'agissant du respect des données personnelles des citoyens. Chaque partie risque par ailleurs de soutenir que la loi la plus favorable à sa thèse s'applique et l'éventuelle double application de lois nationales aux contenus divergents posera sans conteste des difficultés.

IV. CONCLUSION

34. Le R.G.P.D. ne doit pas avoir pour effet d'interdire à certains mineurs de s'inscrire sur un réseau social tel que Facebook sans l'accord de leurs parents. Ce règlement a uniquement vocation à encadrer le sort des données personnelles des citoyens, et notamment des mineurs. L'article 8 du texte régit spécifiquement la manière dont peut être recueilli le consentement d'un mineur, lorsque c'est cette base légale de traitement des données qu'en-tend utiliser le responsable de traitement.

Certains acteurs, étatiques ou médiatiques, affirment pourtant que l'âge pour accéder aux réseaux sociaux sans permission parentale est l'âge fixé par le R.G.P.D. ou les lois nationales l'implémentant, à savoir celui du « consentement numérique ». Ce raccourci n'est ni opportun, ni suffisant, ni efficace.

réclamation devant tout tribunal de cet État membre qui est compétent pour statuer sur la réclamation. Dans tous les autres cas, vous acceptez que la réclamation doit être résolue devant un tribunal compétent de la République d'Irlande et que la loi irlandaise régira les présentes Conditions et toutes les réclamations, sans égard aux dispositions en matière de conflits de lois ».

⁹⁸ Exemple inspiré de la contribution de N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 78.

⁹⁹ Le champ d'application territorial du R.G.P.D. est défini en son article 3.

¹⁰⁰ Conditions générales de Facebook disponibles à l'adresse: <https://www.facebook.com/legal/terms>: « si vous êtes un consommateur et que vous résidez habituellement dans un État membre de l'Union européenne, les lois de cet État membre s'appliqueront à toute réclamation, à toute cause d'action ou à tout litige à notre encontre, qui découle des présentes conditions ou des Produits Facebook, ou en lien avec ceux-ci ("réclamation"), et vous pouvez résoudre votre

35. Premièrement, l'accord éventuellement exprimé pour l'utilisation de données est à différencier de celui manifesté lors de l'inscription sur le réseau, qui engendre uniquement la conclusion d'un contrat d'utilisation avec celui-ci. Lors de la création du compte, l'utilisateur consent en effet aux conditions générales du réseau, et à la politique d'utilisation de données, mais n'est pas encore sollicité pour donner son accord quant au traitement de certaines de ses données personnelles. Il est donc tout à fait possible qu'un mineur ait, en vertu du droit des contrats, la capacité de discernement suffisante pour conclure valablement ce contrat d'utilisation, mais n'ait pas encore atteint l'âge du consentement numérique fixé par le R.G.P.D., en manière telle que le responsable de traitement puisse être contraint de faire appel aux parents du mineur lorsqu'il doit obtenir ce consentement particulier.

Par ailleurs, il n'est pas suffisant de calquer les seuils d'âges en estimant que ce qui est manifesté lors de l'inscription (un accord parental ou une acceptation du mineur en âge de la formuler seul) est de nature à permettre le respect des exigences du règlement européen en matière de consentement. Ce consentement doit en effet être caractérisé et spécialement éclairé dans le chef des enfants.

Enfin, une telle restriction « à l'entrée » des réseaux, si elle existe, n'est nullement efficace. En pratique, il est très facile de mentir sur son âge lors de l'inscription, pourvu qu'un âge supérieur à 13 ans soit encodé. Aucune vérifi-

cation n'a lieu, ni au niveau de l'inscription, ni d'ailleurs lorsque le consentement particulier est demandé pour l'utilisation de certaines données.

La protection des plus jeunes voulue par le législateur européen est également affaiblie suite à la marge de manœuvre laissée aux États membres dans la fixation du seuil d'âge du consentement numérique, qui aboutit à des conflits de loi applicable.

36. Les prestataires de services de la société de l'information comme Facebook peuvent se contenter de déployer des efforts raisonnables pour se conformer au règlement, ce qui déforce probablement la mise en œuvre de procédés efficaces pour vérifier qui surfe sur leur réseau. Dès lors, plutôt que de verrouiller l'accès au réseau inopportunément, certains prônent tantôt une éducation plus poussée aux médias et à la protection des données, tantôt une sensibilisation plus poussée dans le chef des parents afin qu'ils surveillent leurs enfants lors de leur expérience sur les médias sociaux.

Il semble en effet qu'il s'agisse de pistes intéressantes qui, combinées aux règles existantes, devraient toutefois mener prochainement à un positionnement des Autorités de contrôle et de la jurisprudence sur les mesures réellement prises par les responsables de traitement pour mettre les plus jeunes à l'abri des dangers d'un partage massif de leur vie privée, notamment sur la base d'un consentement tronqué.