nos 122-123
Droit de la consommation
DCCR
Consumentenrecht

DOCTRINE - RECHTSLEER

Consentement et RGPD : des zones d'ombre !

Yves Poullet

1. Le consentement est devenu, avec la Charte européenne des droits fondamentaux, la première source de licéité des traitements de données à caractère personnel. Cette source s'inscrit parmi d'autres fondements, en particulier le contrat et l'intérêt légitime. Le RGPD en a renforcé les exigences et les a déclinées suivant les données concernées ou les traitements en cause. Faut-il conclure que tout est dit en la matière ? Notre propos est de relever certaines zones d'ombre et d'attirer l'attention sur les dangers liés à cette hypertrophie du consentement. La récente législation californienne adoptée en juin de cette année, le « *Consumer Privacy Act* »[1], nous paraît proposer une autre approche par ailleurs suivie par la proposition de directive européenne sur les contrats à contenu numérique[2]. En d'autres termes, notre propos est de répondre à la question : avons-nous besoin du consentement ?

2. Pour répondre à cette question, la démarche suivante est proposée. Dans un premier temps, nous partirons des textes, celui du RGPD[3], certes mais également des avis[4] et des *Guidelines*[5] émis par le groupe dit de l'article 29 et depuis endossés, mise en application du RGPD oblige, par le Comité européen de protection des données

[1] *Consumer Privacy Act – An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy*, Assembly Bill No. 375, approuvé par le « Governor » de l'État de Californie, le 28 juin 2018 (en abrégé, CCPA).

[2] Commission européenne, Directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, COM(2015) 634 final, 9 décembre 2015. Sur ce projet de directive, voy. le commentaire très critique et plein d'humour de S. GUTWIRTH et G. GONZALEZ-FUSTER, « L'éternel retour de la propriété des données – de l'insistance d'un mot d'ordre », in E. DEGRAVE *et al.* (dir.), *Droit, normes et libertés dans le cybermonde, Liber Amicorum Yves Poullet*, coll. du CRIDS, Larcier, n° 43, pp. 135 et s. et l'avis 4/2017 du CEPD, 17 mars 2017.

[3] Règlement (UE) n° 2016/679 du 27 avril 2016, *J.O.U.E.*, L 119/1, 4 mai 2016.

[4] Groupe de l'article 29, « Avis 15/2011 sur la définition du consentement », 01197/11/FR WP187, 13 juillet 2011 ; voy. également, « Avis 06/14 sur la notion d'intérêt légitime poursuivi par le responsable du traitement au sens de l'article 7 de la directive 95/46/CE », 844/14/FR WP 217, 9 avril 2014.

[5] Groupe de l'article 29, « Guidelines on consent under Regulation 2016/679 », 17/EN WP 259, 28 novembre 2017. On ajoute que le 25 mai 2018, l'*European Data Protection Board* (Comité européen de protection des données), mis en place par le RGPD (articles 68 et s.), doté de compétences nettement élargies par rapport au groupe de l'article 29, a confirmé les Guidelines rédigées par le groupe de l'article 29. Le communiqué de l'EDPB précise leur portée : « *The positions of EDPB are recommendations for the practical implementation of the GDPR. They have no binding effect for courts. Ultimately, they are views agreed between the different EU authorities – in other words – positions of an executive body which cannot replace EU laws…* ».

créé par l'article 68 du règlement[6]. Cette première analyse nous permet d'aborder ce que nous appelons les zones d'ombre. Le consentement distingué du contrat est-il un acte unilatéral ? Avec quelles conséquences ? Comment lire l'article 6 du RGPD qui consacre le consentement par rapport à l'article 5 qui fixe les principes applicables à tous les traitements ? Les raisons pour lesquelles le RGPD souhaite distinguer le consentement du contrat sont-elles pertinentes ? C'est à cette question que nous chercherons à répondre dans la seconde partie en analysant les textes récents californiens et européens repris au point précédent. En conclusion, nous plaiderons pour une remise en cause à la fois de l'approche individualiste qui caractérise le RGPD et de la prééminence qu'il confère au consentement.

I. Le consentement au traitement : l'analyse des textes

3. Notre réflexion part d'un étonnement. Le consentement n'a pas été de toute éternité consacré comme cause de légitimité des traitements de données à caractère personnel. Ainsi, les législations nationales de première génération ne mentionnent pas le consentement. Sur le plan international, ni la Convention n° 108 (1981), ni les lignes directrices de l'OCDE (1980), ni les lignes directrices des Nations unies pour la réglementation des fichiers de données personnelles automatisées (1990) ne mentionnent le consentement. C'est à la directive européenne 95/46 que l'on doit l'introduction à la fois d'une définition du consentement (article 2, h)[7]) mais au-delà sa consécration par l'article 7 du consentement comme principe de légitimation du traitement, le premier cité[8].

Depuis, le consentement est devenu le pilier essentiel sur lequel s'appuie le droit devenu quasi constitutionnel de la protection des données. L'article 8 de la Charte européenne des droits fondamentaux du 7 décembre 2000, devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne[9], énonce ce droit comme suit :

---

[6] Nous n'avons pas pu tenir compte des « Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects » adoptés par l'EDPB, le 9 avril et soumis à consultation publique. Ces Guidelines étudient l'étendue et les limites d'une base contractuelle en cas de traitement de données à caractère personnel soit à des fins de prévention de fraude, d'amélioration du service ou de personnalisation du contenu. Ces Guidelines confirment notre conviction selon laquelle le consentement comme base autonome de licéité d'un traitement nous apparaît superflu.

[7] « h) "consentement de la personne concernée" : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

[8] « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si : a) la personne concernée a indubitablement donné son consentement ou… ».

[9] L'article 6 du Traité sur l'Union européenne (TUE) dispose : « L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux (…) laquelle a la même valeur juridique que les traités ».

> « Toute personne a droit à la protection des données à caractère personnel le concernant.
> 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.
> Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

L'article 16 du Traité sur le fonctionnement de l'Union européenne reprend le libellé même de l'article 8 de la Charte et donne pleine compétence aux autorités européennes pour fixer les règles relatives à la protection des données dans le respect du droit exprimé par la disposition[10].

4. Le règlement (RGPD), pris sur la base de cette compétence, accorde une attention plus grande encore au consentement considéré par le Parlement européen[11] comme « l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données ». Le consentement apparaît par ailleurs comme la consécration la plus évidente du droit à l'« autodétermination informationnelle », qui fonde le régime de protection des données et s'entend comme la liberté de principe de consentir au traitement des données à caractère personnel[12]. Ceci dit, le RGPD renforce de manière substantielle[13] à la fois ses exigences quant à la qualité du consentement, sa nature mais également sa place parmi les autres bases de licéité du traitement. Détaillons les prescrits du RGPD relatifs au consentement[14].

---

[10] Parmi de nombreux commentaires de ces dispositions, voy. A. Debet, J. Massot et N. Metallinos, *Informatique et Libertés*, Lextenso Éditions, 2015, pp. 73 et s. ; C. de Terwangne et K. Rosier (dir.), *Le Règlement général de protection des données (RGPD/GDPR)*, coll. du CRIDS, Larcier, n° 44 ; T. Leonard *et al.*, *Le RGPD : Commentaires article par article*, disponible sur le site : https://www.gdpr-expert.eu.

[11] Comité LIBE du Parlement européen, 21 novembre 2013, Rapport sur la 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Rapporteur J. Ph. Albrecht, « Exposé des motifs », pp. 218-219.

[12] Ce droit a été inséré dans la loi française du 6 janvier 1978 par la loi pour une République numérique du 7 octobre 2016 qui complète l'article 1er ainsi : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ».

[13] Groupe 29, « Guidelines on consent under Regulation 2016/679 », last revised and adopted on 10 April 2018, 28 novembre 2017, WP 259 rev.01, p. 16, 152. L'avis n° 15/2011 (précité, p. 12) réclamait déjà un renforcement des exigences en matière de consentement.

[14] Nous n'aborderons pas ici la question du consentement des mineurs et de la marge de manœuvre laissée sur ce point aux États membres.

A. Les exigences quant à la qualité du consentement

5. La définition du consentement est donnée par l'article 1.11. 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 ». Chaque qualificatif mérite nombre de commentaires[15]. L'exigence d'une manifestation de volonté *libre* signifie que la personne concernée dispose d'une véritable liberté de choix ou est en mesure de refuser ou de retirer son consentement sans subir de préjudice, par exemple par un surcoût disproportionné[16] du service offert. Par ailleurs, on veille à ce qu'aucun risque « de tromperie, d'intimidation, de coercition, ou de conséquence négative significative » n'existe dans les faits[17]. Cette exigence d'un consentement libre soulève la question délicate de la possibilité de fonder le consentement dans le contexte des relations entre employés et employeurs[18] ou administrés et administrations[19] mais, au-delà, chaque fois qu'il y a, comme le note le groupe de l'article 29, « *imbalance of powers* »[20], ce qui pourrait bien être le cas lorsque le service ou le produit est offert dans un contexte de quasi-monopole ou concerne un « bien » de première nécessité. Nous reviendrons sur ce dernier point (*infra*, n° 22) mais notons dès maintenant, à l'appui de notre remarque, que la proposition de règlement européen en cours de discussion finale sur le traitement loyal des utilisateurs professionnels des plateformes en ligne[21] impose des obligations

[15] L'auteur renvoie aux études déjà mentionnées (note 10).

[16] Nous ajoutons « *disproportionné* ». Il nous apparaît en effet normal que le prestataire de services puisse justifier certains avantages aux personnes qui consentent au transfert de données supplémentaires ou à des traitements complémentaires au vu des perspectives de bénéfices liés à ces compléments d'activité générés par ces consentements.

[17] Sur ces points, voy. Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 3.

[18] La question de la licéité du consentement dans le cadre de la relation employeurs-employés est abordée avec nuances dans l'opinion 15/2011 sur la définition du consentement (déjà cité, p. 14) qui conclut : « *Altough there may be a strong presumption that consent is weak in such contexts, this does not completely exclude its use, providedere are sufficient guarantees that consent is really free* ».

[19] Sans doute, n'est-ce qu'un principe pour lequel certaines exceptions peuvent exister. Ainsi, une administration peut dans le cadre des services nouveaux offerts à ses administrés, offrir sur la base du consentement des services d'alerte ou d'informations que l'administré pourrait solliciter. L'employeur, de même, peut proposer à ses employés de bénéficier, moyennant transmission de données relatives à son identité, des bons d'achat ou de réduction auprès de firmes tierces.

[20] Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, pp. 5-6. Il est étonnant que les Guidelines se limitent à l'examen des seules situations de l'employeur et de l'administration sans évoquer ces autres situations d'« *imbalance of powers* », très souvent présents dans les services offerts par les réseaux sociaux, de moteurs de recherche et, de manière générale, par les plateformes en ligne.

[21] Cf. « Draft Regulation on promoting fairness and transparency for business users of online intermediation services », Bruxelles, 26 avril 2018 COM(2018) 238 final 2018/0112 (COD). Voy., en particulier, le considérant n° 2 : « *Given that increasing dependence, the providers of those services often have superior bargaining power, which enables them to effectively behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union* ».

nouvelles[22] à charge des opérateurs de ces plateformes[23], considérant la situation de déséquilibre entre ces derniers et leurs utilisateurs professionnels et *a fortiori* non professionnels.

Enfin, conformément à l'article 7.4., le consentement est présumé ne pas avoir été donné librement si l'exécution d'un contrat est suspendue au consentement pour le traitement de données qui ne sont pas nécessaires à ce contrat. Cette disposition retiendra notre attention lorsque nous considérerons les liens entre les divers fondements de licéité des traitements.

Le consentement doit être *spécifique*. Comme le note le considérant n° 32 du RGPD, « [l]e consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités », en d'autres termes, un consentement propre sera réclamé chaque fois que la finalité poursuivie pour laquelle un consentement est exigé est différente. Le Groupe de l'article 29[24] parle à cet égard de « granularité » du consentement. « Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, ajoute l'article 7.2. du RGPD, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions… ».

L'exigence d'un consentement *éclairé*[25] suppose que la personne concernée reçoive une information, précise l'article 7.2. « sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ». Elle implique un contenu informationnel minimal. Le considérant n° 42 du RGPD réclame que la personne concernée ait connaissance au moins de l'identité du responsable du traitement et des finalités du traitement auquel sont destinées ses données à caractère personnel.

---

[22] Ainsi, par exemple, assurer la transparence des critères de *ranking* des sites web ; décrire le traitement différencié que les plateformes accordent aux services offerts par elles-mêmes, par des sociétés contrôlées par elles ou par d'autres sociétés ainsi avantagées ; notifier à l'avance les modifications envisagées et ne les appliquer qu'après un délai d'au minimum 15 jours ; en cas de résiliation de la fourniture du service à un client professionnel, lui fournir les raisons sans délai ; etc.

[23] La définition de la notion est donnée par l'article 2 (é) de la proposition de directive, elle est particulièrement large. « *"Online intermediation services" means services which meet all of the following requirements : (a) they constitute information society services within the meaning of Article 1(1)(b) of Directive (EU) No 2015/1535 of the European Parliament and of the Council (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded (c) they are provided to business users on the basis of contractual relationships between, on the one hand, the provider of those services and, on the other hand, both those business users and the consumers to which those business users offer goods or services* ;… ».

[24] Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 10.

[25] La directive parlait de consentement « informé ». Le terme « *informed* » est repris dans la version anglaise. Le mot éclairé semble plus exigeant que le mot « informé » dans la mesure où l'information peut être d'un niveau tel qu'elle n'« éclaire » pas la personne concernée.

Les Guidelines du groupe de l'article 29[26] considèrent que d'autres informations sont nécessaires[27] « *to allow the data subject to genuinely understand the processing operations at hand* ». C'est sur la base d'un manque d'informations voire d'informations ne permettant pas un choix libre que les autorités de la concurrence italiennes ont récemment interdit le transfert des données à caractère personnel de WhatsApp à Facebook[28].

Enfin, le RGPD estime que le consentement doit être *univoque*. Mme de Terwangne[29] évoque à cet égard les débats sur le choix de ce qualificatif de préférence à ceux de « non ambigu » (terme utilisé par la directive 95/46) ou d'« explicite », réclamé par le Parlement et conservé pour certains types de données ou d'opérations[30]. Le consentement doit être manifesté « par une déclaration ou un acte positif clair » selon le principe de *distinction* du consentement affirmé par le Groupe de l'article 29[31]. Ainsi, si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, « cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé »[32].

Il est clair que l'indication suivant laquelle la poursuite de la navigation sur un site web équivaut à une acceptation est non recevable et que la présentation d'*opt-in*

---

[26] Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 13.

[27] Ainsi, le type de données visées par le traitement envisagé, sur l'existence du droit de retirer le consentement donné (art. 7, § 3), le cas échéant, l'utilisation éventuelle des données pour une prise de décision automatisée (art. 22, § 2, c)) et, le cas échéant, les risques liés au transfert des données vers un pays n'offrant pas de protection adéquate et en l'absence de garanties appropriées (art. 49, § 1er, a)).

[28] L'autorité antitrust italienne (Autorità Garante della Concorrenza e del Mercato) a jugé que WhatsApp avait, entre autres, incité les consommateurs à donner un consentement plus large que nécessaire pour continuer d'utiliser le service et leur avait fait croire qu'ils n'auraient plus accès à l'application s'ils n'acceptaient pas les nouvelles conditions d'utilisation (décision du 11 mai 2017, http://www.agcm.it/component/joomdoc/allegati-news/PS10601_scorrsanz_omi.pdf/download.html).

[29] C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in C. DE TERWANGNE et K. ROSIER (dir.), *Le règlement général de la protection des données, Analyse approfondie*, *op. cit.*, pp. 125 et s.

[30] Sans entrer dans les détails, notons que le consentement doit être explicite :
- lorsque le consentement est nécessaire et que le traitement porte sur des données relevant selon l'article 9 du RGPD de catégories particulières de données ;
- lorsque la personne renonce au droit de s'opposer aux décisions fondées exclusivement sur un traitement automatisé de données (article 22.2, c) ;
- lorsqu'il s'agit d'autoriser un flux transfrontière, « après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées » (article 49, 1.a).

[31] Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 15. « Le groupe de l'article 29 précise également que les responsables de traitement peuvent développer une procédure de consentement adaptée à leur organisation, telle que des mouvements ("*swipe*" sur un écran, faire un signe devant une caméra, incliner son smartphone dans le sens des aiguilles d'une montre) qui sont des actes positifs » (N. WEINBAUM, « Le consentement à l'ère du RGPD et de la Blockchain », *La semaine juridique, Entreprises et affaires*, 2018, n° 10, p. 30).

[32] Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 16.

précochés ne peut équivaloir à un consentement[33]. La question de la qualité du consentement vis-à-vis de traitements utilisant l'intelligence artificielle est particulièrement soulignée par le projet de rapport *Ethical Guidelines for a Trustworthy AI* récemment émis par le *High Level Expert Group on Artificial Intelligence*[34]. En particulier, on note la remarque suivante : « *As current mechanisms for giving informed consent in the internet show, consumers give consent without consideration. This involves an ethical obligation to develop entirely new and practical means by which citizens can give verified consent to being automatically identified by AI or equivalent technologies. Noteworthy examples of a scalable AI identification technology are face recognition or other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, automatic voice detection). Identification of individuals is sometimes the desirable outcome and aligned with ethical principles (for example in detecting fraud, money laundering, or terrorist financing, etc.). Where the application of such technologies is not clearly warranted by existing law or the protection of core values, automatic identification raises strong concerns of both legal and ethical nature, with the default assumption being that consent to identification has not been given. This also applies to the usage of "anonymous" personal data that can be re-personalized* »[35].

6. On notera que c'est au responsable du traitement de devoir démontrer premièrement que le consentement a bien été donné[36], ce qui suppose l'archivage des consentements donnés mais en outre que toutes les exigences de qualité du consentement imposées par le RGPD ont bel et bien été rencontrées par le système mis en place par lui pour recueillir le consentement. Il s'agit là certes d'une application du principe d'*accountability*, devenu principe général de la protection des données mais que l'article 7.1 rappelle fort à propos s'agissant du consentement : « Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant ». À ce propos, on note les implications techniques de ce devoir : l'article 28 de la loi française du 20 juin 2018 dispose qu'en application de l'article 7 du RGPD, « lorsque le traitement repose sur le consentement de la personne concernée, le responsable de traitement doit être en mesure de démontrer que les contrats qu'il conclut portant sur des équipements ou

[33] Les Guidelines du groupe de l'article 29 précitées donnent d'autres exemples de formules de consentement à considérer comme univoques ou non (Groupe 29, « Guidelines on consent under Regulation 2016/679 », précité, p. 17).

[34] Le projet de rapport soumis à l'ensemble des personnes intéressées a été publié le 18 décembre 2018 (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf).

[35] Projet de rapport cité, p. 11.

[36] On notera qu'en principe, le responsable de traitement devra vérifier l'authenticité du consentement, ce qui peut être difficile. Sur cette question et la solution qu'offrirait la technologie de la Blockchain, N. Weinbaum, « Le consentement à l'ère du RGPD et de la Blockchain », *op. cit.*, p. 31.

services incluant le traitement de données à caractère personnel ne font pas obstacle au consentement de l'utilisateur final… Peut en particulier faire obstacle à ce consentement le fait de restreindre sans motif légitime d'ordre technique ou de sécurité les possibilités de choix de l'utilisateur final, notamment lors de la configuration initiale du terminal, en matière de services de communication au public en ligne et aux applications accessibles sur un terminal, présentant des offres et des conditions d'utilisation de nature équivalente selon des niveaux différenciés de protection des données personnelles »[37].

7. Le cumul d'autant de qualités du consentement surprend. Si d'autres législations protectrices, en particulier du consommateur, réclament le consentement, aucune n'impose autant d'exigences qualitatives à ce dernier. Faut-il y voir dans cette avalanche de qualificatifs une prise en considération de la nécessité particulière de protection qu'imposent les risques majeurs en matière de protection des données et donc de libertés, là où ailleurs, seuls des intérêts économiques sont en jeu ? Faut-il au contraire, devant la réalité des consentements exprimés sur la toile, dont peu sinon aucun ne remplit les conditions légales, constater que ce cumul n'est que pure incantation, là où la pratique des consentements individuels représente une illusoire protection ? Si tel est le cas, il faut admettre que réclamer que le consentement donné présente tant de qualités semble vain. Notre opinion est qu'à ce consentement individuel, il serait préférable, vis-à-vis des « *privacy policies* » imposées plutôt que proposées par les prestataires de services de la société de l'information, de réclamer une négociation collective comme le droit de la consommation le prévoit. Soumettre les « *privacy policies* » à un « consentement collectif » qui fixerait ce qui est acceptable, ce qui est exclu et les marges de manœuvre laissées au prestataire et, peut-être au consentement individuel. Une telle négociation est à notre avis plus protectrice que le consentement individuel, bien souvent illusoire.

Continuer à fonder la légitimité des traitements opérés par des prestataires offrant des services à des franges importantes de la population présente par ailleurs le risque majeur que, saisi par un consommateur ayant « consenti » dans les conditions qui sont celles de chacun de nous lorsque nous naviguons sur le web et cliquons machinalement « j'accepte », les juges des Cours de Strasbourg ou de Luxembourg ne relèvent la distorsion entre la réalité d'un tel consentement et les exigences du RGPD rappelées ci-dessus, que ces juges n'exigent demain le respect de toutes les conditions mises à la licéité du consentement mais de telles exigences ruineraient le recours dans la réalité au consentement. Notre propos – et nous y reviendrons (*infra*, n° 30) –, c'est l'approche purement individualiste du consentement qui nous apparaît

[37] Cet article évite en particulier que les utilisateurs d'un terminal ne soient enfermés dans un éco-système imposé par le fournisseur du terminal ou un opérateur dominant et par là même contraints d'utiliser des services installés par défaut et sans alternative possible.

critiquable là où seule une négociation collective qui fixe les limites du consentement individuel nous apparaît la solution.

8. L'article 7.3 du RGPD[38] précise enfin que le consentement peut être retiré à tout moment. Cette possibilité doit faire l'objet d'une information de la personne concernée et la demande de retrait doit pouvoir s'effectuer de façon aussi facile que le consentement n'a été délivré. Afin de veiller aux intérêts du responsable du traitement qui, de manière légitime, jusqu'au moment du retrait, a procédé au traitement des données collectées, l'article précise bien que le retrait s'effectue sans que ce retrait n'ait de conséquences sur les traitements de données préalablement collectées. Cette protection du responsable a cependant des limites dans la mesure où l'article 17 du RGPD garantit à la personne concernée un droit à l'effacement des données la concernant lorsqu'elle retire son consentement et lorsqu'il n'existe pas d'autre fondement juridique au traitement. Le retrait du consentement pose en outre un problème du fait de l'interprétation donnée par le Groupe de l'article 29 aux dispositions sur les changements de fondements de finalités. Notre point B sur la nature et la place particulière du consentement parmi d'autres causes de licéité du traitement nous donnera l'occasion de revenir sur ce point.

B. La nature et la place particulière du consentement parmi les causes de licéité du traitement

1. Le consentement, un acte unilatéral ?

9. T. Leonard écrit[39] : « D'après nous, le consentement visé par le GDPR ne doit pas être perçu comme créant une relation contractuelle spécifique avec le responsable du traitement mais comme l'exécution d'un devoir légal qui s'impose à titre de protection particulière des personnes concernées par les données. Qu'il constitue la base de licéité ou qu'il permette de lever une interdiction de traitement des données à caractère personnel, il s'impose de par l'effet obligatoire de la loi et non pas comme base d'un accord de volontés entre co-contractants concernant les diverses modalités du traitement à venir… En définitive, le consentement de la personne concernée apparaît comme un acte juridique unilatéral permettant de poser toute une série

[38] « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement ». À noter que dans le cadre de la directive 95/46, l'opinion 15/2011 sur la définition du consentement (déjà citée, p. 32) estimait déjà que le droit au retrait existait implicitement dans cette directive et était exprimé par plusieurs dispositions de la directive e-Privacy 2002/58.

[39] T. Leonard, « Yves, si tu exploitais tes données ? », in E. Degrave *et al*. (éd.), *Law, Norms and Freedoms in Cyberspace, Liber Amicorum Yves Poullet*, coll. du CRIDS, Larcier, n° 43, 2018, p. 663.

d'actes sur les traitements en cause dans le respect du GDPR ». Il s'agit donc d'opposer contrat, acte juridique bilatéral et consentement, acte unilatéral. Le consentement figurerait comme une base de licéité distincte, nécessaire là où la stricte « économie » du contrat ne suffit plus à justifier le traitement de données. Le consentement serait une sorte d'acte unilatéral, dans la mesure où la seule volonté de la personne concernée porterait sur la création d'effets juridiques voulus[40], en l'occurrence la licéité du traitement ou la levée d'interdiction du traitement. P. Wery[41] définit en ce sens l'acte unilatéral comme « une manifestation de volonté émanant d'une personne par laquelle celle-ci décide de faire naître certains effets de droit, sans avoir, pour ce faire besoin du consentement d'autrui ». Sans doute, ces effets de droit sont prévus et encadrés par la loi mais ils sont voulus par la personne concernée sur les données de laquelle porte le traitement. Bien évidemment, il ne peut s'agir, comme c'est le cas dans l'offre publique de récompense, d'un engagement unilatéral de volonté qui mettrait à la charge de la personne concernée des obligations[42] et notamment rendrait impossible toute possibilité de retrait[43], ce que le RGPD prévoit explicitement. La figure de l'engagement unilatéral exclue, peut-on voir dans le « consentement » du RGPD un acte unilatéral d'un autre type ? Il est coutume en droit belge d'analyser l'envoi des conditions générales d'un contrat, d'une part, et leur acceptation, d'autre part, comme constitutifs de deux actes juridiques unilatéraux, le second étant qualifié d'« acte réceptice », dans la mesure où la production des effets juridiques est suspendue à la prise de connaissance de cette acceptation par l'émetteur de l'offre[44]. S'il faut dès lors parler d'acte unilatéral, ce n'est pas pour l'opposer au contrat, dans la

[40] Sur la distinction entre fait et acte juridiques, voy. la thèse déjà ancienne mais toujours d'actualité de J. Hauser, J. Flour, J.L. Aubert et E. Savaux (*Droit civil*, vol. 1, *L'acte juridique*, 2e éd., 2001, n° 497) qui définissent l'acte juridique unilatéral comme suit : « un acte volontaire par lequel une personne, de par sa seule volonté, détermine des effets de droit ».

[41] P. Wery, *Droit des obligations*, vol. 2, *Les sources des obligations extracontractuelles, le régime général des obligations*, 2e éd., p. 23.

[42] L'engagement unilatéral ferait naître à charge de celui qui l'émet des obligations vis-à-vis des tiers. La figure de l'engagement par volonté unilatérale est fortement discutée en France. À ce propos, J.L. Aubert, *v°* « Engagement par volonté unilatérale », *Rép. Civ. Dalloz*. Elle est reçue plus volontiers en Belgique, nonobstant de sévères critiques en ce qui concerne ses applications, notamment à toute une série d'engagements bancaires (Y. Poullet, *La garantie automatique bancaire en droit comparé*, thèse, Louvain-la-Neuve, 1982).

[43] Comme l'écrit Aubert (*Introduction au droit*, 9e éd., A. Colin, 2002, p. 228, note 4) : « Il va de soi que la question (de la reconnaissance de l'engagement par volonté unilatérale) n'a de sens qu'autant qu'il s'agit d'une obligation véritable qui, comme telle, présente un caractère irrévocable, c'est-à-dire que le débiteur ne peut réduire à néant par sa seule volonté. C'est là un point essentiel car on a objecté… que si la volonté individuelle avait le pouvoir de se lier, elle aurait pareillement le pouvoir de se délier. L'affirmation est cependant incompatible : la liberté susceptible d'être reconnue à chacun est de se lier ou de ne pas se lier, elle n'est pas de se lier et de se délier ».

[44] À ce sujet, voy. 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 H. Jacquemin et M. Nihoul, *Vulnérabilités et droits dans l'environnement numérique*, coll. de la Faculté de droit de l'UNamur, Larcier, 2018, p. 74 et les nombreuses références citées, note 153.

mesure où il ne représente qu'une étape de celui-ci. Le consentement est une réponse à une proposition de traitement et à ses modalités, décrites en particulier à travers les « Privacy Policies » dont la personne est informée. Sans doute, reconnaîtra-t-on que bien souvent cette proposition est à prendre ou à laisser et que les « Privacy Policies » ne sont pas négociables ; mais en quoi cela nous étonnera-t-il, à l'heure où les contrats avec les consommateurs, mais non uniquement, sont généralement des contrats d'adhésion et que la théorie du consentement, « acte unilatéral réceptice », y prend naissance ? Au surplus, on souligne que lorsque l'on consent, c'est au regard d'une offre de services et il est difficile de ne pas appeler cela un contrat. On rappelle d'ailleurs que l'analyse des qualités du consentement renvoie à l'analyse du comportement de ce contractant, qu'il soit privé ou public et que la théorie des vices de consentement s'applique à cet acte unilatéral comme en matière de contrat[45].

10. Sans doute, dira-t-on, il importe que le consentement, voire les consentements relatifs aux traitements de données à caractère personnel, soient l'objet d'une ou de déclarations distinctes. Mais est-ce une difficulté, dans la mesure où dans le cadre de transactions passées avec les consommateurs, le droit – précisément pour protéger ces derniers – exige diverses signatures afin de matérialiser la prise de conscience de certaines dispositions ou de certains effets de la transaction et s'assurer de l'adhésion à celles ou ceux-ci ? Dans une étude détaillée sur les mécanismes contractuels mis en place dans le cadre de réseaux sociaux, J.-P. Moiny[46] mettait en évidence cette solution des consentements séparés : « Les consentements dissociés, une volonté expresse serait nécessitée, l'internaute serait mieux éclairé – il serait au moins invité à se poser des questions –… ». Bref, ce qui importe, ce n'est pas de distinguer le consentement du contrat mais de distinguer les consentements au sein du contrat et en tout cas du consentement global au contrat et de prévoir pour chaque finalité spécifique pour laquelle la cause de licéité excède les besoins stricts du contrat ou l'intérêt légitime supérieur du responsable du traitement, un consentement particulier. Une telle séparation des consentements rejoint la volonté des autorités européennes sans s'éloigner des règles de droit civil. Autre sujet de réticence, le caractère unilatéral du retrait s'opposerait à la nature contractuelle du consentement, condition de licéité du traitement. Cette objection peut de même être rejetée dans la mesure où d'autres législations consacrent le droit de rétractation aux fins de protection du consommateur et ce au nom de la

[45] « *Consent is also a notion used in other fields of law, particularly contract law… There is no contradiction, but an overlap, between the scope of civil law and the scope of the Directive : the directive does not address the general conditions of the validity of the consent but it does not exclude them. It means, for instance, that to assess the validity of a contract have to be taken into account* » (opinion 15/2011, déjà citée, p. 6).

[46] J.-P. Moiny, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée – quelques réflexions en droit belge et américain », *Annales de la Faculté de droit de Liège*, 2010, pp. 134 à 218.

protection de ce dernier. Que le besoin de protection d'une personne faible à un autre titre, à savoir la personne concernée, justifie ce droit de retrait du contrat au nom de l'ordre public est évident sans qu'il y ait lieu de recourir à l'artifice de l'acte unilatéral rétractable. « Il appartient alors au législateur – et à la jurisprudence – si cela est politiquement souhaitable – et cela l'est lorsqu'il est question de droits et libertés fondamentaux –, d'intervenir pour "rétablir l'équilibre" »[47]. Telle est la justification du droit de retrait, dès lors d'ordre public et donc auquel la personne concernée ne peut renoncer même contractuellement. La nature contractuelle du consentement entraîne le droit de la personne concernée d'exiger le respect des engagements pris par le responsable de traitement à travers la *Privacy Policy*, entrée dans le champ contractuel et notamment de s'opposer à toute modification unilatérale de cette *Policy*, considérée *a priori* comme abusive. Il est clair que cette sanction n'exclut pas les autres sanctions prévues par le RGPD mais s'ajoute à celles-ci en permettant notamment la réclamation de dommages et intérêts contractuels. Enfin et surtout, la reconnaissance du caractère contractuel permet, lorsque celui qui émet le consentement revêt à la fois la qualité de personne concernée et de consommateur[48], de considérer les *privacy policies* comme partie intégrante des contrats de consommation dont la réglementation pourrait s'appliquer dès lors à ce qui en est partie intégrante, en particulier mais nous reviendrons sur ce point, les dispositions en matière de clauses abusives[49].

2. La place du consentement comme cause de licéité du traitement[50]

11. L'article 6.1. place le consentement en tête des conditions de licéité : « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est

[47] *Ibid.*, p. 222.

[48] Il est à noter que la C.J.U.E. n'hésite pas à utiliser tantôt le concept de « personne concernée », tantôt de « consommateur ». Ainsi, dans l'affaire *Schrems II* par exemple, Maximilian Schrems est qualifié de consommateur par la C.J.U.E. Sans doute, on exceptera de la qualification de « consommateur », le cas des employés et des administrés mais le consentement est-il vraiment à l'œuvre dans ces cadres ? Le consentement du salarié n'est pas considéré comme valable sauf exception, étant donné le lien de subordination en ce qui concerne les salariés et la nécessité d'une obligation légale pour légitimer les traitements des administrations.

[49] En France, les clauses abusives sont désormais visées par le Code civil. L'article 1171 dispose en ce sens que : « Dans un contrat d'adhésion, toute clause qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite ». La révision du Code civil belge en cours de discussion propose en l'article 5.41 du Code des obligations, une disposition similaire à travers la notion d'abus de circonstances que l'article en projet définit comme suit : « déséquilibre manifeste entre les prestations par suite de l'abus par l'une des parties des circonstances liées à la position de faiblesse de l'autre partie ».

[50] Il serait utile de s'interroger sur la place du consentement lorsque le responsable du traitement recourt à un système d'Intelligence artificielle (IA). En effet, quant au profilage souvent obtenu par des systèmes d'IA, le RGPD indique que la personne a le droit de ne pas faire l'objet d'une décision automatisée. Outre le fait que ce principe connaît d'importantes exceptions, on serait, à la lecture du texte du RGPD,

remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques… ». Nous analyserons plus loin si cette condition qualifiée de nécessaire est également suffisante (*infra*, n° 32). Notre attention se concentrera à ce stade sur la place de cette condition de licéité par rapport aux autres conditions de licéité, en particulier le contrat (point b) et l'intérêt légitime (point f). À cet égard, on se référera à l'avis particulièrement éclairant du Groupe de l'article 29, en date du 9 avril 2014 sur la notion d'intérêt légitime du responsable de traitement sur la base de l'article 7 de la directive 95/46/CE[51], avis auquel les Guidelines relatives au consentement prises cette fois sur la base du RGPD font toujours référence[52].

L'avis souligne la particularité du consentement comme condition de licéité par rapport aux autres conditions[53]. Si nous nous en tenons aux deux autres conditions de licéité que sont le contrat et l'intérêt légitime, nous notons que le contrat existant ou à conclure (mesures précontractuelles) ne peut rendre licites les traitements que dans le cas où ces derniers sont strictement parlant nécessaires à l'exécution de ce contrat. La référence à l'intérêt légitime comme condition de licéité exige de son côté le contrôle de la balance d'intérêts ou de droits entre ceux avancés par le responsable de traitement et ceux de la personne concernée[54], sachant que ceux-ci peuvent être contradictoires, les uns rejoignant ceux du responsable, les autres s'en éloignant[55]. Dans le cas du consentement, aucune condition n'est mise, si ce n'est celles des qualités exigées par la définition du consentement dont le Groupe de l'article 29 rappelle, en 2017, la nécessité d'une vérification[56].

---

davantage sur de l'opt-out que sur de l'opt-in. Le consentement n'est donc pas à proprement parler au cœur du dispositif puisque, dans les cas où la personne peut faire usage de son droit de ne pas faire l'objet d'une décision automatisée (en dehors des exceptions de l'article 22 du RGPD dont l'application n'est pas des moindres), la personne concernée utiliserait donc, selon le texte, son droit d'opposition et non sa capacité à consentir.

[51] « Avis 06/14 sur la notion d'intérêt légitime poursuivi par le responsable du traitement au sens de l'article 7 de la directive 95/46/CE », 844/14/FR WP 217, 9 avril 2014.

[52] Groupe de l'article 29, « Guidelines on consent under Regulation 2016/679 », 17/EN WP 259, 28 novembre 2017, en particulier p. 9.

[53] On note qu'en cas de changement de finalités (article 6.4. RGPD), le responsable du traitement devra vérifier certaines conditions pour déterminer si la finalité nouvelle est compatible avec celles pour lesquelles les données ont été dans un premier lieu collectées, SAUF en particulier s'il y a eu consentement.

[54] À cet égard, l'analyse très fine et la procédure en trois étapes proposée par le Groupe de l'article 29 dans son avis 06/2014, déjà cité, pp. 52 et s. : « *To ensure protection from the start, and to avoid that the shifting of the burden of proof is circumvented, it is important that steps are taken before the processing starts, and not only in the course of ex-post "objection" procedures. It is therefore proposed that, in the first stage of any processing activity, the data controller shall take several steps. The two first steps could be listed in a recital of the proposed Regulation and the third one in a specific provision* ».

[55] « *The first ground, Article 7(a), focuses on the consent of the data subject as a ground for legitimacy. The rest of the grounds, in contrast, allow processing – subject to safeguards – in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest* » (avis 06/2014, déjà cité, p. 48).

[56] « *Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them*

En ce qui concerne la distinction entre contrat et consentement, la disposition de l'article 7.4. du RGPD, dont le contenu a déjà été mis en lumière par les avis et opinions précédant l'adoption du RGPD, énonce clairement : « Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat »[57]. Cette disposition interdit ou plutôt présume comme consentement non valable le fait qu'à l'occasion de la signature d'un contrat, on ne réclame, comme condition de l'obtention d'un service, un ou des consentements pour des traitements non nécessaires à l'exécution du contrat. Ainsi, on peut imaginer qu'un opérateur de réseau social n'exige pour le service qu'il offre, la possibilité d'utiliser les données pour profiler la personne concernée, ce qui n'est pas à strictement parler nécessaire à l'exécution du contrat. Sans doute, faut-il voir dans ce prescrit, la conséquence de l'exigence du caractère libre du consentement[58] : la crainte de ne pas voir s'exécuter le contrat rend le consentement non libre[59].

Toujours en ce qui concerne la relation entre consentement et contrat, l'article 7.2. du RGDP distingue le consentement au traitement, du consentement au contrat, du moins dans la forme : « Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions… ». En d'autres termes, le RGPD exige que le ou les consentements relatifs au traitement lorsqu'ils sont nécessaires pour fonder la licéité du traitement soient clairement dissociés du consentement donné aux conditions générales du contrat. Faut-il pour autant voir dans cette disposition une nature non contractuelle du consentement tel que consacré dans le RGPD ? Nous ne le pensons pas.

---

without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful » (Groupe de l'article 29, « Guidelines on consent under Regulation 2016/679 », 17/EN WP 259, 28 novembre 2017, p. 4).

[57] L'avis 06/2014 sur la notion d'intérêt légitime, déjà cité, se réfère à une décision de la Cour de Strasbourg de 1983 pour préciser que l'exigence du caractère « nécessaire », sans équivaloir à « indispensable » « n'a pas la souplesse de termes, tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" » (C. DE TERWANGNE, « Les principes relatifs au traitement de données à caractère personnel et à sa licéité », *op. cit.*, p. 133).

[58] Comme le note le Groupe de l'article 29 dans ses Guidelines déjà citées (p. 17), développant ainsi le considérant n° 43 du GDPR : « *A strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of the service* ». Nous reviendrons sur ce point lors de notre analyse du projet de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, COM(2015) 634 final, 9 décembre 2015 et le Californian Consumer Privacy Act.

[59] Sur ce point, voy. T. LEONARD, « Yves, si tu exploitais tes données ? », *op. cit.*, pp. 664 et s.

12. Au-delà, l'avis de 2011 sur la notion de consentement introduit l'idée d'une subsidiarité du consentement. Ainsi, dans l'exemple développé de l'achat d'une voiture[60], le Groupe de l'article 29 répartit les fondements de licéité des différents traitements suivant leur adéquation la plus conforme aux finalités, réservant au consentement ce qui ne peut être justifié par les autres fondements. En d'autres termes, dans les traitements opérés par les responsables de traitement du secteur privé, on considérera que la licéité du fondement devrait être recherchée d'abord dans les nécessités du contrat à venir ou à exécuter, à défaut dans l'intérêt légitime supérieur du responsable et ce n'est vraiment qu'en dernier lieu, qu'on trouvera dans le consentement la base nécessaire à fonder une base de licéité aux traitements qui n'ont pu la trouver dans les deux autres fondements[61]. Ainsi, le consentement suppose que ni la relation contractuelle ni l'intérêt légitime n'ont pu fonder le traitement en cause. On souligne qu'un tel raisonnement conduit à réserver le consentement à des hypothèses où, *a priori*, il est difficile de justifier le traitement et que, dès lors, on peut comprendre le rappel des exigences de qualité du consentement et déplorer leur absence dans la réalité de nos consentements. Ce point nous amène à une autre critique fondée sur le lien à opérer entre les conditions de licéité de l'article 6 du RGPD et les principes relatifs au traitement de données à caractère personnel énumérés à l'article 5 du même RGPD. Nous l'aborderons au point C.

13. Le Groupe de l'article 29[62] dans ses Guidelines récentes sur le consentement affirme un principe non sans conséquence sur l'enjeu de la distinction entre les différentes bases de licéité : « … *as a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases* »[63]. Ainsi les traitements répondant à une finalité doivent se voir assigner une et une seule base de licéité. Cette assertion poserait, selon Th. Leonard[64], une difficulté au moment où la base

[60] « Example: buying a car
The data controller may be entitled to process personal data according to different purposes and on the basis of different grounds:
– Data necessary to buy the car: Article 7(b),
– To process the car's papers: Article 7(c),
– For client management services (e.g. to have the car serviced in different affiliate companies within the EU) : Article 7(f),
– To transfer the data to third parties for their own marketing activities: Article 7(a) » (« Avis 15/2011 sur la définition du consentement », 01197/11/FR WP187, 13 juillet 2011, p. 7).

[61] Nous aurons l'occasion de montrer dans la seconde partie comment l'EDPS applique ce principe de subsidiarité dans son analyse critique de la proposition de directive relative aux contrats de fourniture à contenu numérique (*infra*, n° 22).

[62] Un récent avis de l'EDPS par contre reprend la première opinion du Groupe de l'article 29 (15/2011) : « Cela n'exclut pas le recours simultané à plusieurs fondements, pour autant qu'il soit utilisé à bon escient » (avis 8/2018 du CEPD sur le paquet législatif, « Une nouvelle donne pour les consommateurs », 5 octobre 2018, p. 17).

[63] « Guidelines on consent under Regulation 2016/679 », 17/EN, WP 259, p. 22.

[64] Selon Leonard (« Yves, si tu exploitais tes données ? », *op. cit.*, p. 663), le Groupe de l'article 29 fait ainsi une interprétation *ultra legem* de l'article 6 et rompt avec l'interprétation donnée jusqu'ici par le même Groupe.

de licéité s'avère déficiente, ainsi en cas de retrait du consentement, dans la mesure où le contrat ou l'intérêt légitime ne pourront servir à fonder le traitement ni en tout ni en partie sauf à recommencer l'ensemble de la procédure qui permettra de fonder alors le traitement sur un autre fondement. Cette critique ne semble pas totalement fondée. Certes, la création d'une base de données peut se justifier au regard de plusieurs finalités : la liste des clients peut se justifier tant par la réalisation du contrat conclu avec eux, que par l'intérêt légitime supérieur du responsable du traitement que par le consentement des clients mais qu'on ne s'y trompe pas, à chacune de ses bases de licéité répondent des traitements différents et les données traitées ne sont pas les mêmes : ainsi, la finalité contractuelle ne nécessite pas, en principe, toutes les données sur lesquelles les systèmes d'intelligence artificielle travailleront pour mieux profiler les services et produits à offrir aux clients. Le retrait du consentement n'affectera donc pas la base de données « clients » mais bien la possibilité de constituer un vaste réservoir de données et d'y appliquer un système d'intelligence artificielle.

3. Le consentement au regard du lien entre les articles 5 et 6 du RGPD

14. Il est entendu que l'article 6 en énonçant les causes de licéité ne dispense pas le responsable de traitement de respecter les principes de l'article 5 relatifs au traitement de données à caractère personnel. Les principes de loyauté des traitements, de légitimité des finalités, d'exactitude des données, ceux de proportionnalité tant des données que de durée des traitements et, enfin, de sécurité doivent s'appliquer. En d'autres termes, si les conditions de licéité constituent une condition nécessaire de la validité des traitements, elles ne sont pas suffisantes et exigent une analyse *in casu* du respect des principes de base de légitimité des traitements. L'article 8 de la Charte européenne et l'article 16 du Traité de Lisbonne prennent soin de réclamer le cumul de l'examen des deux articles, soit le respect à la fois des principes et la vérification des conditions de licéité des traitements : « Ces données doivent être traitées loyalement, à des fins déterminées *et* [nous soulignons] sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ». L'affirmation est également incontestable à la lecture du rapport de la Convention n° 108[65], modifiée récemment qui, à propos de son article 5 qui cumule à la fois les principes et les conditions de licéité, énonce : « Le paragraphe 2 prévoit que la licéité du traitement de données est subordonnée à l'une ou l'autre des deux conditions essentielles que sont le consentement de la personne concernée ou l'existence

[65] Rapport explicatif – STCE 223 – Traitement automatisé des données à caractère personnel (Protocole d'amendement), 10.X.2018, p. 8, nos 41, 42 et 44.

de fondements légitimes prévus par la loi. Les paragraphes 1[66], 2, 3 et 4[67] de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données ». Sans doute, en ce qui concerne les textes dérivés de la Charte et de l'Union européenne, la réponse au départ peu claire dans le cadre de la directive s'affermit progressivement dans les considérants du RGPD et des Guidelines. Sous l'empire de la directive 95/46, seul un passage de l'avis du Groupe de l'article 29 en date de 2011 (soit après l'adoption de la Charte) sur le consentement notait sans le souligner[68] que « *Reliance on consent to process personal data does not relieve the data controller from his obligation to meet the other requirements of the data protection, for example to comply with the principle of proportionnality (article 6.1 (c)), security of the processing ex article 17, etc.)* »[69]. Toujours en référence à cette directive, la Cour de justice de Luxembourg interprétait le lien entre les deux articles, à l'époque les articles 6 et 7 de la directive, comme suit : « tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncés à l'article 6 de ladite directive et, d'autre part, répondre à l'un des six principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette même directive »[70]. Dans le cadre de l'interprétation à donner aux articles 5 et 6 du RGPD, les Guidelines[71] sont plus affirmatives encore que toujours discrètes à propos de la nécessité de la lecture conjointe de ces deux articles : « *Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and fundamentally unfair* ». Sans doute, regrettera-t-on que les Guidelines si prolixes en ce qui concerne les qualités du consentement ne le soient pas également en la matière.

15. En effet, quand peut-on considérer qu'un consentement présentant toutes les qualités requises, ne se substituant à aucune autre cause de licéité puisse être rejeté à

[66] « Le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu ».

[67] Le paragraphe 2 exige un fondement légitime pour traiter les données (article 6 RGPD) et renvoie donc aux conditions de licéité (consentement ou autres bases reconnues par le législateur). Quant aux paragraphes 3 et 4, ils expriment les principes de licéité, loyauté, finalité et de qualité des données également affirmés par l'article 5 du RGPD.

[68] Opinion 15/2011, déjà citée, p. 34.

[69] Même réflexion : « L'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être considérée ».

[70] C.J.U.E., 24 novembre 2011, arrêt *ASNEF et FECEMD c. Administracion del Estado*.

[71] Guidelines, déjà citées, p. 4.

défaut de respecter les principes repris à l'article 5 ? C. de Terwangne[72] l'affirme et son raisonnement sur le plan théorique est correct : « Ainsi, un traitement basé sur le consentement de la personne concernée porte peut-être atteinte de manière disproportionnée à un intérêt collectif qui n'a forcément pas été pris en compte par la personne concernée qui n'a envisagé, comme il se doit, que ses propres droits et intérêts pour donner son consentement. La condition de finalité légitime de l'article 5, § 1er, b), n'est, dans ce cas, pas rencontrée[73] alors même que l'article 6 est respecté. Le traitement de données envisagé doit être déclaré illégal ». Mais dans la réalité, les choses seront moins évidentes. Ainsi, considérera-t-on que le consentement explicitement donné par l'utilisateur à une plateforme musicale en ce qui concerne la possibilité de lui recommander des morceaux sur la base de l'analyse par intelligence artificielle de données telles que son écoute, les lieux, le temps et le volume d'écoute croisées, avec d'autres données par exemple sur les sites visités avant et après l'accès au site de la plateforme est proportionné ou non ? Une réponse négative m'étonnerait dans la mesure où la plateforme pourra exhiber du fait que c'est en pleine conscience que le consentement dûment informé a été donné et que dès lors on peut et doit juger qu'*a priori* les données recueillies ont été jugées proportionnées. Autre exemple : contacté par un assureur – automobile –, je me vois proposer une police à moitié prix, à condition que j'accepte le placement d'un mouchard qui, en temps réel permettra à l'assureur de suivre mes déplacements, de juger de ma conduite au regard des prescrits du Code de la route et les heures de conduite. Mon consentement à cette offre remplit, par hypothèse, les conditions de qualité. Le jugera-t-on non conforme aux principes de légitimité des finalités voire de proportionnalité, en notant que mon acceptation jointe à celles de tant d'autres attirés par la perspective d'une diminution de prime ruine le sacro-saint « dogme » de la mutualisation des risques qui gouverne le système des assurances ? Sans doute, la dérive des assurances dites « *one-to-one* » mériterait une réflexion collective, « politique » au sens noble du terme, mais un juge pourrait-il au nom de ce « dogme » remettre en cause mon consentement, par exemple au nom de la primauté de ma liberté de déplacement ? À tout le moins, on le pressent, le consentement considéré comme l'expression même et suprême de l'autodétermination dans la conception individualiste critiquable, qui est celle du RGPD[74] permet difficilement la remise en cause du consentement par la lecture conjointe

[72] C. de Terwangne, « Les principes relatifs au traitement de données à caractère personnel et à sa licéité », *op. cit.*, p. 118.

[73] En définitive, tout dépend de quel point de vue, le caractère « légitime » du traitement doit s'apprécier ? Le jugera-t-on au regard de l'intérêt collectif ? de l'intérêt personnel ? de la balance à opérer entre les intérêts personnels de la personne concernée et ceux du responsable ? La légitimité s'apprécie, nous semble-t-il, au cas par cas et laisse une marge d'appréciation aux autorités de protection des données qui, en définitive, devront l'apprécier *in concreto*.

[74] Sur ce point, notre ouvrage, *La vie privée à l'épreuve du numérique*, coll. du CRIDS, Larcier, n° 46, 2019.

des articles 5 et 6. En toute hypothèse, dans une telle conception, le consentement crée, au vu de la légitimité supérieure qu'il a, une forte présomption de respect des principes de finalité légitime et de proportionnalité énoncés par l'article 5. Si nous le regrettons, sans doute sera-t-il nécessaire de remettre en cause le « dogme » du consentement, au profit d'une réflexion plus collective sur les enjeux des traitements des données et de la possibilité de juger de leur légitimité à l'aune de cette réflexion. C'est le propos de la seconde partie.

16. Quelques réflexions concluent cette première partie :

a. le consentement consacré depuis peu par les législations de protection des données constitue à la fois la condition de licéité la plus conforme au principe d'autodétermination informationnelle mais également la plus subsidiaire dans la mesure où il est convenu de ne s'y référer que dans les cas où aucune autre condition de licéité n'est susceptible d'être retenue, c'est-à-dire dans les cas où le ou les traitements en cause ne trouve(nt) pas facilement de justification à leur légitimité ;

b. le consentement est une condition nécessaire mais non suffisante de la légitimité du traitement, dans la mesure où les principes applicables à tout traitement doivent être respectés. L'examen de ces principes a fait l'objet d'un examen insuffisant mais devrait conduire à une réflexion plus collective à propos de la légitimité des traitements fondés sur le consentement soit qu'ils enfreignent la règle de proportionnalité, soit la règle du juste équilibre, soit et surtout qu'ils constituent un préjudice pour d'autres personnes concernées ou susceptibles d'être concernées. En d'autres termes, au jugement purement individuel de légitimité que traduit le consentement doit pouvoir s'opposer la volonté de préserver des intérêts sociaux et collectifs ;

c. les conditions sévères mises à la reconnaissance du consentement peuvent s'expliquer par le caractère subsidiaire du consentement comme fondement de licéité. Cependant, elles sont à ce point exigeantes que leur rencontre dans la pratique vécue dans le contexte des opérations courantes de l'internet les rend illusoires ;

d. la nature contractuelle du consentement devrait être reconnue. L'approche contractuelle répond mieux à la réalité des opérations effectuées sur la toile. Outre que la nature d'acte juridique unilatéral ne correspond pas à la réalité de la plupart des consentements noués avec le fournisseur du service par l'interactivité du réseau, le caractère contractuel du consentement ne nuit pas aux dispositions certes exorbitantes du droit commun du RGPD et liées au consentement. La pratique des consentements multiples et dissociés de même que la possibilité de rétractation ont été largement consacrées par le droit de la consommation aux fins de protection de la partie faible. Par identité de motifs, ces dispositions

impératives sont pleinement justifiées par la protection des libertés des personnes concernées et s'imposent nonobstant toute clause contraire[75] ;

e. au bénéfice de ces dernières, on relève en outre que l'analyse contractuelle fait entrer la « *Privacy Policy* » dans le champ contractuel et permet à la personne concernée de bénéficier des protections accordées au consommateur lorsqu'à la qualité de « personne concernée », l'internaute ajoute celle de « consommateur ». Cette dernière remarque introduit les réflexions de la seconde partie.

II. Consentement et fourniture de données

17. Deux textes récemment apparus abordent la question délicate de la règlementation des nombreux contrats conclus sur le web par lequel un service numérique est offert et dont l'objet nécessite la collecte d'informations à caractère personnel. Le premier est américain, californien pour être précis. Il s'agit du California Consumer Privacy Act[76] dont les similarités avec le texte du RGPD doivent être soulignées[77]. Le second est européen : il s'agit d'une proposition de directive élaborée dans le cadre d'une politique européenne fixant « Une nouvelle donne pour les consommateurs »[78]

---

[75] Le législateur californien est clair à ce propos : « *1798.175 – This title is intended to further the constitutional right of privacy… The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control. 1798.180-This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business* » (*Consumer Privacy Act – An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy*, Assembly Bill No. 375).

[76] *Consumer Privacy Act – An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy*, Assembly Bill No. 375, approuvé par le « Governor » de l'État de Californie, le 28 juin 2018.

[77] Future of Privacy Forum, *Comparing Privacy Laws: GDPR vs CCPA*, juin 2018, disponible à l'adresse : http://www.dataguidance.com. « *The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA") (SB-1121 as amended at the time of this publication) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data, whether the information was obtained online or offline. The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered to be one of the most significant legislative privacy developments in the country. Like the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy. The CCPA will take effect on 1 january 2020, but certain provisions under the CCPA require organizations to provide consumers with information regarding the preceding 12-month period, and therefore activities to comply with the CCPA may well be necessary sooner than the effective date* ».

[78] C'est le titre de la communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen intitulée « Une nouvelle donne pour les consommateurs », COM(2018) 183 final.

et modifiant trois directives en matière de protection des consommateurs[79]. Notre propos n'est pas de les analyser en détail mais simplement de montrer comment ces textes permettent de compléter les réflexions tenues jusqu'ici sur le consentement, en sachant que le domaine des services couverts par les deux réglementations concerne les hypothèses majeures où le consentement est délivré par les personnes concernées. Ces deux textes militent pour un changement d'approche de la protection des données que l'on peut énoncer comme suit. Premièrement, ils reconnaissent que l'économie de contrats soi-disant gratuits repose en fait sur l'avantage tiré par les entreprises qui offrent des services numériques tirent des données qu'elles collectent et exploitent[80]. Secondement, elles démontrent que le but de la protection des données est atteint également par des dispositions de protection des consommateurs et plaident dès lors pour une alliance entre protection des consommateurs et protection de la vie privée. Nous analyserons ensuite en quoi et *in fine*, aborderons l'intérêt de l'approche contractuelle consumériste retenue par ces deux textes, certes perfectibles sur le plan de la protection des données à caractère personnel mais qui annoncent d'autres avancées en matière de protection des données.

18. Les deux textes évoqués encadrent ce que la proposition de directive européenne « une nouvelle donne pour les consommateurs » qualifie, d'une part, de « contrats de fourniture de contenu numérique *non fourni sur un support matériel* »[81], soit « tout contrat en vertu duquel un professionnel fournit ou s'engage à fournir un contenu

[79] Proposition de directive du Parlement européen et du Conseil modifiant la directive 93/13/CEE du Conseil du 5 avril 1993, la directive 98/6/CE du Parlement européen et du Conseil, la directive 2005/29/CE du Parlement européen et du Conseil et la directive 2011/83/UE du Parlement européen et du Conseil concernant une meilleure application et une modernisation des règles de protection des consommateurs de l'UE, COM(2018) 185 final.

[80] « La proposition étend l'application de la directive 2011/83/UE aux services numériques pour lesquels les consommateurs ne versent pas d'argent mais fournissent des données à caractère personnel, telles que : stockage dans le nuage, réseaux sociaux et comptes de messagerie électronique. Compte tenu de la valeur économique croissante des données à caractère personnel, ces services ne peuvent pas être considérés comme simplement "gratuits". Les consommateurs devraient donc avoir le même droit aux informations précontractuelles et d'annulation de contrat dans un délai de rétractation de quatorze jours, indépendamment du fait qu'ils paient pour le service avec de l'argent ou en fournissant des données personnelles » (proposition de directive modifiant la directive 93/13/CEE du Conseil du 5 avril 1993, la directive 98/6/CE du Parlement européen et du Conseil, la directive 2005/29/CE du Parlement européen et du Conseil et la directive 2011/83/UE du Parlement européen et du Conseil concernant une meilleure application et une modernisation des règles de protection des consommateurs de l'UE, Bruxelles, 11 avril 2018, COM(2018)185 final, p. 2).

[81] La même directive parle également de contrat de service numérique et le définit comme suit (article 2, 17 et 18) : « *contrat de service numérique* » comme étant « tout contrat en vertu duquel le professionnel fournit ou s'engage à fournir un service numérique au consommateur et le consommateur paie ou s'engage à payer le prix de celui-ci. Sont également inclus les contrats en vertu desquels le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf si les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel afin de fournir le service numérique ou de lui permettre de respecter les exigences légales qui lui incombent, pour autant qu'il ne traite pas ces données à une autre fin ».

numérique spécifique au consommateur, et le consommateur paie ou s'engage à payer le prix de celui-ci. Sont également inclus les contrats en vertu desquels le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel »[82] et, d'autre part, de contrats de service numérique, à savoir, « tout contrat en vertu duquel le professionnel fournit ou s'engage à fournir un service numérique au consommateur et le consommateur paie ou s'engage à payer le prix de celui-ci. Sont également inclus les contrats en vertu desquels le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel ».

19. Les deux notions sont larges. Elles visent tous les contrats par lesquels un prestataire de services soit offre via Internet des contenus produits et diffusés sous forme numérique (vidéo, jeux, musique), soit permet la création, le traitement et le stockage de données sous une forme numérique, données fournies par l'utilisateur du service (essentiellement les services du cloud), soit, enfin, autorise le partage ou toute autre forme d'interaction de données sous forme numérique en provenance d'autres utilisateurs du service (en particulier les services de réseaux sociaux)[83]. En ce qui concerne la « contrepartie » exigée de l'utilisateur des contrats visés, la proposition souligne que cette contrepartie n'est pas nécessairement une contrepartie en monnaie mais peut, nouveauté de la proposition de directive, également consister en la fourniture de données à caractère personnel. Les considérants de la proposition s'en expliquent comme suit : « Par conséquent, cette directive (celle 2011/83/UE) ne s'applique pas aux contrats de services numériques dans le cadre desquels le consommateur four-

[82] Il est à souligner que la directive exclut précisément de son champ d'application, les contrats où le prestataire ne collecte les données que pour les seuls besoins de la fourniture du service et des obligations légales liées à cette fourniture, ainsi les obligations comptables et fiscales. Cette exclusion rappelle en son premier point (besoins de la fourniture du service) le libellé utilisé par l'article 6.1.b) du RGPD en ce qui concerne le fondement contractuel des traitements. Par ailleurs, sont également inclus dans la définition ci-dessus « les contrats en vertu desquels le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf si les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel afin de fournir le contenu numérique ou de lui permettre de respecter les exigences légales qui lui incombent, pour autant qu'il ne traite pas ces données à une autre fin ».

[83] L'article 2 de la proposition de directive définit en effet très largement la notion de « contenu numérique » : « (a) les données produites et fournies sous forme numérique, par exemple des vidéos, enregistrements audio, applications, jeux numériques et autres logiciels, (b) tout service permettant la création, le traitement ou la conservation de données sous forme numérique, lorsque ces données sont fournies par le consommateur, et (c) tout service permettant le partage de données sous forme numérique fournies par d'autres utilisateurs de ce service ou permettant toute autre interaction avec ces données ; ». Sur ces deux notions et l'incertitude qui régnait dans la première proposition de directive en ce qui concerne l'application du texte de la proposition aux plateformes et fournisseurs d'accès internet, voy. J. Rochfeld, « Le "contrat de fourniture de contenus numériques" : la reconnaissance de l'économie spécifique "contenu contre données" », *Dalloz IP/IT*, janvier 2017, p. 16. *Cf.* également, H. Jacquemin, « Digital Content and Sales or Services Contracts under the EU Law and Belgian/French Law », *JPITEC*, 9 (2017), p. 27 et J. Senechal, « La notion de fournisseur de contenu numérique : quel rôle pour les plateformes en ligne », *Dalloz JP/IT*, janvier 2017, p. 22.

nit des données à caractère personnel au professionnel sans contrepartie pécuniaire. Compte tenu de leurs similitudes et de l'interchangeabilité des services numériques payants et des services numériques fournis en échange de données à caractère personnel, ils devraient être soumis aux mêmes règles au titre de la directive 2011/83/UE. Par conséquent, le champ d'application de la directive 2011/83/UE devrait être étendu aux contrats dans lesquels le professionnel fournit ou s'engage à fournir un service numérique au consommateur et dans lesquels le consommateur fournit ou s'engage à fournir des données à caractère personnel. À l'instar des contrats de fourniture de contenu numérique non fourni sur un support matériel, la directive devrait s'appliquer chaque fois que le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel ». La même réflexion préside à l'approche californienne : « *Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories* »[84]. On note que le texte californien ne distingue pas, comme le fait la définition européenne proposée, les services numériques gratuits ou non dans la mesure où le caractère « payant » des services numériques, même ceux apparemment gratuits, est évident. Par contre, le texte autorise l'opérateur d'un service à réclamer un prix « juste » au cas où le consommateur refuserait le transfert de données à caractère personnel et à l'inverse, le consommateur, personne concernée à réclamer une diminution de prix ou autre « juste » compensation en cas de vente de données à des tiers[85]. Sans doute, la volonté des auteurs européens était de bien faire et d'éviter toute mauvaise interprétation d'un texte qui aurait pu conduire à ne pas soumettre les services soi-disant de la toile au régime juridique de protection des consommateurs[86] ; mais était-ce bien nécessaire ?

---

[84] Assembly Bill No. 375) : « *An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy* ».

[85] Il est en effet intéressant de noter l'approche consumériste de la loi fondée sur la valeur marchande de la donnée et dont le « consommateur » peut réclamer un juste prix voire se faire offrir une compensation : « *The bill would grant a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed. The bill would require a business to provide this information in response to a verifiable consumer request. The bill would authorize a consumer to opt out of the sale of personal information by a business and would prohibit the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data. The bill would authorize businesses to offer financial incentives for collection of personal information…* » (Assembly Bill No. 375 : « *An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy* », Preamble).

[86] Comme le note R. Robert (« Peut-on payer avec ses données personnelles ? La proposition de directive "contenu numérique" introduit le ver dans le fruit », *J.D.E.*, 2017, p. 356) : « On peut se féliciter de

20. Il y a longtemps que le droit prend en compte non l'apparence mais la réalité des transactions sur Internet[87]. Ainsi, « les services de la société de l'information visés par la directive "Commerce électronique" ne se limitent pas exclusivement aux services donnant lieu (formellement) à la conclusion de contrats en ligne, mais, dans la mesure où ils représentent une activité économique, ils s'étendent à des services *qui ne sont pas rémunérés par ceux qui les reçoivent*, tels que les services qui fournissent des informations en ligne ou des communications commerciales, ou ceux qui fournissent des outils permettant la recherche, l'accès et la récupération des données ». La justice et les autorités de protection des consommateurs, souligne J. Rochfeld[88], ne se laissent plus duper par l'affirmation des opérateurs des services numériques selon laquelle la gratuité de leurs services les met hors-jeu des législations de protection des consommateurs.

Cette justification ne satisfait pas entièrement[89] les autorités de protection des données, en particulier le CEPD qui, dans ses avis répétés à propos des deux versions[90] de la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, résume comme suit ses craintes : « Le CEPD craint que l'introduction par la proposition de la notion de "contrats de fourniture de contenu numérique ou de service numérique pour lesquels les consommateurs doivent fournir des données à caractère personnel au lieu de payer une somme d'argent" puisse être

---

l'intention du législateur qui était d'étendre la protection de la proposition de directive aux contenus pour lesquels la contrepartie ne serait pas de l'argent ».

87 « Dans l'économie numérique, les acteurs du marché ont souvent et de plus en plus tendance à considérer les informations concernant les particuliers comme ayant une valeur comparable à celle de l'argent. Il est fréquent que du contenu numérique soit fourni, non pas en échange d'un paiement, mais moyennant une contrepartie non pécuniaire, c'est-à-dire en accordant l'accès à des données à caractère personnel ou autres. Ces modèles commerciaux spécifiques sont appliqués sous de multiples formes sur une grande partie du marché. Établir une distinction en fonction de la nature de la contrepartie serait discriminatoire pour certains modèles commerciaux. Cela inciterait inutilement les entreprises à s'orienter vers une offre de contenu numérique en contrepartie de données » (proposition de directive, considérant n° 13).

88 J. Rochfeld, « Le "contrat de fourniture de contenus numériques" : la reconnaissance de l'économie spécifique "contenu contre données" », *op. cit.*, p. 19. L'auteure se réfère à la recommandation de la Commission des clauses abusives (n° 2014/02) et une décision de la cour d'appel de Paris du 12 février 2016 dans une affaire *Facebook* (*D.*, 2016, p. 422).

89 Le CEPD souligne le côté positif de la proposition qui refuse toute différenciation entre services payants et services dits gratuits : « Cette différenciation semble injuste, compte tenu de la valeur économique tirée des consommateurs sur les marchés numériques ».

90 La proposition de directive du Parlement européen et du Conseil déjà citée modifiant la directive 93/13/CEE du Conseil du 5 avril 1993, la directive 98/6/CE du Parlement européen et du Conseil, la directive 2005/29/CE du Parlement européen et du Conseil et la directive 2011/83/UE du Parlement européen et du Conseil concernant une meilleure application et une modernisation des règles de protection des consommateurs de l'UE, COM(2018) 185 final avait été précédée d'une première proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, COM(2015)634 final – 2015/0287 (COD) qui avait fait d'un premier avis du CEPD (« Avis 04/2017 du CEPD sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique », 14 mars 2017).

source de confusion pour les prestataires de services, qui seraient amenés à penser que le traitement de données fondé sur le consentement dans le cadre d'un contrat est conforme à la législation dans tous les cas, même lorsque les conditions de validité du consentement définies dans le RGPD ne sont pas remplies. Cela porterait préjudice à la sécurité juridique »[91]. En conclusion, « le CEPD estime qu'il convient de modifier les définitions proposées du "contrat de fourniture de contenu numérique non fourni sur un support matériel" et du "contrat de service numérique" afin d'éviter une comparaison explicite ou implicite entre la fourniture de données à caractère personnel et le paiement d'une somme d'argent. Une telle comparaison pourrait en particulier permettre de contourner le RGPD en introduisant potentiellement une interprétation large du "traitement nécessaire à l'exécution du contrat", qui est l'un des fondements juridiques du traitement des données à caractère personnel visés à l'article 6, paragraphe 1, point b), du RGPD ». À y regarder de près, l'objection du CEPD est donc double[92] : la première, fondamentale, rejette toute idée de paiement par fourniture de données à caractère personnel et rejette l'utilisation du terme « contrepartie » dans un contrat qui dès lors serait un contrat synallagmatique parfait ; la seconde a trait au brouillage des causes de licéité des traitements à laquelle la proposition de directive contribue et en ce sens le rappel net de la distinction entre contrat et consentement.

21. La première objection nous apparaît mériter les réflexions suivantes. Si la vie privée en tant que liberté est hors commerce et ne peut être objet de transactions, il est difficile de soutenir que chaque donnée à caractère personnel, en tant qu'élément de notre vie privée est indisponible. F. Rigaux, auteur majeur en matière de vie privée[93], écrit très justement : « L'indisponibilité a pour objet qui n'intéresse aucun contractant : il est assurément illicite de disposer pour l'avenir de la totalité d'un attribut déterminé de la personnalité, de renoncer à l'exercice de la liberté d'expression, d'aliéner "le droit à la propre image" ou de conférer à un cocontractant une appropriation illimitée des faits à venir de la vie privée, non de consentir à l'exploitation

[91] Avis 8/2018, déjà cité, p. 18, n° 52 ; même remarque in avis 04/2017, déjà cité, p. 9.

[92] D'autres objections pourraient être adressées, ainsi pourquoi la proposition de directive se focalise sur les données *fournies* par le consommateur. Or la plupart des données collectées par les prestataires de services ne sont pas au sens propre fournies par le consommateur mais sont générées par le fonctionnement de multiples techniques (*cookie*s, lecteurs de *tags RFID*, *spywares*…) mises en place par ce prestataire dans les terminaux du consommateur « À l'instar des contrats de fourniture de contenu numérique non fourni sur un support matériel, la directive devrait s'appliquer chaque fois que le consommateur *fournit ou s'engage à fournir* des données à caractère personnel au professionnel » (considérant n° 24 de la proposition de directive COM(2018) 185). La présente directive ne devrait pas s'appliquer aux cas où le fournisseur recueille des informations, y compris des données à caractère personnel, comme l'adresse IP, ou d'autres informations générées automatiquement, comme les informations recueillies et transmises par un cookie, sans que le consommateur ne les ait fournies activement, même si le consommateur accepte le cookie.

[93] F. Rigaux, *La vie privée, une liberté parmi les autres*, Bruxelles, Larcier, 1992, p. 155.

par autrui de biens particuliers actuellement disponibles ». Th. Leonard[94] surenchérit : « l'exemple du droit à l'image et de l'exploitation qu'en font certaines personnes connues ou inconnues est en effet incontestable. Toute une industrie se fonde sur l'exploitation de photographies, révélant le cas échéant des éléments intimes de leur vie privée au grand public, sur internet ou d'autres médias, contre rémunération parfois très élevée. La validité de telles conventions, et partant du consentement de la personne concernée qui en est la base, ne peut être remise en cause par le fait que l'octroi d'une rémunération conditionne le consentement ». Tout récemment, dans une affaire concernant la participation à une loterie d'un internaute où ce dernier devait accepter de pouvoir être contacté par d'autres entreprises, l'avocat général de la C.J.U.E.[95] émettait l'opinion que dans la mesure où la finalité de l'activité de loterie proposée était indiscutablement la vente à des tiers, des données relatives aux participants, la fourniture de données était indiscutablement « l'obligation principale mise à la participation à la loterie ».

22. Cette possibilité de contractualisation des données à caractère personnel existe bien mais elle ne signifie pas la contractualisation « à tout prix », ni surtout que nos données dites à caractère personnel seraient notre propriété, propriété que nous serions libres de mettre en commerce librement[96]. Comment peut-on parler de propriété à propos de données à caractère personnel ? Au-delà de l'argument avancé par les auteurs contre une telle propriété, à savoir l'impossibilité pour le consommateur, personne concernée[97], de déterminer la valeur patrimoniale de « son bien », on opposera à l'approche propriété les arguments suivants[98]. Le premier est simplement de rappeler que le droit de la propriété protège des biens matériels et que le droit de la propriété intellectuelle ne peut s'entendre que de données, résultant d'une création intellectuelle originale, même si des exceptions ont été consenties via des protections « *sui generis* » comme le régime des bases de données ou tout récemment le secret

[94] T. Leonard, « Yves, si tu exploitais tes données ? », *op. cit.*, p. 670 ; de manière plus nuancée, R. Robert, « Peut-on payer avec ses données personnelles ? La proposition de directive "contenu numérique" introduit le ver dans le fruit », *op. cit.*, p. 357.

[95] Opinion de l'avocat général Szupnar, 21 mars 2019, C-673/17, *Planet 49 GmbH vs. Bundesverband der Verbraucherzentralen und Verbraucherverbânde*, en particulier les n^os 97 et s.

[96] Dans le même sens, A. Pierucci, « Le rôle du consentement de la personne concernée dans le marketing électronique », *Ubiquité*, 2001, pp. 15 et s. L'auteure compare le rôle et la légitimité du consentement dans le modèle fondé sur le droit de la propriété et dans le modèle fondé sur le droit de la personne pour conclure au rejet du premier modèle qui n'accorde qu'une protection illusoire à la personne concernée.

[97] Voire également du responsable du traitement dans la mesure où dans le cadre de *big data*, toutes les données collectées ne seront pas nécessairement jugées utiles dans le cadre du fonctionnement des algorithmes utilisés et du fait qu'il peut difficilement au moment de la collecte des données connaître toutes les opportunités d'exploitation des données qui lui seront offertes.

[98] Sur ces objections, voy. nos remarques sur le débat, « Propriété vs Libertés », in *La vie privée à l'heure du numérique – Essai*, coll. du CRIDS, n° 46, Larcier, 2019, à paraître, n^os 63 et s.

d'affaires[99]. Le deuxième constate que les données nous concernant sont loin d'être nos « produits »[100] : certaines sont partagées avec d'autres[101], d'autres proviennent de notre interaction avec des tiers, d'autres, enfin, même si elles nous concernent, nous sont largement inconnues et si connues, incompréhensibles. Comment dès lors parler de propriétés de données dans de tels cas ? Le troisième argument met en évidence le risque d'une telle reconnaissance. Si le droit reconnaît à la personne concernée la maîtrise de « mes » données, il doit lui être loisible de pouvoir les « vendre », les « louer » ou en céder le droit d'usage, c'est l'essence même de la reconnaissance du droit de propriété qu'il soit intellectuel ou non[102]. Il y a donc une contradiction à affirmer la « propriété » des données à caractère personnel au moment même où le principe même de cette reconnaissance serait d'en limiter l'aliénabilité et ce pour protéger la personne qualifiée de « propriétaire ». Le quatrième argument est développé par D. Solove[103] lui-même, pourtant défenseur faute de mieux du droit de propriété. Il note en effet que cette reconnaissance ne résout pas le problème de la dissymétrie de pouvoir informationnel entre la personne concernée et le responsable : « *The power inequalities that pervade the world of information tranfers* ». En d'autres termes, la possibilité de négociation offerte par la reconnaissance d'un droit de propriété renvoie au jugement de la seule personne concernée quant à sa « commercialisation ». C'est à elle que reviendrait le soin de décider de l'exploitation ou non de ses données ; sa volonté risque d'être exploitée par des « vendeurs », souhaitant « rentabiliser » leurs données et par des « acheteurs », capables de surenchères pour capter des clients ou des marchés[104]. La « vie privée » deviendrait ainsi un privilège de nantis.

23. La contractualisation de nos données s'opère donc non sur la base d'un transfert de propriété mais comme la conséquence de la reconnaissance d'un droit d'accès à

[99] Sur les limites de l'approche « Propriété » des biens immatériels, voy. T. Espeel, *Building Competitive Markets for Digital Data – The Interface between Data Ownership and Access to Data*, mémoire DTIC, Namur, 2018 (à paraître).

[100] Outre que les données collectées sont souvent triviales (par exemple, la géolocalisation, la durée d'écoute, l'intensité de volume d'écoute, etc.) et ne prennent « sens » que dans le cadre des algorithmes du responsable de traitement, on ajoute que la catégorie de données à caractère personnel contient les métadonnées qui permettent le croisement de données (les « *Tags RFID* », les *cooki*es, les numéros IP…) et qui sont attribuées par le responsable. Ces données ne peuvent être qualifiées « mes » données.

[101] À l'intérieur des *big data*, sont prises en considération non mes données individuelles mais bien les résultats de multiples combinaisons de critères qui concernent des données personnelles ou non venant de nombreuses sources et concernant de multiples personnes. C'est ce résultat qui à un moment donné, déterminera mon profil.

[102] J. Litman, « Information Privacy/Information Property », *Stanford Law Review*, 2000, n° 52, 1283.

[103] D. Solove, « Privacy and Power, Computer Data Bases and Metaphors for Information Privacy », *Stanford Law Review*, 2001, n° 53, p. 1452.

[104] Comme le note l'avis du CEPD (avis 08/2018, p. 17), « Il a été signalé que de nombreux prestataires de services numériques déploient des "stratégies de conception" ou des "*dark patterns*" (des interfaces conçues pour que les utilisateurs fassent des choix sans en être conscients) aux nouvelles conditions contractuelles ».

un ou plusieurs services mis à notre disposition par le fournisseur de celui ou ceux-ci et à partir desquels ce dernier pourra trouver profit auprès de tiers par la publicité ou la cession de listes de cibles potentielles qui permettront le développement des activités commerciales ou non de ces tiers[105]. Le contrat, bien évidemment, est soumis, comme nous l'avons souligné en première partie, aux règles impératives que le droit de la protection des données à caractère personnel impose au nom de la protection de nos libertés et dignité[106]. Les données ne sont pas des biens et en tout cas ne peuvent être construites sur la base des mêmes concepts que ceux des biens c'est-à-dire en termes de droits réels ou de propriété intellectuelle. La protection des données s'origine dans les droits de la personnalité dans la mesure où leur exploitation peut aboutir à porter atteinte à des libertés et valeurs fondamentales, parmi lesquelles figure la dignité de l'homme. Ce n'est pas en termes de propriété qu'il faut réfléchir mais plutôt en termes de droits de la personnalité. Ainsi, un consentement distinct de celui global est nécessaire pour parfaire le contrat, le droit au retrait du consentement s'impose et avec le CEPD, nous rappelons que le RGPD confère un certain nombre de droits concernant le traitement des données à caractère personnel (droit d'être informé, droit d'accès, droit à l'effacement, droit à la portabilité des données).

24. À ces droits, s'en ajoutent d'autres, liés cette fois à la protection du consommateur, celles des législations de protection des consommateurs, mais également celles spécifiques proposées pour les contrats de service numérique ou de fourniture de contenu numérique. Au rang des premières, on épingle en particulier la prohibition des clauses abusives ou des manœuvres déloyales, comme la manipulation des classements dans la présentation des résultats lors de recherche sur les moteurs de recherche[107] ; au rang

[105] Ainsi dans l'affaire *Unabhängige Landeszentrum für Datenschutz Schlewzig-Holstein c. Wirtschafstakademie Schleswig-Holstein Gmbh*, C.J.U.E., 5 juin 2018, aff. C-210/16. En l'occurrence et selon les conclusions de l'avocat général Y. Bot, il a été constaté que « Facebook Inc. a mis au point le modèle économique conduisant à ce que la collecte des données lors de la consultation de pages fan, puis l'exploitation de ces données puissent permettre, d'une part, la diffusion de publicités personnalisées et, d'autre part, l'établissement de statistiques d'audience à destination des administrateurs de ces pages ».

[106] En particulier, les principes de loyauté, de finalité légitime et de proportionnalité.

[107] À cet égard, voy. l'explication détaillée de l'article 1er de la proposition de directive COM(2018) 185, modifiant la directive 93/13/CEE du Conseil du 5 avril 1993, la directive 98/6/CE du Parlement européen et du Conseil, la directive 2005/29/CE du Parlement européen et du Conseil et la directive 2011/83/UE du Parlement européen et du Conseil concernant une meilleure application et une modernisation des règles de protection des consommateurs de l'UE. « En ce qui concerne la publicité cachée, les consommateurs qui utilisent des applications numériques comme des places de marché en ligne, des outils de comparaison, des boutiques d'applications ou des moteurs de recherche attendent des résultats de recherche "naturels" ou "organiques" fondés sur la pertinence de leurs recherches et sur des paiements par des tiers. Cependant, comme le soulignent également les orientations de 2016 sur la directive 2005/29/CE, les résultats de recherche contiennent souvent des "placements payants" (lorsque des tiers paient pour bénéficier d'un meilleur classement) ou des "inclusions payantes" lorsque des tiers paient pour apparaître dans la liste des résultats de recherche. Les placements payants et les inclusions payantes ne sont souvent pas indiqués du tout, ou ils ne sont indiqués que d'une manière ambiguë et pas clairement visible pour les consommateurs. Les dispositions pertinentes de la directive 2005/29/CE sur l'interdiction de la publicité

des secondes[108], le droit de rétractation[109-110] ou en droit californien[111], le droit d'exiger la suppression de toutes les données collectées à son propos[112] et de s'opposer à la vente de données à des tiers : « *Do not sell my Personal Information* ». Mais là ne s'arrête pas l'intérêt de l'entrée du droit de la protection des consommateurs dans les considérations des « *privacy advocates* », comme il sera montré au terme de nos réflexions sur la seconde objection du CEPD que nous abordons maintenant.

25. Le RGPD[113] s'inquiète des confusions que la proposition de directive introduit entre les conditions de licéité. La constatation que le projet de directive fasse référence à l'existence d'un contrat entre le prestataire et le « consommateur » n'exclut pas qu'au regard du RGPD, le traitement exigera l'existence d'un consentement

---

cachée devraient donc être clarifiées afin de préciser qu'elles s'appliquent non seulement au contenu éditorial des médias mais aussi aux résultats de recherche en réponse aux requêtes en ligne du consommateur ». À propos de ces manœuvres déloyales, la proposition de directive ouvre le droit du consommateur à réparation contractuelle et extracontractuelle et à des actions contre la pratique des entreprises en cause.

[108] Ainsi, l'accès aux recours collectifs, comme le reconnaît l'avis 08/2018 du CEPD : « Le CEPD accueille favorablement la nouvelle proposition relative aux recours collectifs abrogeant la directive 2009/22/CE57, qui est destinée à faciliter les recours pour les consommateurs victimes de la même infraction dans une situation dite de préjudice de masse. L'article 2, paragraphe 1, de cette proposition dispose que « [l]a présente directive s'applique aux actions représentatives intentées contre les infractions commises par des professionnels aux dispositions du droit de l'Union énumérées à l'annexe I qui portent atteinte ou sont susceptibles de porter atteinte aux intérêts collectifs des consommateurs […] ».

[109] « Les contenus numériques et les services numériques sont souvent fournis en ligne dans le cadre de contrats en vertu desquels le consommateur ne paie pas de contrepartie pécuniaire, mais fournit des données à caractère personnel au professionnel. Les services numériques se caractérisent par une implication continue du professionnel pendant toute la durée du contrat pour permettre au consommateur d'utiliser le service, par exemple la création, le traitement, le stockage et le partage de données sous forme numérique ou l'accès à celles-ci. Des contrats d'abonnement à des plateformes de contenus, des services de stockage dans le nuage, des messageries web, des réseaux sociaux et des applications dans le nuage sont autant d'exemples de services numériques. L'implication continue du prestataire de services justifie l'application des règles sur le droit de rétractation prévues dans la directive 2011/83/UE qui permettent effectivement au consommateur de tester le service et de décider, pendant une période de 14 jours à compter de la conclusion du contrat, de le conserver ou non » (proposition de directive COM(2018) 185, considérant n° 21).

[110] Ce droit de rétractation ne se confond pas avec le droit de la personne concernée au retrait du consentement, comme le rappelle le CEPD : « L'article 7, paragraphe 3, du RGPD dispose que le responsable du traitement doit veiller à ce qu'il soit à tout moment aussi simple pour la personne concernée de retirer que de donner son consentement. Par conséquent, le CEPD tient à souligner que l'introduction par la proposition d'un délai de quatorze jours pour se rétracter du contrat ne peut pas être considérée comme une limitation du droit au retrait du consentement à tout moment prévu dans le RGPD. Dès lors, le CEPD ne voit pas très bien comment le délai de quatorze jours pour se rétracter d'un contrat à distance ou d'un contrat hors établissement envisagé dans la proposition interagirait avec le droit de retirer son consentement au traitement de données à caractère personnel en vertu du RGPD » (avis 08/2018, n° 53, p. 18).

[111] CCPA, section 1798, 120 et 135.

[112] CCPA, section 1798.105 : « *(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer* ». À noter que ce droit va au-delà des droits reconnus par le RGPD en cas de retrait de consentement, qui permet au responsable du traitement de continuer le traitement des données obtenues et traitées avant ce retrait.

[113] Avis 08/2018, p. 17 mais surtout l'avis 04/2017, p. 13.

au sens et aux conditions fixées par le RGPD. À cet égard, le CEPD rappelle l'article 7.4., qui émet (voy. *supra*, n° 11) des doutes sur la validité des contrats qui établissent un lien entre le consentement de la personne concernée et la fourniture d'un service et souligne la nécessité de distinguer les champs d'application des trois conditions de licéité : le consentement de la personne concernée [article 6, paragraphe 1, point a)], l'intérêt légitime du responsable du traitement [article 6, paragraphe 1, point f)], le respect d'une obligation légale (par exemple, le respect d'obligations de conformité ou de conservation des données) [article 6, paragraphe 1, point c)], ou l'exécution du contrat interprétée de manière stricte [article 6, paragraphe 1, point b)]. Si cette distinction doit être maintenue et que dans les cas où ni les nécessités du contrat ni l'intérêt légitime supérieur ne peuvent être invoquées, un consentement qui, comme nous l'avons vu, n'est pas en dehors du contrat mais est spécifique et s'ajoute à celui global, son application n'a rien d'évident.

26. En effet, « ce qui est (strictement) nécessaire à l'exécution du contrat » peut être variable[114]. Prenons l'exemple d'une plateforme de musique en ligne, quel est le service qu'elle vous offre : fournir de la musique à votre demande, certes et, dans ce cas, les données qu'elle sera en mesure de traiter aux fins de l'exécution des contrats, seront limitées mais sans doute, elle vous proposera bien plus : vous proposer des musiques en accord avec les besoins que votre « profil » laisse deviner voire vous distiller la publicité pour des événements qui devraient vous intéresser, vous proposer des services complémentaires voire, pour ce faire, vous mettre en contact avec des tiers « choisis », ce qui implique la vente de vos données. Est alors justifiée une collecte bien plus large et d'autant plus large qu'elle justifie alors l'utilisation de systèmes d'intelligence artificielle aux fins de profiler les consommateurs. Or, on le sait, ces systèmes d'intelligence artificielle travaillent sur un nombre de données dont la pertinence n'est pas définie à l'avance au mépris du principe de proportionnalité (article 5.1.(c) du RGPD) et posent des questions de transparence quant à la logique suivie (article 13.2.(f))[115]. Si telle est la dimension du contrat, on voit mal en quoi l'article 7.4 constituerait une objection à fonder les multiples traitements du presta-

[114] On ajoutera que la proposition de directive s'applique aux contrats de fourniture de contenu numérique et aux contrats de service numérique « sauf si les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel afin de fournir le contenu numérique ou de lui permettre de respecter les exigences légales qui lui incombent, pour autant qu'il ne traite pas ces données à une autre fin », c'est-à-dire dans les cas où le fournisseur recueille les données requises pour que le contenu numérique fonctionne conformément au contrat, par exemple la localisation si elle est nécessaire au bon fonctionnement d'une application mobile, ou à la seule fin de satisfaire à des exigences légales, par exemple lorsque l'enregistrement du consommateur est requis, pour des raisons de sécurité et d'identification, par les législations applicables.

[115] Sur les problèmes que les systèmes d'intelligence artificielle, en particulier de *deep learning*, posent en ce qui concerne certaines dispositions du RGPD, voy. Y. Poullet, « Le droit face aux développements de l'intelligence artificielle dans le domaine de la santé », *LDI*, n° 152, octobre 2018, pp. 51 et 52.

taire de services sur les nécessités d'un contrat accepté par le consommateur. On le pressent, la solution, pour peu qu'on soit soucieux de la protection d'un utilisateur des services numériques ou à contenu numérique, à la fois en tant que consommateur que personne concernée, n'est pas dans la distinction entre contrat et consentement comme les distingue le RGPD mais résulte, à notre avis, d'une combinaison de dispositions où se complètent les droits de la protection des données, de la consommation sans oublier celui de la concurrence[116].

27. La première proposition de protection tant des données que des consommateurs est d'obliger les prestataires majeurs[117] de services numériques ou de fourniture de contenu numérique à prévoir différents niveaux de services, le service de base doit correspondre aux services de base, c'est-à-dire à l'objet principal du service ou à la seule fourniture du contenu[118], pour la réalisation duquel le nombre de données collectées reste minimal. Au-delà, on devrait pouvoir distinguer différents services auxquels est associée chaque fois la collecte de données complémentaires. À chacun de ces niveaux devrait correspondre la nécessité d'un consentement séparé, comme proposé plus haut (*supra*, n° 11). Peut-on comme le permet le CCPA[119]

[116] Sur cette combinaison absolument nécessaire, J. Senechal, « Vulnérabilités et contrôle du contractant à l'ère du numérique », in H. Jacquemin et M. Nihoul (coord.), *Vulnérabilités et droits dans l'environnement numérique*, coll. Faculté de droit de l'UNamur, 2018, p. 119 : « Dans ce contexte tendant à traiter de manière similaire les opérateurs ayant opté pour des modèles économiques différents, il semble difficile de ne pas étendre aux contrats de fourniture de service en ligne "gratuits" les règles du droit de la consommation, lorsque cette extension s'avère pertinente ». Dans le même ouvrage, pour une belle application des règles du droit de la consommation aux services de la société de l'information, voy. H. Jacquemin, « Protection du consommateur et numérique en droits européens et belge », *op. cit.*, pp. 237 et s.

[117] Comme la CCPA (Section 1798, 140 (c)) le prévoit, les entreprises sous un certain seuil d'activités devraient être exemptées de ces devoirs : « *A company that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($ 25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information* ».

[118] À notre avis, on est alors dans la situation décrite par le considérant n° 25 de la proposition de directive COM(2018)185 déjà citée pour l'exclure de l'application des dispositions de la proposition : « Lorsque le contenu numérique et les services numériques ne sont pas fournis moyennant une contrepartie pécuniaire, la directive 2011/83/UE ne devrait pas s'appliquer aux situations où le professionnel recueille des données à caractère personnel exclusivement pour garantir la conformité d'un contenu numérique ou d'un service numérique ou dans le seul but de se conformer aux exigences légales qui lui sont applicables. De telles situations peuvent inclure les cas dans lesquels l'enregistrement du consommateur est requis par les lois applicables à des fins de sécurité et d'identification, ou dans lesquels le développeur de logiciels ouverts recueille des données auprès des utilisateurs uniquement pour assurer la compatibilité et l'interopérabilité de tels logiciels ».

[119] CCPA 1798.125: « *(a) 2)Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data. (b) (1) A business may offer financial incentives, including payments to consumers as compensation,*

autoriser le prestataire de services à adapter son prix en fonction des données fournies par son client ou, pour être plus précis, aux données concernant ce client dont ce dernier consent au traitement ? En la matière, il est certain que la décision ne peut revenir à l'individu seul, décision qui risquerait alors d'être liée à la capacité financière de celui-ci de négocier la défense de sa vie privée. Il est nécessaire que les associations de protection des consommateurs et des données soient associées à toute décision en la matière et que, le cas échéant, des réglementations imposent des balises.

28. Une deuxième proposition tant de droit de la concurrence que de protection des consommateurs est déjà contenue dans le RGPD mais son application aux services, objet de la proposition de directive, nécessite quelques précisions utiles comme en témoigne le CCPA[120]. Il s'agit en effet d'étendre le contenu des données portables au-delà des données « *delivered* » par la personne concernée (article 20 du RGPD) à l'ensemble des données collectées sur la personne concernée (CCPA, 1798, 130), ce qui est bien plus large. Il s'agit ensuite de fixer le délai de réponse à la demande de la personne concernée et de prévoir les diverses hypothèses de délivrance de ce contenu. Ensuite, on ne peut qu'encourager au bénéfice d'une véritable liberté de choix du consommateur, l'application du droit de la concurrence, par la promotion d'un marché à multiples acteurs[121]. À défaut, au-delà des solutions existantes en cas de position dominante, il serait utile en ce qui concerne certains services numériques considérés par la population comme désormais nécessaires à la vie en société (par exemple, le service de communication des réseaux sociaux ou de recherche d'informations), d'appliquer à leurs prestataires les règles de « service universel », c'est-à-dire de fixer l'obligation d'offrir à tous moyennant une redevance ou non un service d'une qualité donnée.

29. Au-delà de ces références souhaitables aux droits de la consommation et de la concurrence, on note l'importance que pourrait avoir l'adoption par le législateur

---

for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data ».

[120] CCPA, 1798, 130 : « *Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable request and shall be made in writing and delivered through the consumer's account with the business…* ».

[121] Comme cela semble le cas en matière de moteurs de recherche avec l'apparition d'acteurs nouveaux à côté de l'acteur majeur, Google, comme Duck Duck Go ou Qwant qui se targuent d'offrir des services tenant compte des besoins de protection des données.

belge de la réforme du droit des obligations actuellement en discussion[122], en particulier la consécration législative du concept de l'abus de droit[123] : « Commet un abus de droit celui qui l'exerce de manière qui dépasse manifestement les limites de l'exercice normal de ce droit par une personne prudente et raisonnable placée dans les mêmes circonstances »[124]. Cette disposition trouve dans l'environnement numérique un terrain d'application évident dans la mesure où, à la complexité du fonctionnement des applications, largement opaque pour la personne concernée, à la quasi-instantanéité de l'émission du consentement, s'ajoute la totale dissymétrie des acteurs en cause. Que le responsable du traitement doive dans un tel contexte agir de manière raisonnable et prudente et ne pas s'écarter d'un usage débordant les traitements qui rentrent dans les « *reasonable expectations* » de la personne concernée, sous peine d'abus de droit, m'apparaît légitime. On ajoute que, selon la réforme projetée, l'article 5.7, § 3, permet à la personne victime, « la réduction du droit à son usage normal sans préjudice de la réparation du dommage que l'abus a causé ». On imagine l'intérêt du recours à la première sanction qui obligerait le responsable du traitement, nonobstant les clauses de la *Privacy Policy* à circonscrire les traitements aux seuls usages non abusifs.

30. Ces diverses solutions nous amènent à reconnaître qu'il reste toujours une place pour le ou les consentements qui doivent continuer à être réclamé(s) non comme un fondement distinct par rapport au contrat mais comme l'exigence d'un ou de plusieurs accords univoques qui sont nécessités au-delà de l'accord contractuel global. Cette place nous apparait cependant devoir être relativisée dans la mesure où nous pensons que l'individu n'est pas en mesure de se protéger efficacement contre la puissance de certains prestataires majeurs dans l'économie du secteur des services du net et la complexité des traitements et des flux de collecte et de communication des données[125]. Par ailleurs, comme nous l'avons montré dans la première partie, l'enjeu des opérations, qui se cachent derrière le consentement individuel, ne concerne pas seulement la personne concernée mais également d'autres personnes qui pourraient

[122] L'avant-projet de loi a été approuvé le 30 mars 2018 par le Conseil des ministres. Depuis, il est discuté en commission parlementaire de la Justice.

[123] D'abord consacrée par la jurisprudence, notamment par l'arrêt du 16 décembre 1982 (*Pas*., 1983, I, p. 472) et par la doctrine (notamment, P. Wery, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2e éd., pp. 138 et s., et la doctrine nombreuse y citée).

[124] Il s'agit du § 1er de l'article 5.7. du projet de réforme.

[125] À cet égard, les conclusions de N. Richards et W. Hartzog, « The Pathologies of Digital Consent », article à paraître in *Wash. U.L. Rev.*, 2016, 11 avril 2019, p. 4 de la version provisoire : « *Let us be clear about our claim… we believe that consent should retain its prominent place in our law generally. Our argument is more nuanced. Consent is undeniably powerful and often very attractive. But we have relied upon it too much and deployed it in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power* ». Les auteurs développent longuement les « pathologies » qui affectent la qualité du consentement et le rendent bien souvent une illusion dangereuse pour la protection des personnes concernées.

être discriminées[126], voire des choix de société. La nécessité de prendre en considération d'autres intérêts que les intérêts individuels de la personne concernée, donne son plein sens à un examen des principes affirmés par le RGPD pour tout traitement même ceux fondés sur le consentement. Les considérations de protection des consommateurs, de concurrence et d'accès pour tous à des services essentiels dans notre société de l'information contribuent à cet élargissement de la réflexion et surtout introduisent de nouveaux acteurs, autorité de la concurrence, commissions de protection des consommateurs aux côtés des autorités de protection des données[127].

31. La réflexion menée jusqu'ici nous conduit aux conclusions suivantes :

a. sur la toile, dans le cadre des services offerts aux consommateurs, la contractualisation des relations entre le prestataire de service est une réalité. Dans ce cadre, il est difficile de nier que les données à caractère personnel constituent une contrepartie au service proposé ;

b. la reconnaissance de cette réalité ne signifie en aucune manière une diminution des exigences de la protection de nos données qui s'impose aux contrats de service numérique et de contrats de services de fourniture de contenu numérique. Les droits de la personne concernée doivent y trouver leur application ; le consentement reste exigé même si sa signification ne se conçoit qu'au sein du contrat et sa validité reste soumise aux principes du RGPD relatifs à tout traitement ;

c. la reconnaissance de cette réalité a par ailleurs le mérite de souligner l'intérêt d'une alliance des acteurs et des exigences de la protection des données et des acteurs et des exigences du droit de la protection des consommateurs et de la concurrence et ce, au bénéfice de nos libertés et de la lutte contre les discriminations[128], plaidant pour une approche plus collective de celle-ci, à travers l'idée de « consentement collectif », conclu par le prestataire de services, responsable de traitement et les associations d'utilisateurs, tant celles de consommateurs que

[126] Dans la mesure où leur profil construit à partir de leurs données mais également des miennes comme d'autres utilisateurs conduirait à prendre des décisions désavantageuses pour elles. Le CCPA accorde une importance particulière à ces risques de discrimination, non relevés par contre dans les textes européens : « *(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services* ».

[127] C'est un des thèmes développés dans notre ouvrage, *La vie privée à l'ère du numérique – essais*, coll. du CRIDS, n^os 122 et s., Larcier, 2019, n^os 126 et s.

[128] « La proposition illustre l'importance de veiller à ce que le droit en matière de protection des consommateurs et le droit en matière de protection des données soient appliqués dans un esprit de complémentarité mutuelle, notamment dans l'environnement en ligne de l'Union européenne » (avis 08/2018, déjà cité, p. 16).

les associations de défense de libertés[129]. On ajoutera que dans cette négociation, les autorités de protection sont appelées, si possible, collectivement via le Comité européen de protection des données à jouer un rôle d'entremise ;

d. se précise dès lors notre conclusion à propos du consentement et de son poids au sein du RGPD. Comme l'écrivent Mmes Lobet et Cohen[130], ne s'agit-il pas d'un *privacy bug* ? Le mythe du consentement n'aboutit-il pas à la construction d'un cadre juridique qui affirme l'importance de la vie privée pour l'autonomie des sujets et, partant, la démocratie, mais qui laisse le poids de sa défense aux individus, à travers le concept de « consentement individuel ». L'individu est-il à suffisance armé pour réguler l'utilisation de données certes le concernant mais dont le traitement concerne également autrui voire l'intérêt général ?

[129] À ce sujet, les réflexions de T. Leonard, L. Bygrave et D. Wiese-Schartum, « Consent, proportionnality and collective power », disponible à l'adresse : http://www.uio.no/studies/enner/jus/jus/JURR5630/v11/undervisningsmateriale/consent_proportionality(final).pdf.

[130] C. Lobet-Maris, « Le fétichisme de la donnée à caractère personnel – relecture politique et critique de la vie privée », in E. Degrave *et al*. (éds), *Law, Norms and Freedoms in the Cyberspace, Liber Amicorum Yves Poullet*, p. 696 et J. Cohen, « Privacy, Ideology and Technology », *Georgetown Law Journal*, 89 (2011), p. 2029.