Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Consent

Poullet, Yves

Published in:
La confiance numérique

Publication date:
2022

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2022, Consent: "the privacy bug". dans *La confiance numérique: travaux de la Chaire sur la confiance numérique.* LexisNexis, Paris, pp. 75-117.

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

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

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

Download date: 03. Jul. 2025

Consent: 'The Privacy Bug'[1]

Yves POULLET[2]
Professeur émérite
Co-président de NaDI (Namur Digital Institute), Université de Namur
Professeur associé, Université catholique de Lille
Membre de l'Académie royale de Belgique

Le titre est volontairement provocant même si la réalité des méthodes de collecte « consentie » de données lui donne des accents de vérité. L'article, tout en nuançant le propos, invite à remettre en cause le dogme du consentement. Ce dogme est fondé sur l'argument simple suivant et, en apparence, imparable : le consentement n'offre-t-il pas à la personne concernée la meilleure des protections, puisqu'il fait dépendre de notre bon vouloir dûment informé, libre et spécifique le traitement par autrui de nos données à caractère personnel, devenu comme « notre » propriété. N'est-il pas, par ailleurs, l'expression la plus achevée de notre autonomie ou autodétermination qui définit la vie privée consacrée par l'article 8 de la Convention européenne des droits humains sur lequel s'appuient les législations de protection des données ? Ainsi, on conçoit que le consentement soit 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 de licéité des traitements de données à caractère personnel, en particulier les nécessités du contrat conclu entre le responsable et la personne concernée et l'intérêt légitime supérieur du premier cité. 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 et que nos doutes pèsent peu face au dogme du consentement ? Notre propos est de relever certaines zones d'ombre dans le texte même du RGPD et d'attirer l'attention sur les dangers liés à cette hypertrophie accordé au consentement au regard des technologies émergentes.

(1) Comme l'écrivent M^mes^ Lobet et Cohen (C. Lobet-Maris, *Le fétichisme de la donnée à caractère personnel – relecture politique et critique de la vie privée*, in *Law, Norms and Freedoms in the Cyberspace, Liber Amicorum Y. Poullet*, E. Degrave et *al.* [éds], p. 696 et J. Cohen, *Privacy, Ideology and Technology : Georgetown Law Journal* 2011, 89, p. 2029).

(2) L'auteur tient à remercier M^me^ J. Eynard (Maître de conférences à l'Université de Toulouse) pour ses précieuses observations. Ce texte s'appuie et reprend partiellement l'article : *Consentement et RGPD : des zones d'ombre ! : Droit de la consommation* 2019, n^os^ 122-123, p. 3-37. Il a été achevé le 1^er^ mars 2020 et par conséquence, n'a pas pu tenir compte de tous les développements doctrinaux, jurisprudentiels et réglementaires qui ont pu être publiés depuis, même si certains sont repris.

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 la protection des données, successeur de ce groupe et créé par l'article 68 du règlement. La lecture de ces textes laisse entrevoir quelques zones d'ombre lorsqu'on cherche à répondre aux questions suivantes : 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 des nécessités du contrat sont-elles pertinentes ? La deuxième partie analyse la manière dont la consécration par d'aucuns d'une propriété sur les données à caractère personnel a pu servir d'argument à l'analyse de la validité du consentement comme base de la légitimité du consentement ou, plutôt, d'un contrat de « vente » ou de « licence » de nos données. Enfin, troisième partie, la réalité des applications de l'internet, pour lesquelles notre soi-disant consentement est requis, suggère en effet l'abandon d'une approche individualiste du consentement au profit d'une approche plus collective, voire réglementaire. Cette dernière réflexion nous mènera à la conclusion.

§ 1. – Le consentement au traitement : l'analyse des textes

I. – La montée du consentement dans les textes européens

Notre réflexion part d'un étonnement à la lecture des premiers textes consacrant la protection des données. 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 à la fois l'introduction d'une définition du consentement (art. 2 h)[6] mais, au-delà,

(3) Règl. (UE) n° 2016/679, 27 avr. 2016 : *JOUE* n° 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 juill. 2011 ; V. égal. *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 WP217, 9 avr. 2014.
(5) Groupe de l'article 29, *Guidelines on consent under Regulation 2016/679*, 17/EN WP259, 28 nov. 2017. On ajoute que le 25 mai 2018, *l'European Data Protection Board* (Comité européen de la protection des données), mis en place par le RGPD (art. 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… ».
(6) « *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. »

sa consécration par l'article 7 du consentement comme principe de légitimation du traitement, par ailleurs le premier cité[7].

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[8], énonce ce droit comme suit :

« – 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[9].

Le règlement (RGPD), pris sur base de cette compétence, accorde une attention plus grande encore au consentement. Il est considéré par le Parlement européen[10] 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[11]. Ceci dit, dans la mesure où le consentement constitue une « autorisation »[12] donnée par la personne concernée à un traitement qui, sans cela, serait interdit faute d'autres bases de licéité, le RGPD renforce de manière substantielle[13]

(7) « 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… »
(8) 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 ».
(9) Parmi de nombreux commentaires de ces dispositions, lire A. Debet, J. Massot et N. Metallinos, *Informatique et Libertés*, Lextenso éd., 2015, p. 73 et s. – C. de Terwangne et K. Rosier (ss dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Larcier, coll. « CRIDS », 2018, n° 44. – Th. Léonard et *al.*, *Le RGPD : Commentaires article par article* (www.gdpr-expert.eu). – T. Douville, *Droit des données à caractère personnel*, Gualino, 2021, n^{os} 180 et s. – FRA (*European Union Agency for Fundamental Rights*), *Manuel de droit européen en matière de protection des données*, éd. 2018, p. 159 et s.
(10) Comité LIBE du Parlement européen, 21 nov. 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) : Doc. COM [2012], 0011 – C7-0025/2012 – 2012/0011 [COD], Rapporteur J.-Ph. Albrecht, « Exposé des motifs », p. 218-219.
(11) 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 ainsi l'article 1er : « 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 ».
(12) Sur ce terme et sa signification en droit privé, E. Thullier, *L'autorisation – étude de droit privé*, thèse, LGDJ, 1996, spéc. n^{os} 224 et s.
(13) Groupe 29, *Guidelines on consent under Regulation 2016/679*. Last revised and adopted on 10 April 2018, 28 nov. 2017, WP 259 rev.01, p. 16. 152. L'avis n° 15/2011 (préc., p. 12) réclamait déjà un renforcement des exigences en matière de consentement.

Centre de Documentation

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[14] relatifs au consentement[15].

II. – Les exigences des textes quant à la qualité du consentement

La définition du consentement est donnée par l'article 1.11. du RGPD : « 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[16]. L'exigence d'une manifestation de volonté libre signifie que la personne concernée dispose d'une véritable liberté de choix, ce qui reste à démontrer lorsque le consentement est donné en échange d'un avantage patrimonial[17], et est en mesure de refuser ou de retirer son consentement sans subir de préjudice, par exemple par un surcoût disproportionné[18] du service offert en suite de ce refus ou retrait. 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[19]. 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[20] ou administrés et administrations[21] mais, au-delà, chaque fois qu'il y a, comme le note le Groupe de l'article 29, « imbalance of powers »[22], ce qui pourrait bien être le cas lorsque le service ou le produit est offert dans un contexte de quasi-monopole ou concerne

(14) Nous n'analyserons pas la place que la directive *e-Privacy* en cours de révision donne au consentement.
(15) Nous n'aborderons pas non plus la question du consentement des mineurs et de la marge de manœuvre laissée sur ce point aux États membres.
(16) L'auteur renvoie aux études déjà mentionnées, *supra*, note 9.
(17) Nous reviendrons sur ce point dans le cadre de l'examen de la directive sur les contrats portant sur un contenu numérique. Relevons que la Cour de justice de l'Union européenne, dans une affaire récente (CJUE, 1er oct. 2019, aff. C-573717), où le consentement à l'utilisation des données de la personne concernée à des fins publicitaires était lié à la participation à une loterie, n'a pas eu l'occasion de se pencher sur ce problème dans la mesure où la question préjudicielle posée ne portait pas sur ce point. La Cour relève cependant (§ 64) : « … savoir si la circonstance que le consentement d'un utilisateur au traitement de ses données à caractère personnel à des fins publicitaires conditionne la possibilité, pour celui-ci, de participer à un jeu promotionnel, comme cela semble être le cas… et compatible avec l'exigence d'un consentement libre ».
(18) Nous ajoutons « disproportionné ». Il nous apparaît en effet normal que le prestataire de service puisse accorder 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.
(19) Sur ces points, lire Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., p. 3.
(20) 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 ».
(21) 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 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.
(22) Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., p. 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 présentes dans les services offerts par les réseaux sociaux, les moteurs de recherche et, de manière générale, par les plateformes en ligne.

un « bien » de première nécessité[23]. Nous reviendrons sur ce dernier point à propos des risques de manipulation qui entourent certains traitements, mais notons dès maintenant à l'appui de notre remarque que le règlement européen sur le traitement loyal des utilisateurs professionnels des plateformes en ligne[24] impose des obligations nouvelles[25] à charge des opérateurs de ces plateformes[26], considérant la situation de déséquilibre entre ces derniers et leurs utilisateurs professionnels et *a fortiori* non professionnels. Le projet de règlement dit *Digital Service Act*, en discussion actuellement, oblige par la même raison les très grandes plateformes à faire auditer par des tiers indépendants et agréés leurs algorithmes d'intelligence artificielle de profilage des internautes[27]. Comme le note le considérant 56 du projet :

> « Les très grandes plateformes en ligne sont utilisées d'une manière qui influence fortement la sécurité en ligne, la formation de l'opinion publique et du discours, ainsi que sur le commerce en ligne. La façon dont ils conçoivent leurs services est généralement optimisée au profit de leurs modèles d'affaires souvent axés sur la publicité et peut causer des préoccupations sociétales. En l'absence d'une réglementation et d'une application efficaces, ils peuvent établir les règles du jeu, sans identifier et atténuer efficacement les risques et les préjudices sociétaux et économiques qu'ils peuvent causer ».

Enfin, conformément à l'article 7.4. du RGPD, 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.

(23) Dans le même sens, N. Weinbaum, *La preuve du consentement à l'ère du RGPD et de la blockchain* : *JCP* G 2018, n° 110, p. 29.
(24) Cf. PE et Cons. UE, règl. (UE) n° 2019/1150, 20 juin 2019, promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne : *JOUE* n° L 186/57, 11 juill. 2019. Lire, en particulier, le considérant 2 : « Cela a son importance, principalement parce que l'intermédiation croissante des transactions par le biais de services d'intermédiation en ligne, conséquence d'importants effets de réseau indirects fondés sur les données, conduit à une dépendance accrue de ces entreprises utilisatrices, en particulier des micro-, petites et moyennes entreprises (ci-après dénommées "PME"), à l'égard de ces services pour entrer en contact avec les consommateurs. Du fait de cette dépendance croissante, les fournisseurs de ces services disposent souvent d'un pouvoir de négociation supérieur qui leur permet, dans la pratique, d'agir unilatéralement d'une façon qui peut être inéquitable et nuire aux intérêts légitimes des entreprises utilisatrices qui font appel à eux et, indirectement, des consommateurs dans l'Union. Par exemple, ils imposent parfois aux entreprises utilisatrices, de manière unilatérale, des pratiques qui s'écartent de manière excessive de la bonne conduite commerciale ou qui sont contraires aux principes de bonne foi et de loyauté. Le présent règlement vise à remédier à de telles frictions potentielles au sein de l'économie des plateformes en ligne ».
(25) Ainsi, par ex., 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 quinze jours ; en cas de résiliation de la fourniture du service à un client professionnel, lui fournir les raisons sans délai ; *etc.* Sur ce point, PE et Cons. UE, règl. (UE) n° 2019/1150, 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (*JO* n° L 186, 11 juill. 2019, p. 57).
(26) 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 Council9 ; *(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 ; (…) ».
(27) PE et Cons. UE, Prop. de règlement sur un marché unique des services numériques (loi sur les services numériques) et modification de la directive 2000/31/CE : Doc. COM (2020), 825 final, Bruxelles, 15 déc. 2020 (https://ec.europa.eu/digital-single-market/en/digital-services-act-package).

Centre de Documentation

Le consentement doit être spécifique. Comme le note le considérant 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[28] 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[29] suppose que la personne concernée reçoive une information, « sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples », comme le précise l'article 7.2. Elle implique un contenu informationnel minimal. Le considérant 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. Les *Guidelines* du Groupe de l'article 29[30] considèrent que d'autres informations sont nécessaires[31] « 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[32].

Enfin, le RGPD estime que le consentement doit être **univoque**. M^me^ de Terwangne[33] 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[34]. Le consentement doit être manifesté « par une déclaration ou un acte positif clair » selon le principe de **distinction** du consentement affirmé par

(28) Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., p. 10.
(29) 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.
(30) Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., p. 13.
(31) Ainsi, le type de données visées par le traitement envisagé, sur l'existence du droit de retirer le consentement donné (RGPD, art. 7, § 3), le cas échéant, l'utilisation éventuelle des données pour une prise de décision automatisée (RGPD, 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 (RGPD, art. 49, § 1^er^, *a)*).
(32) 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 (déc. 11 mai 2017, www.agcm.it/component/joomdoc/allegati-news/PS10601_scorrsanz_omi.pdf/download.html).
(33) C. de Terwangne, *Les principes relatifs au traitement des données à caractère personnel et à sa licéité*, in *Le règlement général sur la protection des données, Analyse approfondie*, ss dir. C. de Terwangne et K. Rosier, Larcier, coll. « CRIDS », 2018, n° 44, p. 125 et s.
(34) 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 (RGPD, art. 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 (RGPD, art. 49.1, *a*).

le Groupe de l'article 29[35]. 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 »[36]. Il est clair que l'indication suivant laquelle la poursuite de la navigation sur un site web équivaut à une acceptation est non recevable, faute d'univocité du consentement et que la présentation d'*opt-in* précochés ne peut équivaloir à un consentement[37].

On notera que c'est au responsable du traitement de démontrer premièrement que le consentement a bien été donné[38], 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 pour recueillir le consentement. Il s'agit là d'une application du principe d'*accountability*, devenu principe général de la protection des données et que, fort à propos, l'article 7.1 rappelle 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 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 »[39].

Le cumul d'autant de qualités du consentement exigées par le RGPD surprend le juriste généraliste. Si d'autres législations protectrices, en particulier le droit de la consommation ou le droit de la propriété intellectuelle lorsqu'il s'agit de protéger l'auteur face aux ayants droit, réclament le consentement, aucune n'impose autant d'exigences qualitatives à ce dernier. Faut-il voir dans cette avalanche de qualificatifs

(35) Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., 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, telles 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 : JCP* E 2018, n° 10, p. 30).
(36) Groupe 29, *Guidelines on consent under Regulation 2016/679*, préc., p. 16.
(37) 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*, préc., p. 17).
(38) 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 : JCP* E 2018, n° 10, p. 31. – A. Delforge et Y. Poullet, *Les blockchains : un défi et/ou un outil pour le RGPD*, in H. Jacquemin, A. Cottiga et Y. Poullet (éds), *Les blockchains et les smart contracts*, Cahier du CRIDS, n° 49, Larcier, 2021, p. 97 et s., spéc. p. 129 et s.
(39) Cet article évite en particulier que les utilisateurs d'un terminal ne soient enfermés dans un écosystème 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.

Centre de Documentation

une prise en considération de la nécessité particulière de protection qu'imposent les risques majeurs en matière de protection des données et donc de nos 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 remplissent les conditions légales, déplorer que ce cumul est purement incantatoire, là où dans la pratique, les consentements individuels recueillis en particulier sur le Net représentent une illusoire protection des personnes concernées ? À cet égard, une étude récente[40] conclut : « Although a wide majority of the websites in the sample (69 per cent) has in place a system to ask separate consent for engaging in marketing activities, it is only 16.2 per cent of them that obtain a consent which is valid under the standards set by EU law ». C'est dire que le consentement comme base de licéité des traitements opérés à travers le Net est pour le moins discutable et 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 avec les représentants des personnes concernées, en l'occurrence des consommateurs, comme le prévoit le droit de la consommation. Soumettre les *Privacy Policies* à un « consentement collectif » qui fixerait, à la fois, ce qui est acceptable, ce qui est exclu et les marges de manœuvre laissées au prestataire. Une telle négociation, placée sous la médiation des autorités de protection des données et de la consommation, serait à notre avis plus protectrice que le consentement individuel, bien souvent illusoire. On peut également imaginer que vis-à-vis de certains traitements, il soit interdit légalement de pouvoir obtenir certaines données, en particulier lorsque ces traitements s'appuient sur des techniques d'intelligence artificielle. Nous y reviendrons.

Continuer à fonder sur le consentement la légitimité des traitements opérés par des prestataires offrant des services à des franges importantes de la population présente par ailleurs un risque majeur de contestation judiciaire. Saisis 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 », il est à craindre que 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. Dès lors, ces juges exigeront demain le respect de toutes les conditions mises à la licéité du consentement. De telles exigences ruineraient le recours des responsables de traitement au consentement. Notre propos – et nous y reviendrons – souligne que l'approche purement individualiste du consentement nous apparaît critiquable là où seules une négociation collective ou, dirons-nous, les lois fixant les limites du consentement individuel nous apparaîtraient la solution.

L'article 7.3 du RGPD[41] précise enfin que le consentement peut être retiré à tout moment. Cette possibilité doit faire l'objet d'une information de la personne

(40) M. Borghi, F. Ferreti et S. Karapapa, « Online data processing consent under EU law : a theoretical framework and empirical evidence from the UK », *International Journal of Law and Information Technology* 2013, vol. 21, n° 2, p. 109-153.

(41) « 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.

concernée et la demande de retrait doit pouvoir s'effectuer de façon aussi facile que le consentement a été délivré. Afin de veiller aux intérêts du responsable du traitement qui, de manière légitime, a procédé au traitement des données collectées jusqu'au moment du retrait, l'article précise bien que le retrait s'effectue sans aucune conséquence 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 fondement des finalités. Notre point III consacré à la nature et à la place particulière du consentement parmi d'autres causes de licéité du traitement nous donnera l'occasion de revenir sur cette question.

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

A. – Le consentement, un acte unilatéral ?

Th. Léonard écrit :

« 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 d'actes sur les traitements en cause dans le respect du GDPR »[42].

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[43], en l'occurrence la licéité du traitement ou la levée d'interdiction du traitement. P. Wéry[44] 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 ».

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.

(42) Th. Léonard, *Yves, si tu exploitais tes données ?*, in *Law, Norms and Freedoms in Cyberspace, Liber Amicorum Y. Poullet*, E. Degrave et *al.* (éds), Larcier, coll. « CRIDS », 2018, n° 43, p. 663.

(43) Sur la distinction entre fait et acte juridique, lire 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 ».

(44) P. Wéry, *Droit des obligations*, vol. 2, *Les sources des obligations extracontractuelles, le régime général des obligations*, Larcier, 2e éd., 2016, p. 23.

Centre de Documentation

Sans doute, ces effets de droit sont prévus et encadrés par la loi mais ils sont voulus par la personne concernée sur les données qui sont l'objet du traitement. Bien évidemment, l'acte unilatéral que constitue ce consentement ne peut s'assimiler à celui de l'offre publique de récompense. En effet, dans ce second cas, l'engagement unilatéral de volonté met à la charge de la personne concernée des obligations[45] et notamment rend impossible tout retrait de l'acte unilatéral[46], retrait 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[47]. S'il faut dès lors parler d'acte unilatéral, ce n'est pas pour l'opposer au contrat, dans la 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, en particulier 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[48]. 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[49].

Sans doute, dira-t-on, importe-t-il que le consentement, voire les consentements relatifs aux traitements de données à caractère personnel, soient l'objet d'une ou de

(45) 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 critiquée 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).

(46) Comme l'écrit Aubert (*Introduction au droit*, A. Colin, 9e éd., 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 ».

(47) À ce sujet, lire 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 *Vulnérabilités et droits dans l'environnement numérique*, ss dir. H. Jacquemin et M. Nihoul, Larcier, coll. « Faculté de droit de l'UNamur », 2018, p. 74 et les nombreuses références citées, note 153.

(48) Pour ce motif, à savoir la crainte d'une assimilation du consentement au contrat dont il est l'accessoire, en sens contraire, Th. Douville, *Droit des données à caractère personnel*, Gualino, 2021, p. 112 : « Dans sa nature, il s'analyse comme un acte juridique unilatéral, y compris comme on le verra, lorsqu'il est donné à l'occasion d'un contrat portant sur la fourniture de données ».

(49) « 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 cité, p. 6).

plusieurs 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-ci ou ceux-ci ? Dans une étude détaillée sur les mécanismes contractuels mis en place dans le cadre de réseaux sociaux, J.-P. Moiny[50] 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 avancé par les partisans de la nature unilatérale du consentement, le caractère précisément unilatéral du retrait s'opposerait à la nature contractuelle du consentement, comme 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 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" »[51]. 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[52], de considérer les *Privacy Policies* comme partie intégrante des

(50) J.-P. Moiny, *Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée – quelques réflexions en droit belge et américain : Ann. fac. dr. Liège*, 2010, p. 134 à 218.

(51) J.-P. Moiny, *op. cit.*, p. 222.

(52) Il est à noter que la Cour de justice de l'Union européenne 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 Cour. 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.

Centre de Documentation

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[53].

B. – La place du consentement comme cause de licéité du traitement[54]

L'article 6.1. du RGPD 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 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, au regard en particulier des conditions figurant à l'article 5. 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 (pt b) et l'intérêt légitime (pt 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 base de l'article 7 de la directive 95/46/CE[55], avis auquel les *Guidelines* relatives au consentement prises cette fois sur base du RGPD, font toujours référence[56]. L'avis souligne la particularité du consentement comme condition de licéité par rapport aux autres conditions[57]. 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[58],

(53) 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 actuellement 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 ». Nous reviendrons sur ce point important.

(54) 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, 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.

(55) 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 WP217, 9 avr. 2014.

(56) Groupe de l'article 29, *Guidelines on consent under Regulation 2016/679*, 17/EN WP259, 28 nov. 2017, spéc. p. 9.

(57) On note qu'en cas de changement de finalités (RGPD, art. 6.4.), 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.

(58) 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, p. 52 et s.) : « To ensure protection from the start, and to avoid that the shifting of the burden of proof is circumvented113, 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 ».

sachant que ceux-ci peuvent être contradictoires, les uns rejoignant ceux du responsable, les autres s'en éloignant[59]. 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[60].

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 »[61].

Cette disposition interdit ou, plutôt, présume comme consentement non valable le fait qu'à l'occasion de la signature d'un contrat, on 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 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[62] : la crainte de ne pas voir s'exécuter le contrat rend-elle le consentement non libre[63] ?

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... ».

(59) « 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).

(60) « 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 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 WP259, 28 nov. 2017, p. 4).

(61) 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*, in *Le Règlement général sur la protection des données [RGPD/GDPR]*, ss dir. C. de Terwangne et K. Rosier, Larcier, coll. « CRIDS », n° 44, p. 133).

(62) Comme le note le Groupe de l'article 29 dans ses *Guidelines* déjà citées (p. 17), développant ainsi le considérant 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 de la directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique et du *Californian Consumer Privacy Act*.

(63) Sur ce point, lire Th. Léonard, *Yves, si tu exploitais tes données ?*, in *Law, Norms and Freedoms in Cyberspace, Liber Amicorum Yves Poullet*, E. Degrave et *al.* (éds), Larcier, coll. « CRIDS », 2018, n° 43, p. 664 et s.

Centre de Documentation CRIDS

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.

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[64], 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 que l'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[65]. 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.

Le Groupe de l'article 29[66] 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 »[67]. Ainsi les traitements répondant à une finalité doivent se voir assigner une et une seule base de licéité. Cette assertion poserait, selon Th. Léonard[68], une difficulté au moment où la base de licéité s'avère déficiente ; ainsi en cas de retrait du consentement, dans la mesure où ni le contrat, ni l'intérêt légitime ne pourront servir à fonder le traitement ni en

(64) « 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 juill. 2011, p. 7).

(65) Nous aurons l'occasion de montrer dans la deuxième partie comment l'EDPS applique ce principe de « subsidiarité » du consentement lors de son analyse critique de la proposition de directive relative aux contrats de fourniture à contenu numérique.

(66) Par contre, un récent avis de l'EDPS 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 » (CEPD, Avis 8/2018 sur le paquet législatif : « Une nouvelle donne pour les consommateurs », 5 oct. 2018, p. 17).

(67) *Guidelines on consent under Regulation 2016/679*, 17/EN, WP259, p. 22.

(68) Selon Th. Léonard (*Yves, si tu exploitais tes données ?*, in *Law, Norms and Freedoms in Cyberspace, Liber Amicorum Y. Poullet*, E. Degrave et *al.* [éds], Larcier, coll. « CRIDS », 2018, n° 43, 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.

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, par l'intérêt légitime supérieur du responsable du traitement, que par le consentement des clients. Mais que l'on ne s'y trompe pas : à chacune de ces 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.

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

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, celui 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[69] 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 de fondements légitimes prévus par la loi. Les paragraphes 1[70], 2, 3 et 4[71] de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données ».

(69) Rapport explicatif – STCE 223 – Traitement automatisé des données à caractère personnel (Protocole d'amendement), 10.X.2018, p. 8, n^{os} 41, 42 et 44.

(70) « 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. »

(71) Le paragraphe 2 exige un fondement légitime pour traiter les données (RGPD, art. 6) 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.

Centre de Documentation CRIDS

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[72] 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.* »[73].

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 »[74]. Dans le cadre de l'interprétation à donner aux articles 5 et 6 du RGPD, les *Guidelines*[75] 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.

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 trouvent 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. Ces principes ont fait l'objet d'un examen insuffisant mais qui 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 ou minimisation, 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

(72) Opinion 15/2011, déjà citée, p. 34.
(73) Même réflexion *in* : « 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 ».
(74) CJUE, 24 nov. 2011, *ASNEF et FECEMD c/ Administracion del Estado*.
(75) *Guidelines*, déjà citées, p. 4.

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, du moins dans le cadre des opérations effectuées sur le Net. 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[76].

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 deuxième partie.

§ 2. – Consentement et fourniture de données

Deux textes récemment apparus abordent la question délicate de la réglementation 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* (CCPA)[77], dont les similarités de contenu avec le texte

(76) 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 n° 375).
(77) *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 n° 375. Le texte a été approuvé par le *Governor* de l'État de Californie, le 28 juin 2018. Depuis, des amendements (le 13 septembre 2018 et le 11 octobre 2019) ont modifié le texte originaire. On ajoute qu'en novembre 2020, fut approuvée la proposition dite « 24 », soit le *California Privacy Rights Act* qui amende et étend le texte du CCPA. Le texte de cette loi est accessible sur le site : https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf. Ce texte, en particulier, généralise le droit d'opposition de tout citoyen à la vente de ses données à caractère personnel : « The amendment established a legal

du RGPD doivent être soulignées[78]. Le second est européen : il s'agit de la directive élaborée dans le cadre d'une politique européenne fixant « Une nouvelle donne pour les consommateurs »[79] et modifiant trois directives en matière de protection des consommateurs[80]. 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, 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, selon la doctrine dite de l'« économie de l'attention »[81], sur l'avantage que les entreprises qui offrent des services numériques, souvent gratuitement, tirent des données qu'elles collectent et exploitent[82]. Secondement, ils démontrent que le but

and enforceable constitutional right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information » (Sec. 2. A).

(78) Future of Privacy Forum, *Comparing Privacy Laws : GDPR vs CCPA*, juin 2018 (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 ».

(79) 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 » : Doc. COM (2018), 183 final.

(80) 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, 27 nov. 2019 : *JOUE* n° L 328, 18 déc. 2019.

(81) Cette économie dite de l'« attention » se base sur les théories de H. Simon (prix Nobel d'économie) exprimées pour la première fois en 1971 (*Designing Organizations for an Information-Rich World*, *in* M. Grennberger [éd.], *Computer, communications and the public interest*, Baltimore MD, The John Hopkins Press, 1971, p. 37-72) : « Dans un monde riche en informations, l'abondance d'informations entraîne la pénurie d'une autre ressource : la rareté devient ce que consomme l'information. Ce que l'information consomme est assez évident : c'est l'attention de ses receveurs. Donc une abondance d'informations crée une rareté de l'attention et le besoin de répartir efficacement cette attention parmi la surabondance des sources d'informations qui peuvent la consommer ». La mise en évidence de cette économie de l'attention comme explication des technologies d'IA, qui facilitent la désinformation, est fréquente : « [T]he advertiser usually sets the targeting parameters (such as demographics and presumed interests), but the platform's algorithmic systems pick the specific individuals who will see the ad and determine the ad's placement within the platform ». N. Maréchal et E. R. Biddle, *It's Not Just the Content, It's the Business Model : Democracy's Online Speech Challenge – A Report from Ranking Digital Rights*, New America, 17 mars 2020 (www.newamerica.org/oti/reports/its-not-just-content-its-business-model), p. 13.

(82) « 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 contenus numériques non fournis sur un support matériel, ladite directive devrait s'appliquer chaque fois que le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel,… » (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, 27 nov. 2019 : *JOUE* n° L 328, 18 déc. 2019. Comparer avec le considérant 2 de la proposition de directive du 11 avril 2018 qui a précédé le règlement (PE et Cons. UE, Prop. 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

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. *In fine*, nous 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.

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* »[83], soit « tout contrat en vertu duquel un professionnel fournit ou s'engage à fournir un contenu 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 »[84] 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 ».

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 le service 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)[85].

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 : Doc. COM [2018], 185 final) : « 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 ».

(83) La même directive parle également de contrat de service numérique et le définit comme suit (art. 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 ».

(84) 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 que 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 ».

(85) L'article 2 de la proposition de directive définissait en effet très largement la notion de « contenu numérique » : « *(a)* les données produites et fournies sous forme numérique, par exemple des vidéos, enregistrements

Centre de documentation

En ce qui concerne la « contrepartie » exigée de l'utilisateur des contrats visés, la proposition soulignait 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 expliquaient comme suit :

« Par conséquent, cette directive [2011/83/UE] ne s'applique pas aux contrats de services numériques dans le cadre desquels le consommateur fournit 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 »[86].

On note que, à l'instar de la définition européenne proposée, le texte californien ne distingue pas 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 légitime à réclamer une diminution de prix ou autre « juste » compensation en cas de vente de données à des tiers[87]. Sans doute, la volonté des auteurs européens était de bien faire et d'éviter

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, lire J. Rochfeld, *Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenu contre données » : Dalloz IP/IT* janv. 2017, p. 16. V. égal. H. Jacquemin, *Digital Content and Sales or Services Contracts under the EU Law and Belgian/French Law*, 9 (2017), *JPITEC*, p. 27 et J. Sénéchal, *La notion de fournisseur de contenu numérique : quel rôle pour les plateformes en ligne ? : Dalloz IP/IT* janv. 2017, p. 22.

(86) Assembly Bill n° 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 ».

(87) 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 n° 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 », Préamble).

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[88] mais était-ce bien nécessaire ? La suite, à savoir le texte final de la directive, démontre l'inverse.

Il y a longtemps que le droit prend en compte non l'apparence mais la réalité des transactions sur internet[89]. 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[90], 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[91] les autorités de protection des données, en particulier le CEPD qui, dans ses avis répétés à propos des deux versions[92] 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 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 »[93].

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

(89) « 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 » (Prop. de directive, consid. 13).

(90) J. Rochfeld, art. cité, p. 19. L'auteure se réfère à la recommandation de la Commission des clauses abusives (n° 2014/02) et à une décision de la cour d'appel de Paris du 12 février 2016 dans une affaire *Facebook* (*D.* 2016, p. 422).

(91) 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 ».

(92) 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 (Doc. 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 (Doc. COM [2015], 634 final – 2015/0287 [COD]) qui avait fait d'un premier avis du CEPD (CEPD, avis 04/2017 sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, 14 mars 2017).

(93) Avis 8/2018, déjà cité, p. 18, n° 52 ; même remarque *in* avis 04/2017, déjà cité, p. 9.

Centre de Documentation CRIDS

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[94] : 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 fourniture de données à caractère personnel s'opérerait « contre rémunération », selon les termes mêmes du projet de directive ; 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 deux bases de légalité du traitement, d'une part, le contrat et, d'autre part, le consentement.

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[95], 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 par autrui de biens particuliers actuellement disponibles ».

Th. Léonard[96] 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 ».

(94) En ce sens également, G. Versaci, *Personal Data and Contract Law : Challenges and concerns about the economic Exploitation of the Right to data Protection*, ECRI, 2018, 14 (4), p. 380 et s. D'autres objections pourraient être adressées, c'est pourquoi la proposition de directive se focalise sur les données fournies par le consommateur. Or la plupart des données collectées par les prestataires de service ne sont pas au sens propre fournies par le consommateur, mais sont générées par le fonctionnement de multiples techniques (*cookies*, 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 » (Prop. de directive, consid. 24 : Doc. 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*.

(95) F. Rigaux, *La vie privée, une liberté parmi les autres*, Bruxelles, Larcier, 1992, p. 155.

(96) Th. Léonard, art. cité, p. 670 ; de manière plus nuancée, R. Robert, art. cité, p. 357.

Tout récemment, dans une affaire concernant la participation d'un internaute à une loterie où ce dernier devait accepter de pouvoir être contacté par d'autres entreprises, l'avocat général de la Cour de justice de l'Union européenne[97] émettait l'opinion que, dans la mesure où la finalité de l'activité de loterie proposé 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 ».

Finalement, la directive a été adoptée. Si les auteurs de la directive ont désormais abandonné les termes provocateurs « contre rémunération », ils en ont maintenu le principe : « La présente directive », énonce l'article 3, alinéa 1[98], « s'applique à tout contrat par lequel le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur et le consommateur s'acquitte ou s'engage à s'acquitter d'un prix » et l'alinéa 2 envisage clairement l'hypothèse d'une fourniture rémunérée de données à caractère personnel[99]. Dans une telle hypothèse fondée sur la distinction discutable entre données anonymes et données non anonymes[100], le régime proposé consiste en une addition des règles. À celles mises en place par la directive relative à la conformité, la résolution du contrat, *etc.*, s'ajoutent celles imposées par le RGPD[101] : les considérants 38, 39 et 40 prennent soin de répéter ces règles, en particulier (consid. 38) :

« Lorsque le traitement de données à caractère personnel est fondé sur le consentement, en particulier en vertu de l'article 6, paragraphe 1, point *a*), du règlement (UE) n° 2016/679, les dispositions spécifiques dudit règlement s'appliquent, y compris en ce qui concerne les conditions visant à déterminer si le consentement est donné librement. La présente directive ne devrait pas réglementer la validité du consentement donné » ;

et plus loin (consid. 39) :

« Le droit à l'effacement et le droit du consommateur de retirer son consentement pour le traitement de données à caractère personnel devraient également s'appliquer pleinement en lien avec tout contrat relevant de la présente directive ».

(97) Opinion de l'avocat-général Szupnar, 21 mars 2019, Case C-673/17, *Planet 49 GmbH* vs *Bundesverband der Verbraucherzentralen und Verbraucherverbände*, spéc. n^{os} 97 et s.

(98) Pour être complet, c'est l'article 4 qui modifie la directive 2011/83 et insère dans cette directive un article 3, § 1bis qui prévoit : « La présente directive s'applique également lorsque le professionnel fournit ou s'engage à fournir au consommateur un contenu numérique non fourni sur un support matériel ou un service numérique et que le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf lorsque les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel pour fournir le contenu numérique non fourni sur un support matériel ou le service numérique conformément à la présente directive, ou de lui permettre de remplir les obligations légales qui lui incombent, pour autant qu'il ne traite pas ces données à une autre fin ».

(99) « La présente directive s'applique également lorsque le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur, et le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, (…). »

(100) Des travaux récents ont montré que des données affirmées comme anonymes peuvent, dans le cadre des recoupements que précisément permettent les outils d'intelligence artificielle, être « désanonymisées ». À cet égard, à propos des données de communications téléphoniques rendues anonymes et de la possibilité de ré-identifier les personnes concernées par ces données, V. l'étude de Y. de Montjoie, S. Gambs, V. Blondel et *al.*, *On the privacy-conscientious use of mobile phone data : Scientific Data* 11 déc. 2018, n° 5 (www.nature.com/articles/sdata2018286.pdf).

(101) En ce sens, les réflexions de Versaci, art. cité, p. 379 et consid. 38 : « La présente directive ne devrait pas réglementer les conditions applicables au traitement licite des données à caractère personnel, cette question étant réglementée, en particulier, par le règlement (UE) 2016/679. Dès lors, un traitement de données à caractère personnel en lien avec un contrat relevant du champ d'application de la présente directive n'est licite que s'il est conforme aux dispositions du règlement (UE) 2016/679 concernant les fondements juridiques du traitement des données à caractère personnel ».

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 libre de mettre en commerce librement[102]. Comment peut-on parler de propriété à propos de données à caractère personnel ? Au-delà de l'argument avancé par les auteurs[103] contre une telle propriété, à savoir l'impossibilité pour le consommateur, personne concernée[104], de déterminer la valeur patrimoniale de « son bien »[105], on opposera à l'approche « propriété » les arguments suivants[106]. 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 d'œuvres, résultant d'une création intellectuelle originale, même si des exceptions ont été consenties *via* des protections *sui generis*

(102) Dans le même sens, A. Pierucci, *Le rôle du consentement de la personne concernée dans le marketing électronique : Ubiquité* 2001, p. 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.

(103) À noter que d'autres auteurs défendent l'idée d'une propriété des données à caractère personnel ; ainsi V. Janecek (*Ownership of personal data in the Internet of things : CL&SR* 2018, n° 34, p. 1039 et s.) qui estime que les éléments de contrôle, de protection, de valeur et d'allocation des données à caractère personnel sont bien présents dans le cas des données à caractère personnel générés par l'internet des objets et permettent de plaider pour la qualification de propriété des données. Ces auteurs tirent argument de nouvelles dispositions du RGPD, à savoir le droit au retrait du consentement et celui à la portabilité. Sur la réfutation de ces deux arguments, lire parmi d'autres, Y. Padova, *Entre patrimonialité et injonction au partage : la donnée écartelée ? : RLDI* 2019, p. 50 et 51 : le droit au retrait n'interdit pas la possibilité de traiter les données collectées avant le retrait et n'interdit pas le responsable du traitement de poursuivre le traitement sur d'autres bases que le consentement ; quant au droit à la portabilité, il s'inscrit dans une logique d'ouverture à la concurrence et non de propriété.

(104) 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.

(105) La loi californienne (Sec2. Point E et F) s'exprime comme suit : « Because the value of the personal information they are exchanging for the good or service is often opaque, depending on the practices of the business, consumers often have no good way to value the transaction. In addition, the terms of agreement or policies in which the arrangements are spelled out, are often complex and unclear, and as a result, most consumers never have the time to read or understand them. This asymmetry of information makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses. Unlike in other areas of the economy where consumers can comparison shop, or can understand at a glance if a good or service is expensive or affordable, it is hard for the consumer to know how much the consumer's information is worth to any given business when data use practices vary so widely between businesses ».

(106) Sur ces objections, lire nos remarques sur le débat : *Propriété vs Libertés*, in *La vie privée à l'heure du numérique – Essai*, Larcier, coll. « CRIDS », 2019, n° 46, n^{os} 63 et s. et, plus récemment, *La « propriété » des données. Balade au « Pays des merveilles » à l'heure du big data*, in *Penser le droit de la pensée : Mél. en l'honneur de M. Vivant*, Dalloz, 2019, p. 339 et s. V. égal. l'excellent article de Y. Padova, *Entre patrimonialité et injonction au partage : la donnée écartelée (I) : RLDI* 2019, n° 157, p. 47 et s. Nous ajoutons les réflexions du panel d'experts réunis par le Gouvernement anglais : « However, there would be substantial technical and legal challenges in seeking to value individual contributions of data, not least because personal data often relates to more than one person. Neither is it clear what advantages data ownership would confer to the individual over and above a strong rights framework around consent, portability and removal of data, as introduced by the UK's new data protection laws. There are already several initiatives under development that would allow data subjects to extract value from their own personal data, which could operate within the existing rights-based framework. Furthermore, the Royal Society suggests that extending ownership rights to personal data would ignore the fact that the overall value of a dataset cannot be divided equally amongst its constituent parts. Whilst the supply of data is a necessary condition for creating economic value, it is not always sufficient. For example, the personal data of a single individual may not yield significant economic value when taken in isolation, as it is in the aggregation and effective use of data that value is often realised » (*The economic value of data*, discussion paper, H.M. Treasury, p. 9 : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf).

comme le régime des bases de données ou, tout récemment, le secret d'affaires[107]. Le deuxième constate que les données nous concernant sont loin d'être nos « produits »[108] : certaines sont partagées avec d'autres[109] ; 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 propriété de données dans de tels cas[110] ? Le troisième argument met en évidence le risque d'une telle reconnaissance. Si le droit reconnaît à la personne concernée la maîtrise de « ses » 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[111]. 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[112] 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 transfers ». 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 »[113]. 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[114]. La « vie privée » deviendrait ainsi un privilège de nantis.

(107) Sur les limites de l'approche « Propriété » des biens immatériels, lire T. Espeel, *Building Competitive Markets for Digital Data. The Interface between Data Ownership and Access to Data*, Mémoire DTIC, Namur, 2018, non publié. – T. Hoeren, *A new approach to Data Property : AMI* 2018, p. 58. – S. Gutwirth et G. Gonzalez-Fuster, *L'éternel retour de la propriété des données. De l'insistance d'un mot d'ordre*, in *Law, Norms and Freedom in Cyberspace, op. cit.*, p. 140 et s.

(108) Outre que les données collectées sont souvent triviales (par ex., 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 *cookies*, les numéros IP…) et qui sont attribuées par le responsable. Ces données ne peuvent être qualifiées « mes » données.

(109) À l'intérieur des *big data*, sont pris 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.

(110) « Individuals do not own information about themselves. Information does not pre-exist to its expression or disclosure but it is always to some extent constructed or created by more than one agent » (A. Rouvroy et Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy*, *in* S. Gutwirth et a., *Reinventing Data Protection*, Springer, 2009, p. 45-76. V. égal. la brillante démonstration de J. Kang et B. Bunter, *Privacy in Atlantis : Harvard Journal of Law and Technology* 2004, 18, 230-67.

(111) J. Litman, *Information Privacy/Information Property : Stanford Law Review* 2000, n° 52, 1283.

(112) D. Solove, *Privacy and Power, Computer Data Bases and Metaphors for Information Privacy : Stanford Law Review* 2001, n° 53, p. 1452.

(113) Même remarque *in* Y. Padova, art. cité, p. 54 : « D'autre part, elle augmente le risque d'un accord désavantageux pour la personne, en raison des risques d'asymétrie d'information entre les parties, (…) ».

(114) 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 des nouvelles conditions contractuelles] ».

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 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[115]. 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[116]. Les données ne sont pas des biens et, en tout cas, ne peuvent être construits sur base des mêmes concepts que ceux des biens 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), comme la directive sur les contenus numériques le reconnaît expressément.

À ces droits s'en ajoutent d'autres, liés cette fois à la protection du consommateur, ceux des législations de protection des consommateurs, mais également ceux spécifiques proposés pour les contrats de service numérique ou de fourniture de contenu numérique. Au rang des premiers, on épingle en particulier la prohibition des clauses abusives, des obligations d'information relatives à la présentation des résultats lors de recherche sur les moteurs de recherche et, corrélativement, la prohibition des manœuvres déloyales que constitue désormais la manipulation des classements[117] ;

(115) Ainsi dans l'affaire CJUE, 5 juin 2018, aff. C-210/16, *Unabhängige Landeszentrum für Datenschutz Schlewzig-Holstein c/ Wirtschafstakademie Schleswig-Holstein Gmbh*. 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 ».

(116) En particulier, les principes de loyauté, de finalité légitime et de proportionnalité.

(117) À cet égard, lire l'explication détaillée de l'article 1 de la défunte proposition de directive (Doc. COM [2018], 185 final), 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 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 ». L'article 3 de la directive finalement approuvée introduit un article 4 bis dans la directive 2005/27 qui oblige les plateformes à des informations complémentaires en ce qui concerne

au rang des seconds[118], le droit de rétractation[119][120] ou en droit californien[121], le droit d'exiger la suppression de toutes les données collectées à son propos[122] 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.

Le CEPD[123] s'inquiète des confusions que la proposition de directive introduit entre les conditions de licéité. La constatation que le projet de directive faisait référence à l'existence d'un contrat entre le prestataire et le « consommateur » n'excluait pourtant pas qu'au regard du RGPD, le traitement exige l'existence d'un consentement au sens et aux conditions fixées par le RGPD. À cet égard, le CEPD rappelle l'article 7.4, qui émet des doutes sur la validité des contrats qui établissent

les paramètres de *ranking* des produits proposés suite à une requête : « Lorsque la possibilité est donnée aux consommateurs de rechercher des produits offerts par différents professionnels ou par des consommateurs à partir d'une requête consistant en un mot clé, une phrase ou la saisie d'autres données, indépendamment de l'endroit où ces transactions sont finalement conclues, les informations générales mises à disposition dans une section spécifique de l'interface en ligne, qui est directement et aisément accessible à partir de la page sur laquelle les résultats de la requête sont présentés, concernant les principaux paramètres qui déterminent le classement des produits présentés au consommateur en réponse à sa requête de recherche, et l'ordre d'importance de ces paramètres, par opposition à d'autres paramètres, sont réputées substantielles » et l'article 6 de cette directive ajoute : « Les informations générales, mises à disposition dans une section spécifique de l'interface en ligne qui est directement et aisément accessible à partir de la page sur laquelle les offres sont présentées, concernant les principaux paramètres de classement, au sens de l'article 2, paragraphe 1, point *m*), de la directive 2005/29/CE, des offres présentées au consommateur en réponse à la requête de recherche ainsi que l'ordre d'importance de ces paramètres, par opposition à d'autres paramètres ; ». À propos de manœuvres déloyales en ce qui concerne l'information ainsi due, la directive ouvre le droit du consommateur à réparation contractuelle et extracontractuelle et à des actions contre la pratique des entreprises en cause.

(118) 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, § 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". (…) ».

(119) « 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 » (Prop. de directive : Doc. COM [2018], 185 final, consid. 21).

(120) 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 » (CEPD, avis 08/2018, n° 53, p. 18).

(121) CCPA, sect. 1798, 120 et 135.

(122) CCPA, sect. 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.

(123) Avis 08/2018, p. 17, mais surtout avis 04/2017, p. 13.

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 [art. 6, paragraphe 1, point *a)*], l'intérêt légitime du responsable du traitement [art. 6, paragraphe 1, point *f)*], le respect d'une obligation légale (par ex., le respect d'obligations de conformité ou de conservation des données) [art. 6, paragraphe 1, point *c)*], ou l'exécution du contrat interprétée de manière stricte [art. 6, paragraphe 1, point *b)*]. Cette distinction doit être maintenue ; dans les cas seulement où ni les nécessités du contrat ni l'intérêt légitime supérieur ne peuvent être invoqués, s'impose un consentement qui, comme nous l'avons vu, n'est pas en dehors du contrat mais est spécifique et s'ajoute à celui global tout en restant spécifique.

Revenons dès lors aux deux autres fondements de la licéité d'un traitement : les nécessités de l'exécution du contrat. La condition mise dans ce cas au traitement des données : « ce qui est (strictement) nécessaire à l'exécution du contrat » peut, suivant les applications et contextes, être variable[124]. 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 : des musiques en accord avec les besoins que votre « profil » laisse deviner, voire vous distiller de 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 qui ont accepté ce service supplémentaire. 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 (RGPD, art. 5.1.[c]) et posent des questions de transparence quant à la logique suivie (art. 13.2.[f])[125]. Si telle est la finalité du contrat, on voit mal en quoi l'article 7.4 constituerait une objection à fonder les multiples traitements du prestataire de services sur les nécessités d'un contrat accepté par le consommateur. On le pressent, la solution, pour peu que l'on soit soucieux de la protection d'un utilisateur des services numériques ou à contenu numérique, à la fois en tant que consommateur et 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

(124) 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.

(125) Sur les problèmes que les systèmes d'intelligence artificielle, en particulier de *deep learning*, posent en ce qui concerne certaines dispositions du RGPD, lire Y. Poullet, *Le RGPD face à l'intelligence artificielle*, Cahier du CRIDS, n° 48, Larcier, 2020.

dispositions où se complètent les droits de la protection des données, de la consommation sans oublier celui de la concurrence[126].

La première proposition de protection tant des données que des consommateurs est d'obliger les prestataires majeurs[127] 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[128], 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. Peut-on, comme le permet le *California Consumer Privacy Act* (CCPA)[129], 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.

Une seconde 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

(126) Sur cette combinaison absolument nécessaire, J. Sénéchal, *Vulnérabilités et contrôle du contractant à l'ère du numérique*, in *Vulnérabilités et droits dans l'environnement numérique*, ss coord. H. Jacquemin et M. Nihoul, 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, lire H. Jacquemin, *Protection du consommateur et numérique en droits européens et belge*, *op. cit.*, p. 237 et s.

(127) Comme la CCPA (sect. 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 ».

(128) À notre avis, on est alors dans la situation décrite par le considérant 25 de la proposition de directive (Doc. 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 ».

(129) 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, 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 ».

en témoigne le CCPA[130]. Il s'agit en effet d'étendre le contenu des données portables au-delà des données « delivered » par la personne concernée (RGPD, art. 20) 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[131]. 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 ex., 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.

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 belge de la réforme du droit des obligations actuellement en discussion[132], en particulier la consécration législative du concept de l'abus de droit[133] : « 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 »[134]. 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,

(130) 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… ».

(131) 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.

(132) L'avant-projet de loi avait été approuvé le 30 mars 2018 par le Conseil des ministres. Il n'a pu aboutir sous la précédente législature.

(133) D'abord consacrée par la jurisprudence, notamment par l'arrêt du 16 décembre 1982 (*Pas.* 1983, I, p. 472) et par la doctrine (not., P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2016, 2e éd., Larcier, p. 138 et s. et la doctrine nombreuse y citée).

(134) Il s'agit du § 1er de l'article 5.7 du projet de réforme.

nonobstant les clauses de la *Privacy Policy*, à circonscrire les traitements aux seuls usages non abusifs.

Ces diverses solutions nous amènent à reconnaître qu'il reste toujours une place pour le ou les consentements qui doi(ven)t 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 apparaît cependant devoir être relativisée dans la mesure où nous pensons que l'individu n'est pas suffisamment armé pour 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[135]. Par ailleurs, comme nous l'avons montré dans la première partie, l'enjeu des opérations, qui se cachent derrière le consentement individuel, n'intéresse pas seulement la personne concernée, mais également d'autres personnes qui pourraient être discriminées[136], 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[137].

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'imposent aux contrats de service numérique et aux contrats de services de fourniture de contenu numérique. Les droits de la personne concernée doivent y trouver leur application ; le consentement

(135) À cet égard, les conclusions de N. Richards et W. Hartzog, *The Pathologies of Digital Consent*, in *Wash. U.L. Rev.* 2016, 11 avr. 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.

(136) 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 ».

(137) C'est un des thèmes développés dans notre ouvrage, *La vie privée à l'ère du numérique – essais*, Cahier du CRIDS, n° 42, Larcier, 2019, nos 126 et s.

reste exigé même si sa signification ne se conçoit qu'au sein du contrat et que 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 entre, d'une part, les acteurs et les exigences de la protection des données et, d'autre part, les acteurs et les 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[138], 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 celles de défense des libertés[139]. On ajoutera que dans cette négociation, les autorités de protection sont appelées, si possible, collectivement *via* le Comité européen de la protection des données, à jouer un rôle d'entremise.

d) En exergue de cette contribution, nous nous interrogions : le consentement ne constitue-t-il pas 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 ? Bref, avons-nous besoin du consentement ? La troisième partie de notre contribution amplifie le propos en confrontant ce concept à la réalité des applications nouvelles nées des technologies émergentes.

§ 3. – De la réalité du « consentement » à l'heure des technologies émergentes. Nouveaux défis

L'utilisation des techniques d'intelligence artificielle (IA) ou, pour être plus précis, des techniques de *machine learning* suscite nombre de questions nouvelles. Ces techniques sont en effet fondées sur les connexions statistiques entre données au sein de *big data* et non plus sur celles dites « symboliques » présentes dans nos systèmes experts[140]. Les premières supposent une autonomie de fonctionnement des algorithmes, autonomie parfois limitée dans le cas de systèmes dits « supervisés », parfois plus complète lorsqu'il s'agit de systèmes dits de *deep learning*. Cette autonomie des systèmes de *machine learning* au contraire de ceux symboliques, où les algorithmes traduisent le raisonnement causal tenu par les experts et donc sont transparents du moins aux responsables du traitement, conduisent à une certaine

(138) « 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).

(139) À ce sujet, les réflexions de Th. Léonard déjà cité et L. Bygrave et D. Wiese-Schartum, *Consent, proportionnality and collective power*, *in* Reinventing Data protection, S. Gutwirth - Y. Poullet and alii, Springer 2009, publié également *in* https://www.researchgate.net/publication/226832769.

(140) Sur cette distinction, lire entre autres l'ouvrage très critique sur l'IA de Y. Meneceur, *L'intelligence artificielle en procès*, Bruylant, 2020, p. 19 et s.

opacité, voire à une opacité certaine de la manière dont les corrélations entre données à travers un réseau complexe de neurones fonctionnent. Notre propos n'est pas de reprendre ici des développements étudiés ailleurs[141], mais de nous concentrer sur les défis que le développement des applications utilisant les techniques de l'IA pose en ce qui concerne la licéité du seul consentement pour fonder les traitements en cause. 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*[142]. 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 »[143][144].

On connaît les caractéristiques des outils IA, du moins ceux utilisant les techniques de *machine learning*[145]. La première est certes l'autonomie des systèmes qui explique, en particulier mais non uniquement, dans les systèmes dits de *deep learning*, à la fois l'imprévisibilité, l'évolutivité voire le caractère absurde des résultats de ces corrélations[146], leur évolutivité, le risque de biais ou d'erreurs[147].

(141) Y. Poullet, *Le RGPD face aux défis de l'intelligence artificielle*, Cahier du CRIDS, n° 48, Larcier, 2020.

(142) HLGE (High Level Group of experts) on AI, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 8 avr. 2019, n° 67, texte disponible sur le site : Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu) (consulté pour la dernière fois le 13 janv. 2021).

(143) Ce qui témoigne de la pertinence discutable du maintien d'une distinction entre données anonymes et données non anonymes, distinction qui pourtant continue à être faite, ainsi dans la directive étudiée, qui distingue les contrats de fournitures de données numériques à caractère personnel de ceux portant sur des données anonymes (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, 27 nov. 2019 : *JOUE* n° L 328, 18 déc. 2019).

(144) Lignes directrices citées, p. 11.

(145) B. Frenay et Y. Poullet, *Rapport et propositions de recommandations sur le « Profilage et la Convention 108 » du Conseil de l'Europe*, Rapport présenté au Comité consultatif de la Convention n° 108, p. 9 et s., Strasbourg, 21 sept. 2019 (rapport disponible sur le site du Conseil de l'Europe). À cet égard, les définitions retenues par le projet de recommandations : « Le terme "intelligence artificielle" (IA) désigne un système qui est soit fondé sur des logiciels, soit intégré dans des dispositifs matériels, et qui fait preuve d'un comportement intelligent, notamment en collectant et traitant des données, en analysant et en interprétant son environnement et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques.
L'expression "traitement utilisant des procédés d'apprentissage automatique" (*machine learning*) signifie un traitement utilisant des méthodes particulières d'intelligence artificielle basées sur des approches statistiques pour donner aux ordinateurs la capacité d'"apprendre" à partir de données, c'est-à-dire d'améliorer leurs performances à résoudre des tâches sans être explicitement programmés pour chacune ».

(146) Sur ces caractéristiques, parmi d'autres, l'ouvrage très polémique de Y. Meneceur, *L'intelligence artificielle en procès*, Bruylant, 2020, en particulier les exemples de biais et d'erreurs, p. 166 et s. ; ainsi, la corrélation trouvée par un système d'IA entre le nombre de divorces dans l'État du Maine et la consommation de margarine ou celle entre le taux de suicides aux États-Unis et le niveau de dépense en recherche spatiale…

(147) Sur ces biais et erreurs, lire B. Frenay et Y. Poullet, *Rapport sur le profilage* présenté au Comité consultatif de la Convention n° 108 du Conseil de l'Europe, nov. 2019, p. 15 et s. On cite souvent les biais en défaveur

La deuxième caractéristique de tels systèmes est, comme signalé au point précédent, l'opacité de leur fonctionnement, y compris par leur concepteur et donc la difficulté pour le responsable du traitement de rendre compte du fondement de la décision prise ou proposée par le système vis-à-vis de la personne concernée, là où dans les systèmes causals d'IA dits « symboliques » qui traduisent le raisonnement des experts, la transparence du raisonnement et de son application à un individu est facile. Enfin, une dernière caractéristique est que ces systèmes prétendent à leur capacité de prédiction des comportements de la personne concernée. L'opacité du fonctionnement jointe à cette capacité de prédiction présente une autre conséquence : le risque de manipulation. Cette possibilité de manipulation existe d'autant plus que l'intelligence artificielle permet ce que notre collègue A. Rouvroy appelle la « gouvernementalité algorithmique ». Les profils générés automatiquement par ces systèmes, sans autres fondements que la pure corrélation de données à la fois non contextualisées et également prises dans le cadre de finalités distinctes, constituent des outils non seulement d'analyse du passé, mais également un outil d'action vis-à-vis des individus du fait de la « vérité » à laquelle, en particulier, ces opérations de profilage prétendent aboutir. Le profilage constitue donc, pour celui qui dispose de ces systèmes d'IA, un instrument de prévision de nos comportements futurs[148] d'autant plus puissant que le responsable de traitement se prévaudra de l'« objectivité » et de la quantité des données collectées, souvent triviales et brutes (la localisation, les données de *surfing* ou de consommation...) et, donc, d'autant moins suspectes d'une appréciation subjective douteuse.

Une première manifestation de cette manipulation réside certainement dans ce qu'il est convenu d'appeler les *nudges*[149] : les systèmes vous proposent à vous, conducteur, la meilleure route à suivre ; à vous chercheur, la façon dont votre indice H pourra évoluer ; à vous responsable d'une commune, les zones d'insécurité ou d'abandon où votre police doit intervenir ; à vous ministre de l'Éducation ou enseignant, les critères selon lesquels *a priori* les enfants ont des chances de réussir leur parcours scolaire ; à vous juges, les risques de récidive d'une personne auteur d'une infraction ou la décision la plus conforme au droit ou plutôt ce qui a déjà été jugé comme conforme au droit ; à vous lecteur, les ouvrages qui doivent correspondre à vos goûts. L'ordinateur vous adresse à vous, consommateur X ou Y, la « publicité » ciblée du produit ou service qui est supposé répondre le plus étroitement à vos goûts. Cette manipulation est-elle répréhensible ? Certes, non. Le commerçant a de tout temps eu recours au *bonus dolus*, sans que cette pratique

des populations afro-américaines (critère ethnique surpondéré par rapport à d'autres critères comme le niveau d'éducation, le parcours familial, *etc.*), ainsi, ceux révélés par l'analyse du fameux logiciel COMPAS, système d'intelligence artificielle utilisé par la justice américaine pour « prédire » les risques de récidive des individus arrêtés pour infraction. Sur cette analyse, V. l'étude souvent citée de K. Gummadi, *Discrimination in machine decision making*, accessible sur le site Discrimination_ML_KrishnaGummadi.pptx (iitkgp.ac.in).

(148) Comme l'affirmait le patron d'Amazon, « avant même que vous passiez commande, nous avons déjà préparé votre colis », et le patron de Google renchérit : « It will become very difficult for people to see or consume something that has not in some sense been tailored for them ».

(149) La théorie du Nudge (ou théorie du paternalisme libéral), nous explique Wikipedia, est « un concept des sciences du comportement, de la théorie politique et d'économie issu des pratiques de design industriel, qui fait valoir que des suggestions indirectes peuvent, sans forcer, influencer les motivations, les incitations et la prise de décision des groupes et des individus, au moins de manière aussi efficace sinon plus efficacement que l'instruction directe, la législation ou l'exécution ».

soit considérée comme répréhensible. Elle peut même apparaître comme un bénéfice pour le « client » futur dans la mesure où elle ajoute à son information, lui fait découvrir de nouveaux produits ou services, voire répond à sa demande d'être guidé dans un marché de plus en plus complexe et offrant des produits de plus en plus diversifiés. La manipulation n'est répréhensible que si elle représente un « abus de circonstances », pour reprendre l'expression du projet de loi belge[150]. Le projet de loi définit la notion 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 »[151]. Cette manipulation est par ailleurs punissable, si elle constitue un « abus de la faiblesse d'autrui », selon l'expression de la loi pénale belge du 26 novembre[152]. La nécessité de prise en compte de la vulnérabilité de chacun dans notre société moderne exige cette extension. Même si le risque de manipulation « abusive » est plus grand lorsqu'il s'agit de mineurs, de personnes âgées ou de handicapés, la nécessité de prise en compte de la vulnérabilité de chacun dans notre société moderne exige cette extension nonobstant son caractère flou.

Ce risque de manipulation lié aux systèmes de profilage modernes sera d'autant plus présent que le déséquilibre informationnel est important. Il est patent que les profilages exercés par les grandes plateformes, en particulier celles qui constituent les réseaux sociaux ou apparaissent comme la porte d'entrée (*gatekeeper*) à l'information, qu'elle soit textuelle, sonore ou d'images, peuvent bénéficier des milliers de données accumulées par l'utilisation de leurs services et se nourrir d'autres données accumulées par l'offre d'autres produits ou services. Ainsi, simple exemple, Google peut nourrir ses *big data* des données obtenues lors de l'utilisation par 80 % de la population de son moteur de recherche, des données de géolocalisation liées à l'utilisation par plus de 60 % de la population de son système Android, mais également des données obtenues par les 1 000 sociétés sœurs qui composent le holding Alphabet. Peut-on considérer que le consentement de l'internaute face à Google est libre ou faut-il entourer ce consentement de nombre de conditions préalables ? Nous reviendrons sur ce point.

La manipulation met en lumière l'absence d'une des exigences mises par le RGPD au consentement : les technologies modernes de traitement de l'information interrogent la question de la liberté du consentement. Notre première partie mettait en évidence que les modes de collecte du consentement bien souvent se limitent à un clic sur la formule : « j'accepte » au bas d'une page web où, comble de l'ironie, le responsable du traitement écrit en grandes lettres : « la défense de votre vie

(150) La réforme actuelle menée en Belgique en matière de droit des contrats consacre ce concept, en son article 5.41 du projet de Code des obligations.

(151) Cf. sur cette disposition, son origine et ses commentaires, les réflexions de H. Jacquemin, *Protection du consommateur et numérique en droits européen et belge*, in *Vulnérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage ss coord. H. Jacquemin et M. Nihoul, Larcier, coll. « Faculté de droit de l'UNamur », 2018, p. 241 et s. ; dans le même ouvrage, lire également F. George et J.-B. Hubin, *La protection de la personne en droit des obligations*, p. 67 et s.

(152) La loi du 26 novembre 2011 introduit, dans notre Code pénal belge, la notion d'abus de la situation de faiblesse d'autrui. Au recours adressé par certains contre le caractère flou de cette législation peu respectueuse à leurs yeux du principe de « prévisibilité » de la loi pénale, la Cour constitutionnelle belge, le 7 novembre 2013, justifie l'extension de la manière suivante : « Dans une société démocratique, la protection des personnes en situation de faiblesse constitue une condition essentielle pour protéger les droits fondamentaux de chacun ».

privée est mon souci », ce clic étant par ailleurs une condition de la poursuite de la visite ou en tout cas de sa poursuite utile. Certes, il vous est loisible de consulter la *Privacy Policy* voire, parfois, de paramétrer votre acceptation en ce qui concerne les diverses finalités mais, croyez mon expérience, vous vous épargnerez rapidement ce détour par des pages à la lecture longue, à la compréhension difficile et qui, dans l'attente impatiente où vous êtes de pouvoir accéder à l'information, au service souhaité, vous apparaîtra contre-productif.

Que proposer ? La liberté n'impose-t-elle pas que soient offerts à la personne concernée un choix ou plutôt des choix ? Ne faut-il pas laisser le choix à la personne concernée entre un accès non profilé et un accès profilé, voire entre un accès anonyme ou au contraire identifié ? On reprendra volontiers, sur ces deux points (droit à l'anonymat et droit à ne pas être profilé), la recommandation 3.7 de 2010 du Conseil de l'Europe[153], qui affirme :

> « Dans la mesure du possible et à moins que le service requis nécessite de connaître l'identité de la personne concernée, toute personne devrait avoir accès aux informations relatives à un bien ou à un service ou avoir accès à ce bien ou à ce service sans devoir communiquer de données à caractère personnel au fournisseur du bien ou au prestataire du service. Aux fins d'assurer un consentement libre, spécifique et éclairé au profilage, les prestataires de services de la société de l'information devraient assurer, par défaut, un accès non profilé aux informations relatives à leurs services ».

Au-delà, il importe que la personne concernée puisse, face à certains traitements fondés sur des systèmes d'intelligence artificielle (en particulier lorsqu'il s'agit de profilage à des fins publicitaires), définir la finalité du profilage qu'elle souhaite et, dès lors, réduire le champ des données qui seront exploitées. Prenons l'exemple déjà discuté de l'accès à un service de musique en ligne. Cet accès ne suppose pas que vous soyez d'accord avec le profilage de vos goûts musicaux lequel, par contre, est nécessaire si vous souhaitez, service supplémentaire, que le fournisseur vous conseille ou vous propose des musiques adaptées à vos goûts. Votre choix devrait pouvoir porter sur diverses finalités et, le cas échéant, sur les destinataires tiers qui permettront de réaliser les finalités. Ainsi, pour reprendre toujours l'exemple du service de musique en ligne, peut-être le souhait de l'internaute est-il de recevoir l'annonce publicitaire émanant de tiers à propos de la sortie d'une chanson de son interprète favori ? À l'inverse, le choix de l'internaute peut s'exprimer en sens contraire.

Autre point, admettre le profilage à des fins publicitaires par le responsable de traitement ne signifie pas nécessairement admettre le profilage par des tiers ou la cession de données ou de mon profil à des tiers. Ainsi, l'utilisation de systèmes d'IA dans le cas de voitures connectées devrait distinguer différentes hypothèses : celle où le possesseur de la voiture connectée souhaite connaître son profil de conducteur à des fins personnelles (respect des limites, analyse de la consommation, risques pris [par ex. : conduite en état de somnolence ou d'alcoolisme...]) sans que ces « profils » ne soient accessibles à son garagiste hormis pour des raisons de sécurité ;

(153) Ces dispositions ont été reprises dans le cadre du projet de recommandation sur le profilage, actuellement porté à l'adoption du Conseil des ministres du Conseil de l'Europe (Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Convention 108, Projet de recommandation sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage [révisant la Recommandation [2010]13], T-PD(2019)07Bis.

celle où ce possesseur refuse l'utilisation de tout système d'IA ; celle au contraire où il marque son accord à l'utilisation de certaines données par le concessionnaire ; celle où il accepte (sous réserve de ce qui sera dit plus loin) la communication des données à son assureur afin de bénéficier d'une prime adaptée à « son » risque ; celle, altruiste, où il accepte le transfert de données anonymisées tirées de son utilisation à l'autorité publique à des fins d'améliorer la mobilité des citoyens. Le consentement ne peut être, sauf exceptions, la condition d'accès à des services souvent ressentis comme nécessaires à l'exercice de la vie sociale. Il devrait, sauf nécessité liée au service lui-même[154] (par ex., un service de confection de vêtement sur mesure offert à distance ou un service d'éducation à distance), toujours être accompagné d'une offre d'un service non profilé, qui, par défaut, s'appliquerait[155].

Le consentement doit être informé et spécifique, nous dit le RGPD. Ces exigences posent également problème à l'heure d'une IA opaque **et** aux finalités difficilement circonscrites. L'information est difficilement complète lorsque l'on sait que le propre de l'IA est de travailler avec des *big data* dont le contenu peut difficilement être proportionné *a priori* et, même, dans le cas de systèmes *deep learning*, *a posteriori*. Le responsable du traitement, s'il peut cependant introduire certaines contraintes (par ex., refuser des données sensibles), ne peut deviner les corrélations qui seront opérées par la machine et qui rendront signifiants certains types de données à l'exclusion d'autres. Par ailleurs, le hasard des corrélations peut révéler de manière incidente de nouvelles finalités. Ainsi, exemple extrême, tant IBM que Microsoft[156] ont révélé qu'un système IA associant l'analyse tantôt des frappes sur le *keyboard* des ordinateurs, tantôt du langage utilisé dans les messages échangés, de son évolution, des fautes de frappe, *etc.*, pouvait révéler, mieux que les examens médicaux classiques, des maladies comme la bipolarité ou, de manière très précoce, la maladie d'Alzheimer. Dans un ouvrage récent, Meneceur[157] décrit, entre autres, la façon dont le système HART (*Harm Assessment Risk Trial*) développé au Royaume-Uni par la police de Durham avec l'Université de Cambridge et ayant pour finalités le calcul du risque d'infractions relatives à certaines personnes ou groupes de personnes, de même que la réduction des emprisonnements par l'offre ciblée de peines alternatives, a été alimenté par des données contenant le profil

(154) Mais on est alors dans une hypothèse de licéité du traitement, à savoir le traitement nécessaire à l'exécution du contrat ou de mesures précontractuelles (RGPD, art. 6.1, *b*)).

(155) C'est en tout cas dans ce sens que s'oriente la proposition de règlement e-*Privacy*. Les utilisateurs doivent être informés de toute collecte de données et de la finalité de l'utilisation de celle-ci. Par conséquent, le consentement ne doit pas être caché dans les conditions générales ou lié à d'autres services. Ainsi, un achat en ligne nécessite le transfert des données par l'acheteur pour mener à bien la transaction. Par contre, il n'est pas permis d'utiliser les données transmises à des fins publicitaires. Cela nécessiterait en effet soit un nouvel accord spécifique et, dans ce cas, un consentement clair du client, soit dans le cadre où l'intérêt légitime du responsable du traitement est invoqué, la preuve que la balance d'intérêts a été opérée.

(156) B. Schroder, directeur de la recherche Microsoft Benelux, écrit (*Des cookies, à l'IOT, aux robots et à l'intelligence artificielle*, in *Vie Privée, transparence et démocratie*, Actes du Colloque du REHNAM, Namur, 28 nov. 2019, Y. Poullet [éd.], Cahier du CRIDS, n° 50, Larcier, 2020, p. 69) : « Nous sommes maintenant capables, de résoudre de toutes nouvelles classes de problèmes, telles que la reconnaissance d'image ou la transcription de la voix. Nous pouvons prédire des événements non modélisables. Par exemple, Cornell University détecte la survenance de l'état dépressif de patients bipolaires en analysant les changements dans la frappe de messages sur l'écran d'un smartphone. Un algorithme de Microsoft prévoit un diagnostic futur de cancer du pancréas ou de poumon par l'analyse de l'historique des mots clés entrés dans un moteur de recherche ».

(157) Y. Meneceur, *op. cit.*, p. 100 et 101.

de cinquante millions d'adultes provenant de sources par ailleurs publiques et catégorisant les personnes selon des critères comme l'appartenance ethnique, l'âge, la résidence... En d'autres termes, les *big data* constituées peuvent servir à de nombreuses finalités[158] et notre consentement à y figurer sera dès lors rarement informé et spécifique. À nouveau, on pointe combien l'activité des plateformes pose problème à cet égard, que ces plateformes gèrent les réseaux sociaux ou qu'elles constituent un outil indispensable pour assurer l'accès à l'information comme les moteurs de recherche ou à la communication comme les opérateurs de messagerie électronique. De par l'étendue de leurs activités exercées à travers de nombreuses filiales ou sociétés apparentées, de par le fait qu'elles constituent un passage obligé (*gatekeepers*), elles disposent de données en nombre indéfini qu'elles peuvent croiser, notamment *via* les *cookies* ou autres identifiants. On ne sera dès lors pas surpris qu'elles investissent massivement dans l'intelligence artificielle, par exemple à des fins de marketing ou de recherche (ainsi, les recherches menées par une filiale d'Alphabet : Calypso qui travaille sur le vieillissement). Outre leurs propres développements en IA à des fins internes, elles représentent sur le marché de l'information, l'intérêt d'être un fournisseur de données particulièrement éclairé. Ainsi une société de prêt-à-porter souhaite obtenir les adresses électroniques des personnes susceptibles d'être intéressées par ses produits et, à partir des critères que cette société désignera, elle ira, *via* des API (*Application Programming Interfaces*) et dans le cadre d'un accord bien balisé, fouiller dans les bases de données de la plateforme et acquerra d'elle les données *ad hoc*[159][160]. Autre scénario, la plateforme, à partir du projet de la société, élaborera, comme un fournisseur de services, le système IA capable d'extraire de ses bases de données les données adéquates.

(158) Sur ce point, les lignes directrices de l'EDPB, *Guidelines 8/2020 on the targeting of social media users*, Adopted on 2 Sept. 2020, disponible sur le site de l'EDPB (edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en). Ainsi, récemment, une enquête de Techcrunch, une société de média spécialisée en analyse de technologie digitale, révélait que « la société israélienne Glassbox enregistre ce que vous faites sur votre téléphone, à chaque fois que vous êtes sur le site ou l'application de l'un de ses clients. Cette entreprise d'analyse de données tente de mieux comprendre les comportements des consommateurs et la manière dont ils naviguent dans certaines applications. Ainsi Hotels.com, Expedia, Abercombie & Fitch et bien d'autres encore, font appel à Glassbox pour enregistrer tout ce que font leurs clients lorsqu'ils sont sur leur application : saisir du texte, cliquer, zoomer, tous les gestes sont enregistrés ».

(159) Le rapport de l'ICO (ICO, *Big Data, artificial intelligence, machine learning and data protection*, p. 11 : https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf ; dernière consultation 17 janv. 2021), l'autorité de protection des données, donne l'exemple de la société *Data Shift*. Cette société a pour objet, à partir de données venant de Twitter, Facebook et autres médias sociaux qu'elle analyse de les revendre pour des finalités marketing ou autres.

(160) À noter dès lors cette volonté de soumettre les plateformes à un devoir d'évaluation *a priori* des risques liés à leurs systèmes d'IA de recommandation et de profilage, évaluation qui pour les « très grandes plateformes » (soit utilisées par plus de 10 % de la population européenne) devrait être menée par un auditeur externe accrédité. V., à ce propos, le projet européen de règlement dit *Digital Service Act* qui, en ses articles 26 et suivants, précise : « Les très grandes plateformes en ligne recensent, analysent et évaluent, à compter de la date d'application visée au second alinéa de l'article 25, paragraphe 4, puis au moins une fois par an, tout risque systémique important trouvant son origine dans le fonctionnement et l'utilisation faite de leurs services au sein de l'Union. Cette évaluation des risques est spécifique à leurs services et comprend les risques systémiques suivants :
(a) la diffusion de contenus illicites par l'intermédiaire de leurs services ;
(b) tout effet négatif pour l'exercice des droits fondamentaux relatifs au respect de la vie privée et familiale, à la liberté d'expression et d'information, à l'interdiction de la discrimination et aux droits de l'enfant, tels que consacrés aux articles 7, 11, 21 et 24 de la Charte, respectivement ;
(c) la manipulation intentionnelle de leur service, y compris *via* l'utilisation non authentique ou l'exploitation automatisée de leur service, avec un effet négatif avéré ou prévisible sur la protection de la santé publique, des mineurs, du discours civique, ou des effets avérés ou prévisibles en lien avec les processus électoraux et la sécurité publique ».

Dans de telles hypothèses, s'évanouit le mythe d'un consentement libre, informé et spécifique, nécessaire pour assurer la manifestation du contrôle par la personne concernée de la circulation de son « image informationnelle ».

Le consentement ne dispense pas, avons-nous dit, d'un examen de la légitimité des traitements même si le consentement présume facilement que la personne concernée marque son accord sur le respect du principe de proportionnalité. En matière de profilage utilisant des systèmes d'IA travaillant sur des mégadonnées, cette présomption risque d'être plus difficile à tenir. À cette première réflexion, il est utile me semble-t-il que le consentement ne soit pas systématiquement invoqué mais, comme déjà dit, que d'autres causes de licéité du traitement soient préférées. Ainsi, l'application de systèmes d'IA peut être proposée par les opérateurs de certains services contre des avantages en nature ou financiers. Par exemple, celui qui accepte le profilage publicitaire bénéficiera d'un accès gratuit à une plateforme musicale. Par ailleurs, la personne peut souhaiter recevoir de sa plateforme musicale un service de conseil personnalisé en fonction de son profil calculé par des algorithmes de profilage et se voir guider dans le choix des morceaux. Dans de tels cas, et cette solution a notre préférence, faut-il, dans ces cas, interdire en principe le consentement ? Faut-il dans ces cas réclamer que seules les autres causes de validité soient invocables, qu'il s'agisse tantôt de la nécessité d'exécution d'un contrat ou des mesures précontractuelles, tantôt de l'intérêt légitime de l'opérateur qui trouvera, dans certains cas, dans les trois apports ou plus-value de l'IA : la sécurisation, l'optimisation et l'objectivation, des justifications supplémentaires au traitement à condition que ces justifications l'emportent sur l'intérêt et les libertés de la personne concernée.

Un autre exemple, l'assurance *one to one*, proche des exemples que nous venons d'évoquer, amène cependant d'autres considérations. Prenons le cas d'un candidat souhaitant assurer les risques liés à sa conduite automobile qui se voit promettre par un assureur un important rabais sur ses primes d'assurance à calculer par un système d'IA, à condition que l'assuré permette à ce dernier d'avoir accès aux données émises par différents capteurs placés sur son véhicule, par ailleurs voiture intelligente qui ralentit automatiquement en fonction des prescrits de circulation routière[161]. Faut-il considérer que dans ces cas, le consentement donné par le candidat à l'assurance, voire les nécessités d'exécution du contrat valident le traitement ? L'individualisation des conditions contractuelles en fonction des risques présentés par chacun et calculés « objectivement » par le système heurte le principe de la mutualisation des risques, pilier de notre système d'assurance et sa généralisation impacte l'ensemble de la population assurée. Autre exemple : des systèmes de reconnaissance faciale détectent automatiquement l'état de fatigue des conducteurs et certains peuvent imposer alors l'arrêt de la conduite. On conçoit que ces systèmes pourraient être prônés voire imposés par la loi ou, de manière plus insidieuse mais tout aussi efficace, par les compagnies d'assurance, et ce au nom de la sécurité publique de nos routes. Faut-il suivre cette voie sans qu'il y ait eu débat

(161) Le cas de l'assurance santé *one to one* est plus évident encore. On peut imaginer que les compagnies d'assurance imposent l'utilisation de *body implants* ou de bracelets intelligents mesurant automatiquement le rythme cardiaque, la pression artérielle, le fonctionnement de la mémoire, *etc.*, afin de déterminer la prime d'assurance.

l'*European Data Protection Board* (EDPB), héritier du Groupe de l'article 29[169] : « The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application »[170]. Dans le cadre du projet européen[171] de « *reverse* PSI » qui consiste à permettre le transfert de données d'entreprises et de particuliers au profit d'autorités publiques (B2G), et ce à des fins d'intérêt général comme la recherche médicale, l'amélioration de la mobilité ou la protection de l'environnement, le consentement au transfert de données individuelles au sein de mégadonnées qui pourront être exploitées par les autorités publiques est certes prévu, mais à nouveau devrait être fortement encadré par la loi, selon les rédacteurs du projet. Le consentement ne peut être une base suffisante pour justifier le traitement par l'autorité publique de telles données. Il importera que le traitement auquel se réfère ce consentement puisse s'opérer dans le cadre de missions précises et à des conditions qui permettent le respect plein et entier du RGPD. Certes, on peut imaginer que ce consentement soit une condition du partage B2G des données. Dans ce cas, comme le note la recommandation de l'EDPB citée au paragraphe précédent :

> « Fair and ethical data use », « Data should be shared and used in an ethical, legitimate, fair and inclusive manner, with full respect for the choices made by individuals on how their data can be used ».

En guise de conclusions

La légitimité du consentement, présenté comme la consécration ultime de l'autonomie des individus, résiste mal à la constatation de la perte de contrôle effectif que chacun de nous ressent vis-à-vis de traitements de plus en plus opaques, de flux de plus en plus nombreux, complexes et impliquant des acteurs divers dont certains disposent d'une puissance informationnelle sans commune mesure avec celle des premiers temps de l'informatique. Ces acteurs disposent aujourd'hui d'outils dont le fonctionnement, à défaut de rendre transparents, de prédire le comportement et de manipuler les individus, prétend avec force pouvoir le faire. Dans ce contexte, quelle peut être encore la place du consentement ? Elle est loin d'être négligeable dans la mesure où, prises au sérieux, les exigences du RGPD mettent au centre des préoccupations à la fois les devoirs renforcés d'information et l'offre de choix aux personnes concernées, et ce en distinguant chacune des finalités poursuivies. Certes, pour arriver à ce résultat, des prescrits nouveaux seront nécessaires

(169) EDPB (CEPB en français), *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak*, 21 avr. 2020 (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf).

(170) Sur cet encadrement législatif du consentement, lire S. Parsa et Y. Poullet, *Les droits fondamentaux à l'épreuve du confinement et du déconfinement, La pandémie de Covid-19 face au droit*, Anthemis, 2020, spéc. p. 165 et s.

(171) *Towards a European strategy on business-to-government data sharing for the public interest*, Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, 19 févr. 2020. La Commission européenne a présenté, ce même 19 février, ce document comme un des éléments de sa stratégie en matière de données.

pour lutter contre l'opacité et les risques croissants engendrés par des traitements de plus en plus soutenus par l'intelligence artificielle.

Ces premières réflexions sont loin de suffire. Le consentement est une réponse individualiste qui sous-entend que la personne concernée soit en mesure de comprendre et de maîtriser les risques encourus suite, d'une part, à une collecte diffuse au sein d'un internet des objets et, d'autre part, à la circulation et au traitement de son image informationnelle, véhiculée et ensilée comme tant d'autres à l'intérieur de *big data* dont des algorithmes sortiront des « vérités ». Tel n'est pas le cas, et nous aurons besoin de plus en plus de négociations collectives[172], *multistakeholders*, arbitrées par les autorités de protection des données, afin d'assurer une maîtrise cette fois collective tant des risques individuels que court chacun d'entre nous, que des risques collectifs auxquels notre société doit faire face. Nous devrons en outre recourir à des législations réglementant, voire interdisant certains traitements. C'est dans le cadre de l'application de ces législations que notre consentement devra alors trouver à s'insérer. Au-delà, nous plaidons pour des procédures ouvertes multidisciplinaires, multipartites, à la fois préventives et continues d'évaluation des risques individuels et collectifs liés aux traitements à haut risque. Les dispositions du RGPD relatives à l'obligation pour les traitements à haut risque, prévues aux articles 34 et suivants, doivent être renforcées et élargies aux préoccupations plus collectives[173]. L'audit des systèmes doit être assuré par des auditeurs externes ; des mesures de réduction des risques doivent être étudiées et, le cas échéant, imposées ; le rapport doit être publié[174]. C'est à ce « prix » et à ces conditions que nous retrouverons confiance dans l'outil et pourrons exprimer notre consentement à nouveau libre et informé.

(172) On pourrait, ainsi, introduire l'idée d'une négociation collective des conditions d'utilisation de systèmes de *machine learning* entre associations de consommateurs et responsables de traitements, par exemple, en cas de profilage proposé à grande échelle. La même idée de négociation collective, cette fois avec les syndicats, serait de mise lorsqu'il s'agit de systèmes d'évaluation de membres du personnel ou de candidats à l'emploi. Une négociation collective nous apparaît préférable en termes de protection de la vie privée des personnes concernées que le consentement individuel de ces dernières. Le consentement individuel laisse en effet l'individu seul face à la puissance du responsable de traitement.

(173) Sur ce point, lire nos considérations *in Éthique et droits de l'homme dans notre société du numérique*, Mémoire de l'Académie royale de Belgique, mars 2020, 184 p.

(174) C'est tout le sens de la résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012[INL]).