BANQUE DES MEMOIRES

Master de Droit du Numérique
Dirigé par le Professeur Jérôme PASSA
2022

La protection des données personnelles et de la personne concernée par le consentement au traitement de données

Manel HOUD

Sous la direction de Nana BOTCHORICHVILI

La faculté n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire, ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

Je tiens à remercier Madame le Professeur Nana Botchorichvili pour sa direction bienveillante, sa présence sans faille durant cette année et autour du choix de ce sujet ainsi que ses conseils précieux.

Je remercie Monsieur le Professeur Jérôme Passa ainsi que l'ensemble de l'équipe académique pour la qualité et la diversité des enseignements prodigués cette année.

Je tiens à remercier l'ensemble de la Promotion du Master qui n'a pas manqué de rendre cette année encore plus riche et mémorable par son esprit d'équipe et son implication quotidienne.

ABRÉVIATIONS

AIPD	Analyse d'Impact à la Protection des Données
CE	Conseil d'État
CEPD	Comité Européen de la Protection des Données
CJUE	Cour de Justice de l'Union Européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
G29	Groupe de Travail « Article 29 »
RGPD	Règlement Général sur la Protection des Données`
TIA	Transfer Impact Assessment
UE	Union Européenne

TABLE DES MATIÈRES

INTRODUCTION

1. À l'ère du Big Data, la valeur de la donnée se multiplie de manière incommensurable, celle-ci devenant une arme de pointe pour toute entreprise. Force est de constater le volume inhumain de données traitées, stockées, échangées, exponentiel depuis les années 1970. La « *petite histoire du Big Data* », expression adaptée d'un article de Gil Press pour Forbes[1], est aussi ancienne que la création d'Internet. À partir de 1944, il était question de quantifier le volume d'informations, d'abord par les livres, puis les journaux, enfin par l'encodage d'une information. Après un mouvement de quantification de l'information, celui-ci laisse place à un mouvement de qualité de l'information. Ainsi, dès 1975, le Ministère des Postes et des Télécommunication japonais évoque une nouvelle ère de la société où la priorité est faite à des informations segmentées, détaillées et individualisées répondant aux besoins spécifiques de chacun[2]. En ce sens, la montée en puissance des acteurs tels que Google, Facebook, Amazon et Twitter à partir de 2005 révèle le potentiel de la donnée et la valeur économique qui en découle, à savoir, l'analyse qu'elle en déduit sur le comportement de chacun sur Internet.

2. Néanmoins, cette nouvelle ère n'est pas exempte d'inquiétudes. Dès 1975, l'auteur de « *Assault on Privacy : Computers, Data Banks and Dossiers* » Arthur Miller[3], s'inquiète du traitement par les autorités publiques et économiques de telles informations.

Dans ce sillage de prise de conscience, le Conseil de l'Europe s'empare de ces inquiétudes et soumet au vote des États membres une Convention dite « *Pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel* » en 1981[4], appelée Convention 108. Au sein de ses considérants, il est clairement énoncé qu'à l'ère de « *l'intensification* » de la circulation des données dans le cadre européen, il est « *souhaitable* », nous dirons, nécessaire, « *d'étendre la protection des droits et libertés fondamentales de chacun, notamment le droit au respect de la vie privée* […] » Par la suite, le Parlement Européen adopte une Directive[5] en date du 24 octobre 1995 dite « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ». Les considérants 2 et 3 de la Directive témoignent à cet égard d'une prise de position politique très pratique. En effet, tout en affirmant que les « *systèmes de traitement de données sont au service de l'homme »,* le législateur européen énonce que la libre circulation nécessite « *non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés* ». En plus de

[1] Gil Forbes, 2013, « *A very short history of Big Data* », Forbes.
[2] Idem.
[3] The Chicago History Museum, 1970, « *Arthur Miller and John O'Brien discuss privacy and surveillance* », Studs Terkel Radio Archive.
[4] Strasbourg, STCE 108, *Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel*, 28/01/1981,
[5] Parlement Européen, 24/10/1995, Directive 95/46/CE *relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données*.

prendre une telle position, le législateur européen n'oublie pas le contexte économique dans lequel il s'inscrit, comme l'atteste le considérant 4 [6]de la même Directive. C'est pourquoi, comme le précise le considérant 8, il est important pour les États membres d'avoir un niveau de protection des droits et des libertés équivalent, lequel est « *fondamental* » pour le marché intérieur. Dans un effort d'harmonisation et de coopération constant face à la circulation exponentielle de données personnelles, l'Union Européenne donne naissance au Règlement Général sur la Protection des Données (RGPD) en 2018.

3. Dans le prolongement des réflexions et objectifs de la Convention 108 et de la Directive de 1995, le RGPD place au centre de ses préoccupations la personne concernée par le traitement, soit l'utilisateur, l'internaute dont les données personnelles sont recueillies. Pour ce faire, son article 6 « *Licéité du traitement* », cherche à opérer un équilibre entre les intérêts du responsable de traitement, celui à qui il revient de traiter les données récoltées, et la protection de la personne concernée. Le but n'est pas d'interdire le traitement de données, ces dernières fondant une économie nouvelle, mais de l'encadrer de telle manière à protéger les données personnelles de la personne concernée et sa vie privée. Cette protection est le fil d'Ariane de la règlementation, fruit des réflexions muries 37 ans auparavant. En ce sens, de prime abord, le traitement de données à caractère personnel fondé sur le consentement de la personne concernée paraît être la plus protectrice de cette dernière. Listé en tête de l'article 6 et du considérant 30 de la Directive de 1995, il est pourtant curieux de constater que le consentement n'ait pas une place centrale dans le RGPD, selon Anne Debet, alors même que celui-ci se concentre sur les données dites personnelles[7]. N'y a-t-il pourtant rien de plus intime que ce qui a trait à soi ? N'est-ce-pas pourtant naturel pour tout un chacun de considérer qu'il faille son accord pour traiter de données le concernant, sous quelque forme soit-il ? Le consentement ne serait-il pas le moyen privilégié pour garantir un traitement loyal de données personnelles ? Pourquoi cette absence de hiérarchie ? Malgré ce regrettable constat, l'obtention du consentement, préalablement au traitement, demeure d'une importance capitale pour sa licéité.

4. C'est pourquoi le consentement englobe dans sa définition un impératif d'antériorité. En sus de cet impératif, le consentement exige d'être libre, univoque, spécifique et éclairé. L'ensemble de ces conditions édictées par l'article 7 du RGPD, « *conditions applicables au consentement* » sont interprétées par les lignes directrices du Groupe de travail « l'Article 29 » (G29)[8] ne définissent pas le consentement mais viennent l'encadrer. Le RGPD ne donne donc pas de définition précise sur ce qu'est

[6] Considérant 4, Directive 95/46/CE du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.* « *Considérant que dans la Communauté, il est fait de plus en plus fréquemment appel au traitement de données à caractère personnel dans les divers domaines de l'activité économique et sociale ; que les progrès des technologies de l'information facilitent considérablement le traitement et l'échange de ces données* ».

[7] Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018, p1.

[8] Groupe de Travail « Article 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017

le consentement, contrairement au droit civil qui s'en empare[9]. Bien que ces conditions y ayant trait paraissent dûment protectrices de la personne concernée, force est de constater qu'elles sont difficiles à transposer en réalité. D'après Nathalie Martial-Braz, Professeure de Droit Privé à l'Université Paris-Descartes, il est même illusoire de considérer que le consentement donné traduise *« une pleine et consciente acceptation systématique des conditions de traitement* [10]». Plus encore, le consentement comme base légale de traitement viendrait même déresponsabiliser le responsable de traitement tant celui-ci n'offre pas les garanties de « prise de conscience recherchées [11]». Dans le même temps, Romain Perray[12] évoque un consentement multidimensionnel et pour cause. Selon Anne Debet, celui-ci a une double casquette de protection et de dérogation[13]. Le consentement devient donc une base intéressante et un enjeu de compétitivité pour le responsable de traitement, notamment grâce aux cookies et aux taux de consentement qui en découlent. Le choix d'opter pour le consentement serait-ce donc une ruse pour inclure la personne concernée dans son propre traitement et éviter au plus les contestations, ou fondamental désir de traiter loyalement les données, conformément à l'article 5 du Règlement ?

5. En tout état de cause, le consentement comme base légale d'un traitement de données à caractère personnel est répandu, sûrement pour des raisons de commodité. En effet, à première vue, il est confortable pour un responsable de traitement d'opter pour cette base légale. Il lui suffirait de suivre l'article 7 du RGPD : être en mesure de démontrer qu'il a obtenu le consentement de la personne concernée, distinguer la demande de consentement en des termes clairs, permettre le retrait du consentement obtenu librement. De plus, il lui suffirait de respecter les dispositions de l'article 9 pour traiter des données sensibles, dont il est autorisé à ce faire s'il obtient le « *consentement explicite* » de la personne concernée. Or, les conditions énoncées par les articles 7 et 9 du RGPD suscitent différentes interrogations quant à la teneur des obligations qui pèsent sur le responsable de traitement d'abord et la définition même du consentement ensuite. Comment définir le consentement ? Qu'entend le RGPD par « *consentement explicite »* ? Est-il possible d'assimiler les obligations traditionnelles du droit civil à celles du responsable de traitement ? Quelles sont la nature de ces obligations ? Lui sont-elles opposables par la personne concernée ? Vont-elles varier selon le traitement de données en cause ? Serait-ce possible de dessiner le régime des obligations incombant au responsable de traitement ? Qu'en-est-il en pratique ?

[9] Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique,* PUF, 12ème édition mise à jour « Quadrige », 2018, p.544.
[10] Nathalie Martial-Braz*, Droit des Données Personnelles, les spécificités du droit français à l'égard du RGPD*, Dalloz, 2019, p.143.
[11] Idem.
[12] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.11
[13] Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018.

6. La réponse à ces interrogations est nécessaire pour comprendre si l'équilibre désiré par le RGPD entre les intérêts de la personne concernée et du responsable de traitement est effectif et permet une protection pleine et entière de la partie délivrant ses données. Au regard de l'importance de la donnée allant des domaines statistiques à sensibles, l'analyse de cette protection est essentielle à la compréhension de la collecte quotidienne et systématique de données et alerte aussi chacun sur sa propension à y consentir librement. Toutes ces questions peuvent être réunies au sein de l'interrogation suivante : le consentement au traitement de données à caractère personnel tel que régi par le RGPD permet-il une protection pleine et entière de la personne concernée ?

7. Pour répondre à cette problématique, l'étude sera conduite en deux parties successives. La première partie sur le régime du consentement (*Partie 1*) permettra dans un premier temps d'étudier la définition du consentement (*I*), laquelle sera observée à la lumière de la manifestation de volonté en droit civil (*A*) puis selon les conditions strictement énoncées en la matière (*B*). Par la suite, il conviendra d'analyser les exigences du consentement comme base légale (*II*), analyse qui ambitionnera de déterminer les obligations de forme (*A*) et de fond (*B*) incombant au responsable de traitement en la matière.

La seconde partie envisagera d'appliquer les démonstrations de la première à la pratique (Partie 2). Cette pratique sera divisée en deux catégories, dichotomie inspirée d'une expression utilisée pertinemment par le G29. Ainsi, dans un premier temps, il conviendra d'étudier le consentement dans les *domaines ordinaires (I)* à savoir, les cookies, dont l'importance est capitale dans notre étude et le ciblage de la personne concernée (*A*), puis le transfert de données personnelles (*B*). Par la suite, il sera possible d'envisager les *domaines critiques* spécifiques, expression utilisée par le G29 (*II*), laquelle se concentrera sur la règlementation des mineurs (*A*) et sur les données sensibles de l'article 9 (*B*).

PARTIE 1 – LE RÉGIME DU CONSENTEMENT COMME BASE DE TRAITEMENT

8. Le RGPD, précédé par la Convention 108 dite « *Pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel* » ainsi que par la Directive du 24 octobre 1995 dite « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* », a vocation à assurer la protection des personnes concernées dans le traitement de leurs données à caractère personnel. Son considérant premier ajoute même qu'il s'agit là d'un droit fondamental[14], bien qu'il précise par la suite qu'il ne s'agisse pas là d'un droit absolu[15], soumis donc au principe de proportionnalité.

9. Cette soumission au principe de proportionnalité est utile à notre étude et la motive. En effet, bien qu'il soit utilisé dans le cadre de l'interprétation juridictionnelle et contentieuse, ce principe est transposable en matière de consentement et plus particulièrement dans les rapports entre personne concernée et responsable de traitement. Quelle est la place de la personne concernée donnant son consentement au traitement de ses données à caractère personnel dans le rapport entretenu avec le responsable de traitement ? Lorsque celle-ci donne son consentement, est-elle oubliée ? Quelles sont les garanties que le responsable de traitement doit mettre en œuvre pour assurer un consentement licite et protéger la personne concernée ? Au regard de la lettre des considérants 1 du RGPD et 2 de la Directive du 24 octobre 1995[16], protéger les personnes physiques dans le traitement de données est fondamental, et celles qui octroient leur consentement à un responsable de traitement sont d'autant plus vulnérables. De ce fait, il est important d'extraire des textes et recommandations un régime du consentement et de la relation personne concernée/responsable de traitement qu'il entraîne.

10. Il sera question dans cette première partie d'esquisser ce régime en traitant dans une première section de la définition du consentement puis, dans une seconde section, des exigences du consentement et des obligations qu'elles font naître.

SECTION 1 – DÉFINIR LE CONSENTEMENT

11. Comme énoncé en introduction, le consentement n'est pas défini *per se* dans le RGPD. Plutôt, celui-ci est encadré par des critères : il n'est donc pas défini pour ce qu'il est, mais pour ce qu'il

[14] Considérant 1 RGPD **: «** *La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental […]* »
[15] Considérant 4 RGPD, *« Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité […]* »
[16] Considérant 2, Directive 95/46/CE *relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, « considérant que les systèmes de traitement de données sont au service de l'homme […]* ».

doit être, et comment il doit être. Ces critères énoncés par l'article 4 du RGPD, explicités par les lignes directrices WP259 du G29[17], sont au nombre de cinq. Ainsi, le consentement doit être libre, univoque, spécifique, éclairé et préalable au traitement de données.

12. Avant de les analyser, il convient malgré tout de s'interroger de prime abord sur la place du consentement dans un traitement de données à caractère personnel. À l'instar du droit civil, dont les théories subjectivistes font reposer l'acte juridique sur la « *manifestation de la volonté*[18] », le RGPD offre la possibilité de faire reposer le traitement de données sur le consentement. Ce parallèle permet, avant d'étudier les critères du consentement et leur pertinence (II), d'interroger le fondement général du consentement comme base légale d'un traitement de données à caractère personnel et la place de la personne concernée dans cette hypothèse (I).

I. Le consentement comme manifestation de volonté

13. Que dit le droit sur le consentement ? Alors que l'article 4 du RGPD et 2 de la Directive du 24 octobre 1995 offre une définition similaire du consentement, laquelle est étoffée par des conditions précises, le droit civil offre une conception proche mais aux aboutissants intéressants notre sujet.

14. Ainsi, Gérard Cornu, dans son Vocabulaire Juridique, définit le consentement comme « *l'accord d'une ou plusieurs volontés en vue de créer des effets de droit […]* [19]». Le Professeur ajoute dans la même définition que la rencontre de ces volontés est un contrat. Cette définition rappelle celle de l'acte juridique qui est défini comme la *« manifestation de volonté des individus accomplies aux fins de produire un effet juridique* [20]» selon le Professeur François Terré.

15. À la manière du droit civil qui considère la rencontre des manifestations de volonté comme un acte juridique, ou un contrat, le fruit de la rencontre du consentement de la personne concernée et la volonté du responsable de traitement serait le traitement de données dans le RGPD. À reprendre la définition donnée par le droit civil, le traitement de données serait un acte juridique ou même un contrat. C'est en posant ce parallèle qu'il devient pertinent d'interroger la relation entre la personne concernée et le responsable de traitement et questionner la protection de la partie vulnérable.

[17] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017.
[18] G. RIPERT et J. BOULANGER, *Traité élémentaire de droit civil d'après le traité de M. Planiol*, 2e éd., t. 1, no 561. Aussi, Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique,* PUF, 12ème édition mise à jour « Quadrige », 2018, p.77.
[19] Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique,* PUF, 12ème édition mise à jour « Quadrige », 2018, p.544.
[20] François Terre, Philippe Simler, Yves Lequette, François Chénedé, *Droit civil, Les obligations*, 12e éd., Précis Dalloz 2019, p.6.

Cette conception subjectiviste du droit civil à l'égard de l'acte juridique s'approche de la volonté protectrice du RGPD à l'égard de la personne concernée.

16. De son côté, l'article 4 du RGPD reprend des expressions identiques à celle énoncée par la Directive du 24 octobre 1995 à son article 2 : « *toute manifestation de volonté* » et « […] *que des données à caractère personnel la concernant fassent l'objet d'un traitement*. » Mis en parallèle avec la définition apportée par la doctrine civiliste, le regard apporté sur le traitement de données à caractère personnel comme pouvant être un contrat est fondé. Le consentement RGPD n'est donc pas substantiellement différent du consentement du droit civil. Le RGPD objectivise le consentement en rappelant son contexte juridique ou sa finalité légale : le traitement de données à caractère personnel.

17. À la lumière de ce parallèle, il n'est donc pas étonnant que le consentement puisse fonder un traitement de données à caractère personnel, tant la manifestation de volonté vient fonder une relation contractuelle. Nous dirons même que le consentement vient légitimer le traitement de données. Les premières lignes du considérant 30 de la Directive du 24 octobre 1995 laissent présager cette interprétation : *« considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement* [...] ». Le terme « *en outre* » laisse imaginer qu'en plus d'une autre base de traitement, il est nécessaire d'obtenir le consentement de la personne concernée. Maladresse du législateur européen ou désir de hiérarchie ? La Commission Nationale de l'Informatique et des Libertés (CNIL), dans une délibération n°2020-046 en date du 24 avril 2020 portant avis sur le projet d'application mobile « *StopCovid* » se prononce et dit clairement qu'il n'y a pas de hiérarchie entre les bases légales[21]. Anne Debet, qui optait déjà pour ce constat en 2018, énonce que cette absence est dommageable pour la personne concernée et ses droits fondamentaux[22].

18. Cependant, définir le consentement comme une simple manifestation de volonté n'est pas suffisant en la matière. En effet, contrairement au droit civil où cette rencontre des volontés laisse place à un acte juridique dominé par l'autonomie des volontés, un traitement de données à caractère personnel ne tend pas à laisser cette dernière s'exprimer. C'est pourquoi le RGPD vient préciser, plus encore que son prédécesseur, les conditions de cette manifestation de volonté particulière.

[21] CNIL, Délibération n°2020-046, 24 avril 2020, p.6 : « *Elle rappelle que le droit de la protection des données à caractère personnel n'établit aucune hiérarchie entre les différentes bases légales* [...] »
[22] Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018, p.37-44.

II. Les critères du consentement dans le RGPD

19. Le RGPD, précédé par la Directive du 24 octobre 1995 qui fit de même, instaure des conditions au consentement. C'est d'ailleurs sûrement plus nécessaire en la matière que de définir le consentement comme étant une manifestation de la volonté. La définition de la manifestation de la volonté, bien qu'utile, ne peut être complète sans une appréhension claire des conditions du consentement. Celles-ci sont indissociables de sa définition.

20. Ainsi, la Directive du 24 octobre 1995 définissait en son article 2.h) le consentement comme étant : « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données personnelles la concernant fassent l'objet d'un traitement* ».
Cette définition large imposait alors trois conditions : le consentement devait être libre, spécifique et informé.

21. Le RGPD quant à lui définit le consentement en son article 4.11 comme étant : « *toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des données personnelles la concernant fassent l'objet d'un traitement*. »
Il y a une différence avec la définition de la Directive du 24 octobre 1995. En effet, la définition donnée par le RGPD ajoute une condition de fond et une exigence de forme du consentement. S'agissant de l'exigence de forme, « *un acte positif clair* », celle-ci sera commentée en Section 2 de cette première partie. S'agissant de la condition de fond selon laquelle le consentement doit être « *univoque* », celle-ci sera aussi commentée en Section 2 de cette première partie, étant donné qu'il est difficile de dissocier le caractère univoque du consentement de l'acte positif clair.

Ainsi, il convient désormais de commenter les conditions du consentement dans l'ordre de l'article 4.h) du RGPD : le consentement doit être libre, spécifique et éclairé.

A. Un consentement libre

22. Pour être valable, le consentement doit être libre. Cette condition n'est pas nouvelle en droit, tant elle n'est pas sans rappeler l'article 1140 du Code Civil.[23] Avant de revenir sur cette comparaison avec ce vice du consentement qui interroge les conséquences d'un traitement fondé sur un consentement non valable, il faut définir ce qu'est un consentement libre d'après le RGPD.

[23] Code Civil, Art.1140 : « *Il y a violence lorsqu'une partie s'engage sous la pression d'une contrainte qui lui inspire la crainte d'exposer sa personne, sa fortune ou celles de ses proches à un mal considérable*. »

23. D'après les lignes directrices WP259 du G29, « *l'adjectif libre implique un choix et un contrôle réel pour les personnes concernées* »[24]. Dans son avis 15/2011 WP187 sur la définition du consentement, le G29 énonce que le consentement n'est libre que si la personne concernée ne subira pas de conséquences négatives et néfastes si elle refuse de consentir.[25] Cette approche de G29 sur le consentement libre comme étant l'expression d'un choix réel n'est pas sans rappeler la conception civiliste et de sa théorie des vices du consentement. Ainsi, il est possible de rapprocher cette interprétation du G29 à l'article 1140 du Code Civil qui traite de la violence. Sans parler explicitement de consentement vicié, le G29 parle d'un consentement non valable du fait d'une contrainte ou d'une crainte venant de la personne concernée. Il est clair, à la lumière de cet avis, que le consentement peut être vicié et qu'il est, à cet égard, de la même nature qu'un consentement de droit civil.

De même, le G29, dans le WP131[26], indique à juste titre que le « *recours au consentement doit être limité aux cas où la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice*. »

En ce sens, le Comité Européen à la Protection des Données (CEPD), donne un exemple intéressant dans ses lignes directrices adoptées le 4 mai 2020. En effet, il énonce qu'une application ne pouvant fonctionner sans le consentement de l'utilisateur ne permet pas un consentement libre de celui-ci[27]. Cette interprétation fort intéressante se comprend aisément au regard de la définition donnée par le G29 de l'adjectif libre, soit « *un choix* ». Si l'utilisateur ne peut utiliser son application qu'en consentant, c'est qu'il n'a pas le choix de consentir et qu'il n'est donc pas libre. Le préjudice subi serait l'impossibilité pour lui de recourir à cette application. Cette hypothèse n'est pas rare en pratique, encore plus avec la pratique des cookies qu'il conviendra d'étudier ensuite.

Concernant le « *contrôle réel* », il est permis de penser qu'il s'agisse de la possibilité pour la personne concernée de pouvoir d'abord contrôler sa propre volonté à consentir. Ensuite, il est permis de penser qu'il s'agisse d'un contrôle réel sur les données qu'elle consent à partager au responsable de traitement, pour quelles finalités et les droits qu'elle peut exercer en conséquence. Cette interprétation est liée aux autres conditions du consentement ainsi qu'aux obligations qui incombent au responsable de traitement en ce sens. En effet, le consentement doit être éclairé, la personne concernée doit donc savoir quelles données la concernant feront l'objet du traitement. De même, le consentement de la personne concernée doit être spécifique, elle doit donc savoir dans quel cadre et pourquoi ces données sont collectées. Ces éléments sont nécessaires à un contrôle dit réel : autrement, sans tous ces éléments, il se pourrait que le contrôle soit considéré comme vicié.

---

[24] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.6.

[25] Groupe de Travail « Article 29 », WP187, Avis 15/2011 sur la définition du consentement, 13 juillet 2011, « *Le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement.* », p.14.

[26] Groupe de Travail « Article 29 », WP131, repris de l'avis 15/2011 sur la définition du consentement, 13 juillet 2011.

[27] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, pt.3.1, p.8

24. La liberté du consentement n'implique pas seulement un choix et un contrôle réel. En effet, le consentement ne doit pas être non plus déséquilibré. Dans ce cas, le consentement est considéré comme « douteux ». [28]Le considérant 43 du RGPD prévoit en ce sens que : « *Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable de traitement [...]* ». Les lignes directrices WP259 du G29 parlent de « déséquilibre des rapports de force ».[29] Ce déséquilibre peut s'analyser sous différents prismes : celui des autorités publiques et celui du contexte professionnel [30] . Ces prismes dépendent du responsable de traitement, sa nature et son degré d'influence.[31]

25. Il existe un déséquilibre des rapports de force dès lors que le responsable de traitement est une autorité publique. En effet, le considérant 43 du RGPD prévoit que lorsque le responsable de traitement est une autorité publique, « [...] *il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière [...]* ». Cette conception se comprend aisément : puisqu'une autorité publique n'est pas considérée comme un acteur « normal » de la vie économique du fait de ses prérogatives de puissance publique face à une personne morale, il semble difficile de considérer que celle-ci soit considéré comme un acteur normal, équilibré, face à une personne physique. Dans ce cas précis, la personne concernée n'aura en effet pas consenti librement au traitement de ces données, d'autant plus qu'elle est privée de contrôle, puisque celle-ci ne pourra objecter aux conditions de traitement. En ce sens, l'article 6 c) et e) du RGPD prévoient des bases de traitement plus appropriées aux autorités publiques : l'intérêt légitime et le traitement nécessaire à une mission d'intérêt public. Cette alternative est plus intéressante et respecte la position de l'avis WP131 expliquée plus haut.

Le G29, dans son avis WP187, expliquait déjà pourquoi le consentement n'était pas la « *base juridique adéquate* [32]». Il donne alors un exemple fort pertinent qui démontre la complexité du recours au consentement pour le traitement de données par les autorités publiques. Il prend l'exemple des autorités répressives en précisant que celles-ci « *ne pouvaient se prévaloir du consentement de la personne concernée pour prendre des mesures qui n'ont pas été prévues ou qui ne seraient pas autrement autorisées par la loi* ». Le consentement vient limiter la marge de manœuvre des autorités mais le raisonnement inverse est aussi juste. En effet, la personne concernée qui consent à se voir certaines mesures légales appliquées ne pourrait se prévaloir de l'absence d'autres mesures légales

[28] Nathalie Martial-Braz*, Droit des Données Personnelles, les spécificités du droit français à l'égard du RGPD*, Dalloz, 2019, p.157.
[29] Groupe de Travail de l'Article 29, WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.6.
[30] Groupe de Travail de l'article 29, WP48, Avis 8/2001 *sur le traitement des données à caractère personnel dans le contexte du travail,* 13 septembre 2001.
[31] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.34.
[32] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.17.

auxquelles elle n'aurait pas consenti pour ne pas se les faire appliquer en cas de faute. Couplé à l'exigence de spécificité, l'on sent que le consentement n'est pas le fondement le plus approprié et susciterait nombre de contentieux.

Cependant, il existe toujours des situations dans lesquelles le consentement reste la base la plus appropriée, notamment lorsqu'un lycée demande aux élèves si ce dernier est autorisé à divulguer leurs résultats du baccalauréat ainsi que leur nom sur le site internet de l'école ou dans le journal communal. Il serait difficile ici de faire valoir l'intérêt légitime du responsable de traitement étant donné que l'établissement peut exécuter ses missions sans ces informations. C'est pourquoi le consentement demeure une base de traitement utilisable pour l'autorité publique et même pertinente, dès lors que les élèves ont fait un choix ne les privant pas de l'enseignement de leurs professeurs.

Cette question est intéressante au vu des débats autour de l'open data. Dans ce cas, il est plus favorable à l'autorité publique agissant comme responsable de traitement de faire valoir les bases des articles 6.c) et 6.e) du RGPD.

26. Il existe un déséquilibre des rapports de force en matière professionnelle, plus particulièrement dans les relations de travail entre un employeur et un employé. Le contrat de travail étant caractérisé en droit par un lien de dépendance économique et un rapport de subordination, la question de l'octroi d'un consentement libre par la personne concernée, en l'espèce le salarié, est intéressante. L'avis WP249 rendu par le G29 qui traite explicitement du traitement de données personnel sur le lieu de travail énonce en ce sens, du fait du lien de dépendance économique caractérisant le contrat, que « *les employés sont très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement [...] Compte tenu du déséquilibre du pouvoir, les employés ne peuvent donner leur consentement que dans des circonstances exceptionnelles, dans lesquelles l'acceptation ou le rejet d'une proposition n'a aucune conséquence.* »[33]

Encore plus que lorsque le responsable de traitement est une autorité publique, les conséquences néfastes d'un refus de consentir à un traitement de données sur le lieu de travail sont ressenties plus rapidement et surtout directement par la personne concernée. C'est en ce sens que le consentement ne constitue pas dans ce cas une base de traitement juste pour la personne concernée. Dans l'avis WP249 cité précédemment, le G29 est catégorique en allant jusqu'à dire que le fondement du traitement « *ne doit pas être le consentement des employés* »[34].

En ce sens, une sanction a été rendue par l'autorité grecque de protection des données à l'encontre d'une société. En l'espèce, les employés d'une société ont déposé une plainte auprès de l'autorité grecque de protection des données à l'encontre de leur employeur qui basait le traitement de

[33] Groupe de Travail de l'Article 29, WP249, Avis 2/2017 sur le traitement de données sur le lieu de travail, adopté le 8 juin 2017, p.27.
[34] Idem, p.7.

données des employés sur le consentement. L'autorité s'est prononcée en faveur des employés en énonçant que le consentement en l'espèce ne permettait pas de répondre aux exigences de l'article 5 du RGPD, notamment sur la transparence et la licéité du traitement[35]. De plus, il s'avérait que la société avait menti sur la base de traitement et avait caché la vraie aux employés, ce qui va à l'encontre du principe de transparence. Elle ajoute que le consentement n'est pas un fondement valable en matière de relation de travail.[36] L'autorité a sanctionné la société par une amende de 150 000€.

Il existe évidemment, à l'instar des autorités publiques, des situations dans lesquelles le consentement est un fondement licite en matière de relation de travail. Cependant, pour reprendre les termes du G29, celles-ci sont « *exceptionnelles* ». La CNIL évoque cet exemple sous le prisme d'un clip promotionnel dans un espace de travail où le consentement des employés serait un fondement juste, tant et si bien que le refus n'ait pas de conséquences néfastes sur eux[37]. En tout état de cause, même en cas de situations exceptionnelles, le consentement sera considéré, à juste titre par prudence et faveur à la partie faible, comme étant douteux.

27. L'interprétation du règlement par les autorités de protection des données et par le G29 s'agissant de la liberté du consentement permet de protéger au mieux la personne concernée grâce à un cadre limité d'acception. Ces interprétations sont en faveur de la personne concernée, considérée ici comme une partie faible, ce qui lui offre un plus haut degré de protection.

B. Un consentement spécifique

28. Pour être valable, le consentement doit être spécifique. C'est une exigence commune au RGPD et à la Directive du 24 octobre 1995. En l'absence de détails au sein même de la Directive, le G29, dans son avis 15/2011 WP 187, précise que le consentement ne pouvait pas être « *général* » ou « *s'appliquer à un ensemble illimité d'activités de traitement* ». [38]

Le RGPD, dans son article 5.1b), précise que les données ne peuvent être collectées que pour des « *finalités déterminées, explicites et légitimes*. » Le consentement doit donc être spécifique à ces mêmes finalités pour être cohérent et licite. C'est la position qu'adopte le G29 dans ces lignes directrices[39]. À la lettre de cet article, le législateur semble esquisser une obligation reposant sur le responsable de traitement, laquelle sera analysée en seconde section de cette étude.

---

[35] Summary of Hellenic DPA's decision n°26/2019, "*has unlawfully proceeded the personal data of its employees in an unfair and non-transparent manner contrary to provisions of Article 5(1) indent a) of the GDPR since it used an inappropriate legal basis".*

[36] Idem, "*Consent of data subjects in the context of employment relations cannot be regarded as freely given due to the clear unbalance between the parties".*

[37] CNIL, délibération n°2019-160, 21 novembre 2019, portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel.

[38] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.19.

[39] Groupe de Travail de l'Article 29, WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.14.

Les lignes directrices du CEPD du 4 mai 2020, reprenant les dispositions des lignes directrices WP259 du G29, énoncent que la spécificité du consentement doit être garantie par le responsable de traitement. C'est ainsi que ce dernier doit garantir « *la spécification des finalités en tant que garantie contre tout détournement d'usage / le caractère détaillé des demandes de consentement / la séparation claire des informations liées à l'obtention du consentement des données des informations concernant d'autres sujets.* »

Ces garanties mises en œuvre par le responsable de traitement seront analysées dans la prochaine section comme étant des obligations auxquelles il doit se soumettre.

Ces caractéristiques de la spécificité du consentement se comprennent aisément et sont en parfaite cohésion avec les exigences de liberté et de clarté. En effet, un consentement spécifique permet plus de clarté qui permet un meilleur contrôle et un réel choix venant de la personne concernée. Ceci est aussi protecteur de la personne concernée tant son consentement est limité à des finalités précises, ce qui la protège d'autres usages.

C. Un consentement éclairé

29. Le consentement doit être éclairé. Auparavant, au sein de la Directive du 24 octobre 1995, l'adjectif utilisé était « *informé* ». Ceci impliquait que la personne concernée devait être informée, avant de consentir, des caractéristiques du traitement[40]. S'agissant des informations à communiquer, il conviendra de les analyser en seconde section de cette partie.

Désormais, cette exigence d'information est renforcée par la définition du RGPD en substituant « *informée* » par « *éclairé* ». Ces deux termes similaires n'ont pourtant pas la même force : être éclairé sous-tend une notion de conscience que n'a pas l'information. Ce renforcement est commenté par le CEPD dans ses lignes directrices qui lie cette condition aux principes directeurs du RGPD dont un en particulier, à savoir, la transparence[41]. Le CEPD ajoute que la fourniture d'informations aux personnes concernée préalablement au traitement est « *indispensable afin de leur permettre de prendre des décisions en toute connaissance de cause, de comprendre ce à quoi ils consentent et par exemple d'exercer leur droit de retirer le consentement* ». Cette interprétation est fort intéressante puisqu'elle traite des droits de la personne concernée qu'elle ne peut exercer effectivement sans comprendre le traitement de ses données, compréhension qui passe par un « *consentement éclairé* ». Il ajoute enfin que sans ça, le « *contrôle de l'utilisateur serait illusoire et que le consentement ne constituera pas une base valable pour le traitement* ». [42]

---

[40] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.60.

[41] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, pt.3.3, p.16

[42] Idem.

30. Cette exigence du consentement éclairé n'est pas étrangère au droit tant elle n'est pas sans rappeler l'article 1132 du Code Civil qui traite de l'erreur. En effet, pour poursuivre le parallèle qui a guidé la définition de la manifestation de la volonté puis de caractère libre du consentement, à considérer que le traitement de données est pour le RGPD ce que l'acte juridique est en droit civil, il se peut que le consentement soit vicié du fait d'une erreur. L'erreur en matière de RGPD peut être de fait : par exemple, la personne concernée peut s'être trompée sur l'identité du responsable de traitement. À l'inverse, il peut s'agir d'une erreur de droit : par exemple, le responsable de traitement qui manque de mentionner le droit d'accès sur sa page. De ce fait, pour reprendre l'expression du CEPD, le contrôle de la personne concernée est alors « *illusoire* » et ne peut permettre un consentement valable, du fait d'une erreur découlant d'un manque d'information.

La question de savoir si l'erreur est provoquée ou non est toute aussi intéressante, auquel cas il ne s'agirait plus d'une erreur mais d'un dol, conformément à l'article 1137 du Code Civil.
Il est intéressant d'opérer un parallèle entre les dispositions du Code Civil et du RGPD pour mettre en lumière tant les obligations qui découlent des conditions inhérentes au consentement que les possibles conséquences d'un consentement non valable. En droit des contrats, la sanction est évidente : la nullité[43]. Cependant, le RGPD ne fait pas état de sanctions similaires, si ce n'est de changer de fondement.

D. Conditions supplémentaires en cas de consentement explicite

31. Le droit des données personnelles impose parfois l'obtention d'un « *consentement explicite* » pour le traitement de certaines données. Né dans la Directive du 24 octobre 1995, à l'époque sous l'adverbe « *indubitablement* »[44], le consentement explicite est défini par le G29 dans son avis WP187 n°15/2001 comme ayant le même sens qu'un « *consentement exprès* ». Cette comparaison faite par le G29 manque de clarté au vu de l'ajout par le RGPD de l'exigence d'un « *acte positif clair* »[45]. La jurisprudence de la Cour de Justice de l'Union Européenne (CJUE) dans l'arrêt Planet49[46], laquelle parle de « *consentement actif* » puis du Conseil d'État (CE), qui assimile directement le consentement explicite au consentement standard, [47]viennent brouiller la clarté de la supposée différence entre consentement « standard » et consentement « explicite ». Le caractère libre, éclairé, spécifique, univoque, tous exprimés dans un acte positif clair, semblent déjà être un consentement explicite. L'expression de la CJUE de « *consentement actif* » entre déjà dans cette définition par l'exigence d'un « *acte positif* ». Ce parallèle au « consentement exprès » n'est pas satisfaisant. Il aurait été préférable

[43] Code Civil, Article 1131 : « *Les vices du consentement sont une cause de nullité relative du contrat.* »
[44] Directive 95/46/CE *sur la protection des données à caractère personnel,* 24 octobre 1995, Article 26.
[45] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.28.
[46] CJUE, *Affaire C-673/19, Verbraucherzentrale Bundesverband eV contre Planet49 GmbH, considérants 54 et 62.* + CJUE, Communiqué de Presse n°125/19, « *Le placement de cookies requiert le consentement actif des internautes.* »
[47] CE, 19 juin 2020, n°430810, Société Google LLC, « *le consentement libre, spécifique, éclairé et univoque ne peut qu'être un consentement exprès de l'utilisateur donné en toute connaissance de cause et après une information adéquate sur l'usage [...]* »

d'opter pour une comparaison au droit de la consommation, par exemple avec l'obligation de « double-clic » ou de parler de consentement dynamique.

Les lignes directrices du CEPD viennent adoucir cette complexité dans ses lignes directrices en précisant qu'en matière de consentement explicite, il convenait de mesurer « *les efforts complémentaires qu'un responsable de traitement devrait entreprendre [...]* »[48] pour l'obtenir. Il ajoute que la personne concernée doit « *formuler une déclaration de consentement exprès* [49]», Ce paradigme est plus satisfaisant puisqu'il laisse penser que l'important, en matière de consentement explicite, soit la forme du consentement et l'information relative à celui-ci. In fine, le consentement explicite serait un consentement standard qui devient explicite par la forme et l'information qui l'entourent. Alors que le G29 dans son avis 15/2011 préférait un écrit pour attester d'un consentement explicite[50], l'évolution de la notion telle qu'expliquée par Anne Debet[51] tend à affaiblir cette préférence pour des raisons tant pratiques que juridiques, d'autant plus qu'un consentement explicite donné oralement a été jugé valide en 2020 grâce aux garanties et efforts mis en œuvre par le responsable de traitement, bien qu'il ait commis une faute en cochant par avance la case que devait cocher la personne concernée sur la conservation des données dans le contrat[52]. Cette évolution de paradigme laisse penser que la position du CEPD concernant les efforts complémentaires du responsable de traitement est la plus satisfaisante pour comprendre l'intérêt d'un consentement explicite, intérêt qui nécessite une étude quant à la forme du consentement et les obligations du responsable de traitement en la matière. Cependant, l'ampleur de la protection de la personne concernée donnant son consentement explicite, au regard de celle donnant son consentement standard, reste floue, d'autant plus que les conséquences d'un consentement invalide sont encore à déterminer.

32. En conclusion de cette première section, il est possible de remarquer à quel point les conditions du consentement viennent l'encadrer en théorie. C'est ainsi que la personne concernée peut être effectivement protégée tant les interprétations du CEPD et du G29 optent pour un paradigme clair et défenseur de la personne concernée. Le parallèle effectué avec le droit civil permet de mettre en lumière l'importance du consentement de la personne concernée dans la relation entretenue avec le responsable de traitement, notamment à travers les vices du consentement et ses conséquences.

[48] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, pt.3.3, p.20.
[49] Idem.
[50] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.218.
[51] Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018, p.8.
[52] CJUE, affaire C-61/19, *Orange Romania SA c/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal.* 11 novembre 2020.

SECTION 2 – LES EXIGENCES DU CONSENTEMENT COMME BASE DE TRAITEMENT

33. La définition du consentement a été démontrée ci-dessus. Celle-ci est encadrée par des conditions pertinentes qui esquissent les contours d'un régime du consentement. Pour poursuivre le parallèle avec le droit civil, lequel guide cette première partie, il conviendra d'analyser dans un premier temps les exigences liées à la forme du consentement (I) pour ensuite étudier les exigences de fond du consentement (II).

I. L'exigence de forme du consentement

34. Si le contrat civil a un *negotium*, celui-ci a aussi un *instrumentum*. L'instrumentum correspond au support matériel qui constitue la preuve du negotium, c'est-à-dire le contenu. La condition prévue par le RGPD qui correspondrait le mieux à cet instrumentum a été brièvement présentée ci-dessus et sera ici plus amplement commentée. Il s'agit de l'exigence « *d'acte positif clair* », énoncée à l'article 4 du RGPD. C'est d'ailleurs à travers cet acte positif clair que se traduit le caractère univoque du consentement : c'est par la matérialisation de l'acte pris librement, spécifiquement et de manière éclairée que peut être traduit l'exigence d'univocité.

L'acte positif clair est l'unique exigence explicite de forme inscrite par le RGPD. Mais quelle forme revêt-il ? Cette exigence ne semble pas à première vue requérir une forme précise : il n'est pas indiqué, « une déclaration écrite claire » par exemple. Dans l'article 7 du RGPD concernant les conditions du consentement, le législateur requiert que la demande de consentement soit dans une forme qui la « *distingue des autres questions* ». Pour Romain Perray, l'acte positif clair se traduit par une « *démarche délibérée* »[53]. Cette explication va de pair avec l'exigence de liberté du consentement : un acte délibéré est la traduction d'un choix et d'un contrôle. L'adjectif choisi par le Maître est très pertinent et révélateur. La CNIL tranche en ce sens sur son site en précisant que cet acte ne doit laisser place à « *aucune ambiguïté* [54]». Ces interprétations vont de pair avec les lignes directrices du CEPD qui prévoient que l'acte positif clair ne doit laisser aucun doute sur le consentement de la personne concernée[55]. L'acte positif clair doit être sans équivoque, donc, univoque.

35. Ces précisions, bien qu'utiles à la compréhension de l'exigence, ne suffisent pas à définir la forme de l'acte positif clair. Peut-être que la souplesse de cette exigence est un choix permettant au responsable de traitement d'opter pour la forme qui lui est la plus appropriée, mais il est

[53] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.21.
[54] CNIL, *Conformité RGPD, comment recueillir le consentement des personnes ?* 3 août 2018, www.cnil.fr
[55] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.18.

certain qu'en matière de relation dématérialisée, la forme est un outil de protection satisfaisant et important pour la partie la plus vulnérable. Le droit de la consommation et des contrats électroniques en sont des exemples pertinents, notamment par l'exigence du double-clic[56] qui serait très utile en la matière pour protéger et responsabiliser la personne concernée. Cette possibilité renforcerait sans doute encore plus la condition de liberté et de clarté du consentement, puisque le contrôle de la personne concernée serait renforcé tant elle serait guidée par le responsable de traitement à prendre connaissance une nouvelle fois des informations. Le Professeur Oliver Cachard, sur le double clic, énonce que celui-ci peut « *fragiliser le contrat électronique* »[57]. Cependant, en la matière, il ne semble pas que cette exigence soit un frein au consentement comme fondement légal de traitement, bien au contraire. Cette exigence serait un atout tant pour la personne concernée que le responsable de traitement : la personne concernée est responsabilisée et agit en pleine conscience, ce qui réduit l'erreur et les plaintes contre le responsable de traitement, ce qui est un avantage pour lui. Cette exigence est d'autant plus un atout qu'elle permet de dissiper toute ambiguïté. Le CEPD dans ses lignes directrices l'évoque partiellement dans un exemple en parlant de répéter un mouvement[58].

La forme permet de dissiper l'ambiguïté en cas de doute, d'autant plus que le G29 dans son avis 15/2011 évoque la situation. Il précise qu'en cas de « *doute raisonnable*[59] », le consentement n'est pas traduit par un acte positif clair. Utiliser le prisme de la personne raisonnable n'est peut-être pas le plus approprié pour protéger la personne concernée. En revanche, instaurer plus de sévérités quant à la forme de l'acte positif clair le serait. Il est alors important de prêter attention aux interprétations des autorités et juridictions en la matière afin d'établir au mieux la protection de la personne concernée.

36. Ces premières explications permettent de déceler les cas dans lesquels un consentement est valide, car univoque, des cas dans lesquels à l'inverse, celui-ci est invalide.

Les déclarations écrites sont un exemple d'acte positif clair. Bien que rare en matière numérique[60], il est évident que c'est un instrumentum de choix. Les lignes directrices du CEPD, reprenant à ce titre les lignes directrices WP259 du G29, énoncent que les déclarations écrites sont un instrumentum valides qui « *[...] peuvent adopter de nombreuses tailles et formes [...]* ». Le considérant 32 du RGPD accepte même la voie électronique, ce qui laisse penser que l'écrit électronique serait acceptable aussi. Cette interprétation permet de confirmer le paradigme de souplesse de l'acte positif clair.

---

[56] Code Civil, Article 1369-2 alinéa 1er:« *Pour que le contrat soit valablement conclu, le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation.* » V. Aussi, Alinéa 3 : « *[...] la confirmation de l'acceptation [...]* ».
[57] CEJEM, Oliver Cachard, *Validité et formation du contrat électronique dans la LCEN*, 9 octobre 2003, www.cejem.u-paris2.fr
[58] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.19.
[59] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.23.
[60] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.22.

Le consentement donné oralement peut aussi traduire un acte positif clair. Comme énoncé plus haut, la CJUE[61] s'est prononcée sur la question d'un consentement donné oralement. En l'espèce, une société avait obtenu oralement le consentement de ses clients sur la conservation de leurs données pendant la période précontractuelle grâce à un nombre importants d'informations données. Cependant, lors de la conclusion du contrat, la société avait préalablement coché la case destinée au client concernant la conservation des données. La CJUE retient par application du considérant 32 du RGPD que le consentement obtenu oralement est valide et traduisait un acte positif clair dès lors que le responsable de traitement avait fourni au moment de l'obtention du consentement toutes les informations nécessaires. Or, le fait pour lui d'avoir pré-cocher les cases destinées au client dans le contrat excluait le caractère libre du consentement et n'était donc pas valide, alors même que le client y avait consenti oralement auparavant. Le consentement donné oralement est donc admis dès lors que le responsable de traitement met en œuvre toutes les garanties nécessaires à sa licéité.

Quid du consentement résultant du comportement ? Le G29, sous l'empire de la Directive du 24 octobre 1995, admettait cette possibilité dès lors que le comportement était non-équivoque[62]. Cette conception rappelle en droit civil le mécanisme de la tacite reconduction où les parties continuent d'exécuter leurs obligations alors même que le contrat est arrivé à son terme[63], voire même le commencement d'exécution : le comportement traduit une manifestation de volonté, ici, la volonté de consentir. Cependant, cette possibilité appelle à la vigilance et mériterait d'être corroborée par un autre acte pour renforcer la protection autour de la personne concernée, notamment au regard du principe de spécificité du consentement. En effet, la personne concernée peut se comporter de telle manière à ce que le responsable de traitement suppute le consentement général alors même que la personne concernée se comportait comme tel pour une finalité seulement.

37. Malgré cette souplesse, nombreux sont les cas où le consentement ne traduit pas un acte positif clair.

Tel est le cas des cases à cocher par défaut, qui ne sont pas rares en matière numérique. Ces cases à cocher par défaut sont souvent utilisées en matière de cookies, ce qu'il conviendra d'analyser en Partie 2 de cette étude. Cette conception est aisée à comprendre. En effet, une case à cocher par défaut viole la liberté du consentement, ce qui empêche ce dernier d'être traduit par un acte positif clair, car ni positif, ni clair.

Le silence ou l'inactivité ne traduit pas non plus un acte positif clair, puisque ceux-ci ne traduisent pas un acte positif, mais une abstention. Romain Perray nuance cette idée à travers la

[61] CJUE, affaire C-61/19, *Orange Romania SA c/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal.* 11 novembre 2020.
[62] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.26.
[63] Code Civil, Article 1215 : « *Lorsqu'à l'expiration du terme d'un contrat conclu à durée déterminée, les contractants continuent d'en exécuter les obligations, il y a tacite reconduction. Celle-ci produit les mêmes effets que le renouvellement du contrat* »

dichotomie suivante : il y a soit, absence de comportement de la personne concernée, soit il existe un comportement qui est passif[64]. La CJUE rejoint cette position dans l'affaire Planet 49[65] concernant les cookies en énonçant « *qu'il est impossible de déterminer de manière objective si l'utilisateur d'un site internet a effectivement donné son consentement au traitement de ses données personnelles en ne décochant pas une case cochée par défaut [...]* ». Il sera possible de revenir plus tard dans l'étude sur ce point. Dans le sillage des cases à cocher par défaut, il y a une difficulté avec la condition de liberté du consentement et la manifestation de volonté. L'acte n'est ici pas clair.

Il en va de même pour l'utilisation du service et de la navigation pour les mêmes raisons. Bien qu'auparavant la poursuite de la navigation constituait un consentement valable du fait du comportement de la personne concernée comme étant un soft opt-in[66]dans le cadre de la Directive ePrivacy de 2002, la CNIL change de position. En effet, elle exprime désormais clairement que le fait de « *continuer à naviguer sur un site web, d'utiliser une application mobile ou bien de faire défiler la page d'un site web ou d'une application mobile ne constituent pas un consentement valide* »[67]. Cette position est reprise par les lignes directrices du CEPD qui précise que dans ce cas, il est difficile de distinguer le consentement possible d'une autre activité de l'utilisateur. Ainsi, le consentement manque d'univocité et de spécificité.

Le consentement doit être spécifique, c'est pour cela qu'un consentement dit groupé ou en bloc[68]ne traduit pas un acte positif clair. Le CE s'est prononcé en faveur de cette interprétation dans un arrêt rendu à l'encontre de Google, toujours en matière de cookies[69]. C'est d'ailleurs dans ce contexte que les plus grandes sanctions de la CNIL ont été rendues.

Dans ce sillage, il en va de même pour l'acceptation des conditions générales d'un contrat. Le CEPD tranche en cette faveur et pour cause : le consentement n'est ici pas libre et ne peut traduire un acte positif clair au traitement de données à caractère personnel[70]. La CNIL s'est prononcée en ce sens dans une délibération précédant l'arrêt du 19 juin 2020 du CE contre Google, où elle précise qu'accepter les conditions d'utilisation d'un site (en l'espèce, Google) pour ensuite y créer son compte utilisateur n'est pas un consentement valable. Ceci se comprend parfaitement au regard de la liberté et la clarté du consentement : les conditions générales d'utilisation du site sont souvent opaques et induisent une fatigue informationnelle chez l'utilisateur. Cet élément ne permet pas une manifestation de volonté claire

---

[64] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.27.

[65] CJUE, *Affaire C-673/19, Verbraucherzentrale Bundesverband eV contre Planet49 GmbH*, considérant 62, 1 octobre 2019.

[66] Nathalie Metallinos, *Le RGPD apporte-t-il de réels changements sur la place du consentement ?* Communication Commerce Électronique n°7-8, Juillet 2018, comm.58.

[67] CNIL*, Délibération n°2019-093 portant de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs),* 19 juillet 2019.

[68] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.30.

[69] CE, 19 juin 2020, n°430810, Société Google LLC, « *un consentement recueilli de manière globale pour l'ensemble des finalités [...] ne peut être valide.* »

[70] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.18.

puisque les informations sont presque dissimulées, ce qui est dangereux pour la protection de la personne concernée.

Il revient alors au responsable de traitement d'être diligent, ce qui prête à penser qu'il existe des obligations que le responsable de traitement doit respecter pour un consentement valide, notamment une obligation d'information.

II. Les exigences de fond du consentement

38. Pour que le consentement soit valide, les conditions qui lui sont inhérentes doivent être remplies. C'est au responsable de traitement qu'il revient la charge de les garantir. Reposent donc sur ses épaules des obligations de deux ordres qui, à la lecture de l'article 7 du RGPD, s'imposent comme des obligations de résultat. Il a des obligations tenant au traitement de données personnelles puis des obligations tenant à l'exercice et la garantie des droits de la personne concernée, plus particulièrement le droit de retrait du consentement.
Au sein de la première catégorie, il y a une obligation d'information, traditionnelle, qu'il est possible de trouver sur les épaules de tout contractant en droit. Ensuite, pèse sur lui une obligation de preuve ou de « *démontrabilité*[71] » du consentement qui s'attache plus amplement à la forme.
Au sein de la seconde catégorie se trouve l'obligation pour le responsable de traitement de permettre l'exercice des droits de la personne concernée, à savoir, le droit de retrait du consentement.

A. Les obligations tenant au traitement de données

39. La première des obligations du responsable de traitement est l'obligation d'information. Connue du droit civil notamment[72], celle-ci est essentielle au caractère libre et éclairé du consentement. Pour rappel, la liberté du consentement est traduite par un « *choix réel* » et un contrôle de la personne concernée. Pour contrôler des informations, il faut les obtenir. Quant au caractère clair du consentement, celui-ci tient à la quantité mais aussi à la qualité des informations transmises. Suivant cette dichotomie, il conviendra d'étudier d'abord la quantité et la nature des informations transmises pour ensuite s'intéresser à leur qualité.

40. Les informations devant être transmises sont nombreuses, d'abord du fait de l'existence d'une liste arrêtée d'informations devant être transmises, puis du fait de l'obligation de détailler chaque

[71] Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales, p.5
[72] Code Civil, Article 1112-1 : « *Celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant*. »

finalité pour laquelle le traitement de données est poursuivi. L'obligation d'information n'est donc pas uniquement liée à la condition de clarté du consentement, mais aussi à la spécificité du celui-ci et plus généralement à l'obligation de transparence[73] du traitement de données. C'est pourquoi cette obligation est sûrement la plus importante et celle à laquelle le responsable de traitement doit faire très attention.

Le CEPD, dans ses lignes directrices reprenant les lignes WP259 du G29, fait une liste non limitative des informations devant être transmises par le responsable de traitement quand il recueille le consentement de la personne concernée. Cette liste, d'une « *grande précision*[74] », note les « *éléments cruciaux*[75] » pour garantir le choix réel de la personne concernée. Ainsi, l'on retrouve parmi ces informations requises, l'identité du responsable de traitement, la durée du traitement, la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité, les types de données collectées et utilisées, l'existence du droit de retrait du consentement, les informations concernant la prise de décision automatisée, les informations sur les risques éventuels lors du transfert de données en l'absence de décision d'adéquation et de garanties appropriées, l'identité du responsable de traitement des opérations de lecture ou écriture, la finalité des opérations de lecture ou écriture de données, la manière d'accepter ou de refuser les traceurs ainsi que les conséquences qui s'attachent à un refus ou une acceptation des traceurs.

Les informations sont donc nombreuses, un avantage pour la protection de la personne concernée mais un risque pour elle d'être noyée d'un un amas d'informations qu'elle ne peut pas toujours comprendre aisément. L'avantage pour le responsable de traitement est de clairement limiter son champ d'action en cas de responsable conjoints ou de présence de sous-traitant, bien que cette délimitation n'entraîne pas de limitation de la responsabilité puisque l'article 82 du RGPD instaure une responsabilité in solidum. L'autre avantage de cette obligation d'information pour le responsable de traitement est expliqué par Fabrice Mattita à travers cet adage latin[76] : *Nemo videtur fraudare eos, qui sciunt et consentiunt*. En effet, l'obligation d'information est une garantie pour le responsable de traitement contre le retournement de la personne concernée contre lui. Cette dernière ne pourra pas invoquer une asymétrie d'information, une tromperie contre le responsable de traitement si celui-ci a fait preuve de toutes les diligences. L'usage par le Professeur de cet adage romain permet de prolonger le parallèle effectué avec le droit des contrats en usant de la figure des vices du consentement. Il est donc permis de penser que la personne concernée puisse être victime d'un dol ou d'une erreur provoquée du fait d'une information trompeuse ou mensongère.

S'agissant des modalités de l'information, celles-ci sont essentielles à la garantie d'un consentement éclairé. Elles sont exprimées à l'article 7 du RGPD qui prévoit que chaque demande de

[73] RGPD, Article 5.a).

[74] Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7.12.2020, p.61.

[75] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.15.

[76] Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales, p.6.

consentement doit être rédigée « *en des termes clairs et simples »*. L'information ne doit donc pas être obscure, c'est-à-dire alourdie ou même dissimulée par d'autres informations. De même, les termes utilisés sont capitaux. Ainsi, ils doivent être assez précis pour correspondre à l'information transmise, mais assez vulgarisés pour permettre à chacun de la comprendre. Sur ce point, le CEPD dans ses lignes directrices[77] énonce que « *un message devrait être facilement compréhensible pour l'homme de la rue et pas uniquement par les avocats.* » et qu'en ce sens, une politique de confidentialité rédigée de manière laborieuse truffée « *d'énoncés riches en jargon juridique* » n'était pas une information délivrée en des termes clairs et simples. Cette exigence est d'intérêt public et est la pierre angulaire de la protection de la personne concernée par le consentement. Si le responsable de traitement ne permet pas à celle-ci de comprendre les informations déterminantes à son consentement, alors le traitement de données est illicite et déloyal. La personne concernée se retrouverait dans une illusion de contrôle et de choix dangereuse qui laisserait libre le responsable de traitement d'agir à sa guise. Cette illusion de contrôle est dangereuse pour la relation personne concernée/responsable de traitement tant elle crée un déséquilibre certainement manifeste des rapports de force qui nuit à l'objectif du RGPD.
Il est donc nécessaire d'adapter l'information à la personne concernée et plus particulièrement au public concerné. C'est ici qu'il est possible d'interroger la pertinence du consentement comme fondement d'un traitement de données à caractère personnel, notamment dans des domaines visant un public vulnérable. Une information présentée distinctement, accessible, en des termes clairs, est-elle toujours gage de protection et de garantie d'un consentement donné librement, spécifiquement et clairement ? Cette question sera développée en deuxième partie de l'étude.

41. La seconde obligation incombant au responsable de traitement lorsqu'il fonde son traitement sur le consentement est l'exigence de preuve ou de démontrabilité[78] du consentement. Cette exigence est posée explicitement par l'article 7 du RGPD qui exprime en ce sens qu'il revient au responsable de traitement de démontrer que la personne concernée a bien donné son consentement. Dit autrement, il revient au responsable de traitement de prouver que la personne concernée ait consenti au traitement de ses données personnelles. Cette disposition sécurisante pour la personne concernée va à l'encontre de l'adage latin classique « *actori incumbit probatio* ». En effet, en cas de contentieux, la personne concernée qui prétend ne pas avoir donné son consentement n'a pas à apporter la preuve de son allégation, celle-ci revenant sur le responsable de traitement. La charge de la preuve est ainsi inversée. Cette charge de la preuve ne vaut pas qu'en contentieux puisqu'il s'agit là d'une obligation générale qui précède un litige. Ainsi, systématiquement, le responsable de traitement doit pouvoir,

[77] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.18.
[78] Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales, p.8

contentieux ou non, démontrer tant à la personne concernée qu'à tout autre demandeur que le consentement a été obtenu correctement, et ce à tout moment.[79]

Cette exigence est essentielle à la protection de la personne concernée tant l'objet de la preuve est ici double et lui bénéficie. En effet, la démonstration du responsable de traitement doit matérialiser « *l'acte positif clair* » mais aussi les conditions de fond du consentement, tenant à son caractère libre, spécifique et éclairé. La démonstration est donc une « *garantie* »[80] s'attachant aussi bien à la forme du consentement qu'au fond, à savoir, la pleine conscience de la personne concernée. C'est pourquoi cette exigence permet une protection efficace de la personne concernée lorsque celle-ci consent au traitement de données. Cette disposition est aussi protectrice du responsable du traitement lorsqu'il y a des sous-traitants ou un cas de responsable conjoint de traitement.

S'agissant de la forme de la preuve, les lignes directrices WP259 du G29 précisent que les responsables de traitement sont « *libres de développer des méthodes adaptées à leurs opérations quotidiennes [...]* »[81]. Cette interprétation est le corollaire de l'exigence de forme du consentement qui requiert un « *acte positif clair* », sans spécifier une typologie d'acte à respecter. En ce sens, le RGPD maintient une certaine souplesse au bénéfice du responsable de traitement, sans oublier la protection de la personne concernée. Le CEPD évoque dans ses lignes directrices une exigence minimale que reprend la CNIL. La démonstration doit montrer l'horodatage du consentement[82]. La forme de la preuve est donc libre, mais elle reste soumise à une limite principale que le CEPD évoque dans ses lignes directrices. Le respect de cette exigence de démontrabilité ne peut conduire le responsable de traitement à récolter plus de données que nécessaires, ce qui va de pair avec le principe de minimisation des données.

Les conséquences d'une preuve non valable ou insuffisante sur le traitement de données ne sont pas claires. En effet, puisque cette exigence incombant au responsable de traitement figure dans l'article 7 du RGPD tenant aux conditions de validité d'un consentement, il est permis de penser qu'un consentement qui respecterait toutes les autres conditions mais où la démonstration faille ne peut être considéré valable et permettre le traitement de données voire la poursuite de ce traitement. Il conviendrait donc de supprimer les données collectées. Cette analyse est partagée par Maître Noémie Weinbaum[83] et un arrêt de la CJUE reprenant une sanction de l'autorité roumaine de protection des données. Cette sanction d'interdire de traiter les données ou de supprimer les données va de pair avec l'obligation de traitement loyal et transparent des données personnelles.

---

[79] CNIL*, Délibération n°2019-093 portant de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs),* 19 juillet 2019

[80] Nathalie Martial-Braz*, Droit des Données Personnelles, les spécificités du droit français à l'égard du RGPD*, Dalloz, 2019, p.158.

[81] Groupe de Travail de l'Article 29, WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.14

[82] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.23.

[83] Nathalie Weinbaum, *La preuve du consentement à l'ère de la Blockchain*, La Semaine Juridique, entreprises et affaires n°10, 2018, p.28-32.

42. Le responsable de traitement a donc, *in fine*, une obligation de loyauté envers la personne concernée. Cette obligation de loyauté est décrite par l'article 5 du RGPD qui énonce que les données à caractère personnel doivent être traitées notamment de manière loyale[84]. Ce principe peut être lu comme une obligation d'ordre public, encore plus lorsque le consentement est la base légale d'un traitement de données. En effet, la relation entre la personne concernée et le responsable de traitement devient une relation de confiance et intime qui se rapproche le plus d'un contrat de droit civil. En ce sens, à la lumière des principes des articles 1104 et 1194 du Code Civil, le responsable de traitement doit traiter les données de bonne foi et s'engager auprès de la personne concernée dans ce sillage et ne pas dépasser les limites qu'il instaure lors du recueil du consentement, conformément au principe de spécificité de celui-ci. Autrement, il ferait preuve de mauvaise foi et de déloyauté. Le manquement à cette obligation de loyauté constituerait une faute, un abus dans la relation entre le responsable de traitement et la personne concernée qui ouvre un droit à réparation, droit que le responsable de traitement ne peut interdire, empêcher ou contourner. Cette réparation peut s'appuyer sur un recours juridictionnel et/ou par l'exercice d'un droit que le RGPD consacre, solutions qui toutes deux viennent sanctionner à leur manière le manquement constitué par la faute qui ici, s'analyserait comme une faute contractuelle.

B. Les obligations tenant à l'exercice des droits de la personne concernée

43. Le droit de retrait du consentement est un droit de la personne concernée qui tient au caractère éphémère du consentement, lequel est une manifestation de l'intime d'une personne. La Directive du 24 octobre 1995 n'avait pas expressément prévu cette possibilité. C'est la Directive 2002/58 du 12 juillet 2002 dite Directive ePrivacy qui s'empare de ce droit en précisant en son article 9 que les personnes concernées pouvaient « *à tout moment* »[85] retirer leur consentement et « *interdire temporairement* » le traitement de leurs données personnelles. Les personnes concernées n'ont pas à motiver leur demande de retrait. La demande de retrait peut être motivée par une volonté qui disparaît ou pour sanctionner un comportement jugé déloyal par la personne concernée. Le consentement a donc un caractère « *précaire* »[86] qu'il convient de prendre en compte lors du choix de base de traitement. Ce caractère peut avoir des incidences plus ou moins lourdes selon le secteur d'activités et le traitement en cause, notamment en matière de transferts de données ou de recherches.

Le responsable de traitement doit permettre aux personnes concernées de retirer leur consentement, c'est en ce sens que cette obligation lui incombe. Ceci passe par une information aux personnes concernées avant qu'elles ne donnent leur consentement, eu égard du principe de

[84] RGPD, Article 5.1.a)
[85] Directive 2002/58 *concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques,* 12 juillet 2002, article 9.
[86] Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales, p.10.

transparence, et par des modalités techniques. Ainsi, la CNIL préconise, s'agissant du retrait du consentement, un parallélisme des formes[87] : lorsque le consentement est donné d'une certaine manière, il doit être retiré de la même façon. Le retrait du consentement doit être permis aussi simplement que le recueil. Ces modalités simplifiées sont appréciées *in concreto*, eu égard notamment aux nombres d'actions à mener ou au temps passé. Autrement, cela emprisonnerait la personne concernée dans un engagement perpétuel, ce qui est prohibé par le droit. La simplicité est d'autant plus de mise tant elle permet de ne pas décourager la personne concernée qui souhaiterait retirer son consentement : si elle n'y parvient pas facilement, elle peut abandonner, ce qui causerait un consentement dépourvu de volonté. Ce consentement ci ne saurait être valable et justifier un traitement de données personnelles. Le CEPD tranche en ce sens dans ses lignes directrices en précisant que si le responsable de traitement ne remplissait pas les exigences permettant un droit de retrait effectif, « *le mécanisme de consentement du responsable de traitement n'est pas conforme* ».[88]

Le caractère précaire du consentement pose la question des effets du retrait du consentement : le retrait du consentement est-il rétroactif ? Le G29 se positionne pour la non-rétroactivité du retrait du consentement[89]. Il explique sa position en soutenant qu'avant l'exercice du retrait, les données ont été légitimement collectées, du fait de l'existence d'une manifestation de volonté positive. De ce fait, il serait injuste pour le responsable de traitement que les « *décisions prises ou les processus engagés dans le passé sur la base de ces informations* » [90]soient annulées ou supprimées. La question du retrait interroge la question de la conservation des données qui est plus épineuse. La solution du G29[91] en la matière est de dire que celle-ci est possible si une autre base de traitement le justifie, autrement, il faut supprimer les données. Cette solution n'est pas pleinement satisfaisante puisqu'elle met en exergue un conflit de bases légales de traitement difficilement solvable lorsque le consentement de la personne concernée a été choisi ab initio. Le responsable de traitement pourrait alors invoquer son propre intérêt légitime, ce qui revient à minimiser le pouvoir et le contrôle de la personne concernée sur son consentement. Le responsable de traitement pourrait d'autant plus utiliser cet argument pour ne pas donner droit à une demande de retrait, en prévoyant une base de traitement secondaire qui pourrait être celle de son intérêt légitime qui viendrait s'imposer comme remplaçant dès lors que le consentement est retiré. Le droit de retrait du consentement à lui seul peut donc ne pas suffire à assoir la volonté de la personne concernée qui ne veut plus voir ses données personnelles traitées. Cette demande, dans l'intérêt de la personne concernée, devrait s'accompagner d'une demande d'opposition au traitement ou/et de suppression pour garantir plus aisément la suppression de ses données. Il reviendra au responsable de traitement d'argumenter ce pourquoi la conservation est nécessaire à son intérêt légitime. Quant à la manière de trancher, il serait intéressant d'user soit, du principe de faveur à la partie la plus vulnérable

[87] CNIL, *Conformité RGPD, comment recueillir le consentement des personnes ?* 3 août 2018, www.cnil.fr
[88] CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020, p.24.
[89] Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur la définition de consentement, adopté le 13 juillet 2011, p.37.
[90] Idem.
[91] Idem.

pour assurer sa protection, ce qui peut ne pas être équitable, soit du critère de la balance des intérêts, ce qui supposerait une analyse *in concreto* constante et causerait parfois une insécurité juridique. Plus généralement, la solution proposée par le G29 interroge le choix du consentement comme base de traitement pour un responsable de traitement et l'existence même du consentement comme base de traitement. Le droit de retrait du consentement étant un mécanisme fort en la faveur de la personne concernée, les responsables de traitement ont plutôt intérêt à considérer d'autres bases légales pour assurer la pérennité de leur traitement.

44. Le régime du consentement tel qu'étudié en cette première partie a permis de démontrer les mécanismes par lesquels la personne concernée était protégée par son propre consentement. La définition même du consentement, agrémentée de conditions strictes auxquelles le responsable de traitement doit veiller, permet dans un premier temps de garantir la pleine conscience de la personne concernée, laquelle garantit sa protection. Les obligations incombant au responsable de traitement, lesquelles sont, à la lecture des textes, de véritables obligations de résultat, viennent renforcer la position de la personne concernée en mettant sa protection au centre des préoccupations du responsable de traitement.

Cependant, la souplesse voulue par le RGPD vient assombrir ce constat. Anne Debet dit du consentement comme base de traitement que celui-ci a deux rôles : celui de protection, et celui de dérogation[92]. C'est en confrontant ces deux rôles à la pratique qu'il convient désormais d'attester de la protection de la personne concernée et ce en analysant chacune d'elle sous le prisme des exigences ici étudiées.

[92] Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018.

PARTIE 2 – L'APPLICATION DU RÉGIME DU CONSENTEMENT

45. Le régime du consentement, tel qu'étudié précédemment, permet de confirmer la volonté protectrice du RGPD à l'égard de la personne concernée. Cependant, la multiplicité des critères à remplir laisse supposer qu'il n'est pas toujours simple pour le responsable de traitement de garantir la protection pleine et entière du consentement de la personne concernée et plus largement de ses données personnelles par ce biais lors de la collecte. Ce constat peut même venir jusqu'à interroger le sens et la portée du consentement comme base de traitement.

46. Il est alors essentiel à l'étude conduite d'analyser la collecte de données fondée sur le consentement au traitement dans différents domaines. Afin d'opérer une division sensée, il convient de reprendre une catégorie décrite par le G29 dans ses lignes directrices, dite, « *domaines critiques spécifiques* »[93]. Sont comprises dans ces domaines les collectes de données de mineurs et de données sensibles. À la lumière de cette expression, il convient donc d'étudier son contraire, lequel inspire l'expression suivante : « *domaines ordinaires* ». Toujours sous le prisme de l'expression du G29, il convient d'inclure dans cette catégorie les collectes de données relatives au ciblage de la personne concernée en général et les transferts de données. Seront donc successivement étudiées les questions de la protection de la personne concernée par le consentement dans le cadre des domaines ordinaires puis dans les domaines critiques spécifiques.

SECTION 1 – LE CONSENTEMENT DANS LES DOMAINES ORDINAIRES

47. Les domaines dits ordinaires dans le cadre de l'étude font référence à l'ensemble des domaines non compris par l'expression du G29 « *domaines critiques spécifiques* ». Sont donc compris les domaines tendant à cibler la personne concernée, en établir un profil (I), puis le transfert de ces données (II). Seront donc successivement étudiés ces deux domaines.

I. Consentement et ciblage de la personne concernée

48. Est entendu par ciblage la politique menée afin de déterminer le profil ou l'usage que fait la personne concernée d'un produit ou d'un environnement. En matière numérique, les entreprises font alors usage de cookies et autres traceurs pour optimiser leur stratégie commerciale. Les entreprises peuvent aussi prendre des décisions suite à un profilage.

[93] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.27

Seront alors successivement étudiées ces deux pratiques à la lumière du consentement et des analyses menées plus haut.

A. Consentement et cookies

49. Les cookies sont définis par la CNIL comme étant des « *fichiers stockés par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est-à-dire dans la majorité des cas à l'ensemble des pages d'un même site web.*) *Ce fichier est automatiquement renvoyé par des contacts ultérieurs avec le même domaine.* »[94] La Directive dite « ePrivacy » soumet les cookies au consentement de l'utilisateur[95], laquelle convient explicitement que le consentement aux cookies a la même définition que le consentement de la personne concernée tel qu'écrit par la Directive du 24 octobre 1995[96]. En ce sens, le consentement aux cookies doit être informé, (et non éclairé qui est un critère issu du RGPD), spécifique et libre. Ces exigences sont retranscrites à l'article 82 de la Loi Informatique et Liberté. Le considérant 26 de la Directive ePrivacy prévoit elle aussi, à l'instar de la Directive de 1995 et le RGPD, un droit pour la personne concernée de retirer son consentement. Le consentement n'est cependant par requis pour tous les types de cookies. Ainsi, la Directive ePrivacy exempte donc le recueil du consentement pour les cookies dits strictement nécessaires aux fonctionnalités techniques et les cookies visant à faciliter la communication[97]. Pour tout autre cookie ne répondant pas à ses finalités, le consentement préalable au dépôt est nécessaire.

S'agissant de la nature du consentement, la CJUE s'est exprimée en la faveur du consentement explicite (ou « consentement actif »). En effet, dans une affaire « Planet49 »[98], la Cour énonce que le consentement de l'utilisateur ne pouvait être considéré comme étant valide si celui-ci devait décocher une case pré-cochée par défaut[99]. Au-delà de la terminologie insatisfaisante tel que précédemment commentée, le sens de celle-ci reste indéniablement pertinent. Dans ses conclusions, la Cour reprend tant les termes du RGPD que de la Directive de 1995 la précédant, en utilisant notamment l'adverbe « *indubitablement* »[100] pour parler du consentement. Elle ajoute que seul un consentement « *actif* » permet d'attester de ce caractère. En conséquence, les cookies non nécessaires, à savoir les cookies marketing, ne peuvent faire l'objet d'une case pré-cochée. Ainsi, la CJUE met fin à la pratique de *soft opt in* qui caractérise un consentement passif qui serait invalide au regard de l'exigence d'un acte positif clair et du caractère indubitable et actif du consentement. Malgré une terminologie peut être maladroite,

---

[94] CNIL, *Cookie*, www.cnil.fr
[95] Article 5.3, Directive 2002/58/CE du 12 juillet 2002 *concernant le traitement de données à caractère personnel et le respect de la vie privée dans le secteur des communications électroniques.*
[96] Considérant 17, Directive 2002/58/CE du 12 juillet 2002 *concernant le traitement de données à caractère personnel et le respect de la vie privée dans le secteur des communications électroniques (dite vie privée et communications électroniques),* « *[...]le consentement d'un utilisateur ou d'un abonné, que ce dernier soit une personne physique ou morale, devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive 95/46/CE. [...]* »
[97] Article 5.3, Directive 2002/58/CE du 12 juillet 2002 *concernant le traitement de données à caractère personnel et le respect de la vie privée dans le secteur des communications électroniques.*
[98] CJUE, *Affaire C-673/19, Verbraucherzentrale Bundesverband eV contre Planet49 GmbH,* 1er octobre 2019.
[99] Idem, considérant 62.
[100] Idem, considérant 54.

la position de la Cour permet assurément de protéger au mieux la personne concernée, en théorie. En pratique, la multiplication des demandes de consentement peut conduire la personne concernée à devenir de plus en plus passive, alors même que son consentement explicite est requis. L'Interactive Advertising Bureau (IAB) démontre dans son baromètre en date de la même année que seulement 56% des médias français avaient opté pour une *consent management platform valide*[101]. Les site web se dotant d'outils d'analyse tel que Google Analytics ou Matomo reposent leur existence et leur pérennité sur ces cookies marketing qui permettent de financer le site web et pour qui le consentement est un enjeu stratégique, le but étant d'avoir le meilleur « taux de consentement ». Commanders Act, dans son Baromètre 2021[102], a montré l'évolution du consentement avant le 31 mars 2021 et après, date à laquelle les organismes avaient obligation de se mettre en conformité pour laisser place à un consentement explicite. Le taux de consentement des utilisateurs a baissé de 8 points en moyenne : 15 sur terminal fixe et 4 sur mobile. S'agissant de l'information de la personne concernée, d'après une étude menée par Opinon Way[103] qui s'appuie sur le comportement de presque onze millions d'internautes, celle-ci est difficilement satisfaisante : les utilisateurs visualiseraient 1,8 fois le message de consentement avant de procéder à leur choix, ce qui veut dire que la décision est prise instantanément, à la première visualisation. Plus encore, seulement 0,1% des utilisateurs atteignent la page des paramétrages de cookies. L'étude générale montre que plus le consentement est explicite, plus les entreprises ont du mal à l'obtenir. L'étude menée par Converteo en 2021 est claire : les entreprises optent pour différentes stratégies pour garantir un taux de consentement élevé en utilisant différentes fenêtres de cookies.[104] Voilà pourquoi les cookies marketing sont aussi importants et motivent les responsables de traitement à contourner cette obligation de consentement explicite et l'information qu'il implique en faveur d'une pratique encore plus contestable qui sera commentée plus tard dans ce développement.

50. Malgré ce cadre clair et cet effort de la CJUE en faveur de la protection de la personne concernée et de la vie privée, le dépôt de cookies continue de fournir un contentieux très riche, notamment contre les contrôleurs d'accès, et pour cause. Les données sont aujourd'hui un enjeu à la fois pro-concurrentiel et restrictif de concurrence, ce qui pose problème. Alec Burnside vient jusqu'à dire que la législation en matière de protection de la vie privée ne suffit pas à elle-même en matière numérique étant donné que le consentement de la personne concernée au traitement de données est constamment mis à mal[105]. Ce constat est naturel et juste : si le cadre légal se suffisait, alors les atteintes au consentement de la personne concernée ne serait pas aussi nombreuses. La jurisprudence des autorités

[101] Idem, reprenant le Baromètre de l'IAB.
[102] Commanders Act, *Baromètre Privacy 2021*, 17 juin 2021, www.commandersact.com
[103] Fair and Smart, *collecte des consentements sur internet : un état des lieux encourageant mais à améliorer*, 3 janvier 2019, reprenant le sondage Opinion Way en date de 2018, www.fairandsmart.com
[104] Converteo, Livre Blanc 2021, *Baromètre, taux de consentement à mi-septembre 2021,* www.converteo.com
[105] Alec Burnside, V. OCDE DAF/COMP/M(2016)2/ANN2/FINAL 8 juin 2017, traduit de l'anglais. « *[...] privacy law alone may not suffice, since we observe in digital markets constant violations of the fundamental principle that data should be only used for the purposes that the individual (data subject) consented to. »*

nationales a alors un grand rôle à jouer pour maintenir la protection de la vie privée face à ces géants d'internet. La CNIL s'inscrit alors dans une stratégie globale de mise en conformité au sein de laquelle, entre 2020 et 2021, elle a adopté environ 70 mesures correctrices en matière de cookies. Ces mesures sont à 60% destinées à ces contrôleurs d'accès et ont donné naissance à des sanctions de grande importance[106]. Ainsi, le CE, dans un arrêt en date du 28 janvier 2022[107], confirme la sanction prise par la CNIL à l'encontre de Google à hauteur de 100 millions d'euros[108]. L'arrêt est rendu au visa de l'article 82 de la Loi Informatique et Liberté et énonce que la CNIL était compétente en la matière, que celle-ci avait jugé à bon droit que Google n'avait pas offert une information claire et complète aux utilisateurs, n'avait pas recueilli préalablement leur consentement et ne leur avait pas offert un mécanisme efficace et aussi simple d'opposition aux cookies. De plus, le Conseil d'État ajoute que le montant de 100 millions infligé n'était ni supérieur à la limite fixée par la Loi Informatique et Liberté, ni disproportionné au regard des bénéfices générés par Google et ses cookies publicitaires. Le communiqué de presse du CE mentionne un fait intéressant et révélateur de la philosophie des responsables de traitement : durant la procédure de contrôle effectuée par la CNIL, Google a changé ses pratiques, mais pas de manière à fournir les informations explicites et claires requises sur les finalités de ses cookies et de la façon de s'y opposer.

Or, le consentement aux cookies doit être informé, spécifique et libre. En l'espèce, le consentement de la personne concernée ne respecte pas deux de ces conditions : il n'est ni informé, ni spécifique. In fine, le critère de liberté peut lui aussi être contesté puisque celle-ci est conditionnée par les informations données par le responsable de traitement qui, *in casu*, ne permettent pas d'agir en pleine conscience. Google s'adonne à une dissimulation d'informations tout en rendant exhaustif, difficile et décourageant le processus d'opposition aux cookies, ce qui engage la personne concernée vers une fatigue informationnelle. Pour rappel, retirer son consentement doit être aussi simple que de l'accorder : s'opposer aux cookies doit être aussi simple que d'y accepter[109]. C'est la raison pour laquelle Google, aux côtés de Facebook, est de nouveau sanctionnée par la CNIL dans une délibération en date du 31 décembre 2021[110]. Le responsable de traitement vient en un sens limiter sa contestabilité, donc sa responsabilité, à l'égard de la personne concernée, ce qui nuit fortement à la liberté du consentement. En conclusion, le consentement est invalide, perd de sa force protectrice, alors même que celle-ci est préservée en théorie par la CJUE.

51. Les contrôleurs d'accès ont une tendance à passer outre les exigences des autorités. Ceux-ci peuvent se permettre de payer de lourdes amendes qui, au regard du bénéfice qu'ils génèrent

[106] CNIL,*Cookies : sanction de 50 000 euros à l'encontre de la SOCIÉTÉ DU FIGARO,* 29 juillet 2021, www.cnil.fr
[107] CE, 28 janvier 2022, n°449209.
[108] CNIL, délibération SAN-2020-012, 7 décembre 2020.
[109] CNIL, *Refuser les cookies doit être aussi simple qu'accepter : mise en conformité de tous les organismes mis en demeure et actions à venir de la CNIL,* 29 juin 2021, www.cnil.fr
[110] CNIL, délibération SAN-2021-023 du 31 décembre 2021.

par le dépôt de cookies marketing, ne représentent que peu. Cependant, là n'est pas le cas d'autres acteurs privés qui dépendent beaucoup des cookies marketing et pour qui se conformer entièrement aux dispositions de la CNIL et de la CJUE peut constituer une barrière majeure. C'est ainsi que naît la pratique controversée des *cookies wall* ou mur de traceur. La CNIL définit le cookie wall comme « *le fait de conditionner l'accès à un service à l'acceptation, par l'internaute, du dépôt de certains traceurs sur son terminal (ordinateur, smartphone, etc.*) »[111]. Cette pratique commutative permet de garantir le succès de la publicité ciblée qui finance le site internet. Cet environnement participe au renforcement de l'industrie AdTech (*adverstising technologies*).

Néanmoins, cette pratique est fortement compromettante pour la personne concernée désireuse d'accéder à un service subordonné à l'obtention de ses données personnelles. Prévoyante, la CNIL prévoit dans ses lignes directrices en juillet 2019 l'interdiction pour les responsables de traitement d'opter pour le cookie wall, lequel ne permet pas un consentement conforme. Cependant, le CE, dans une décision en date du 19 juin 2020[112], annule la partie des lignes directrices interdisant le cookie wall en expliquant d'abord que la CNIL ne pouvait imposer d'interdiction générale et absolue dans le cadre d'un acte de droit souple et que ceci relevait de la compétence du législateur. Ensuite, le CE ajoute que la pratique ne mettait pas systématiquement à mal le consentement de la personne concernée dès lors que celle-ci était informée de manière spécifique pour chacune des finalités. La décision du CE, sûrement juste au regard des compétences limitées de la CNIL, reste un échec à la protection de la personne concernée qui fait de plus en plus face à cette pratique.

Face à cette annulation, la CNIL recommande aux éditeurs dans ses lignes directrices de proposer une « *alternative réelle et équitable* » permettant d'accéder au site. Cependant, dans la majeure partie des cas, l'alternative proposée par les éditeurs aux utilisateurs refusant de consentir au traitement de leurs données personnelles est pécuniaire. Le cookie wall devient un *paywall*, lequel est déjà très utilisé par différents acteurs du divertissement ou même de l'information[113]. Cette rémunération a pour but, pour le responsable de traitement, de réparer le « préjudice » subi par l'entreprise de ne pas pouvoir procéder au ciblage de la personne concernée. Pour légitimer une réparation, ce préjudice pourrait être regardé comme une perte de chance, soit la disparition actuelle et certaine d'une éventualité favorable, si les conditions sont remplies.[114]. Or, *in casu*, dans le cas du dépôt de cookies à des fins de ciblage marketing, quelle est l'éventualité favorable ? Est-ce le fait de proposer une publicité correspondant au comportement de l'utilisateur, ou de garantir le fait pour celui-ci de cliquer sur l'offre et de contracter avec le vendeur ? Dans la première hypothèse, il est donc possible de légitimer la réparation du responsable de traitement du fait de la perte de chance, mais pas dans la seconde : il est impossible de prédire sans faille l'achat. Afin de déterminer si la pratique du paywall est licite, la CNIL s'intéresse au

[111] CNIL, *Cookie walls : la CNIL publie des premiers critères d'évaluation*, 16 mai 2022, www.cnil.fr
[112] CE, 19 juin 2020, n°434684.
[113] Voir notamment les politiques de cookies de jeuxvideos.com, tf1.fr, allocine.fr.
[114] Cass. Crim., 18 mars 1975, n° 74-92118

tarif et à la question de savoir si celui-ci est raisonnable. Elle répond que ce critère est à apprécier *in concreto*.

Or, l'alternative payante ne saurait être considérée comme une alternative réelle et équitable au regard des critères du consentement. Cette pratique va à l'encontre des lignes directrices du G29 qui spécifiaient qu'un responsable de traitement ne pouvait subordonner l'accès à son site internet au consentement de la personne concernée. Cela se conçoit aisément au regard du caractère libre du consentement, lequel est ici conditionné au paiement en cas d'opposition aux cookies. Qu'importe la somme désirée par le site internet, il n'empêche que celle-ci enferme la personne concernée dans une illusion de liberté qui est dangereuse et contraire à l'esprit du consentement : l'alternative n'est donc pas réelle. De même, la question de l'audience est à soulever : une audience majeure peut être plus à même de faire un choix éclairé. Mais dans le cadre d'un site avec une audience plus jeune et vulnérable, à l'instar de jeuxvidéos.com, est-ce une pratique appropriée à la protection de la personne concernée que d'opter pour un paywall ? Les sites internet d'informations utilisant le paywall pourraient instaurer des discriminations entre les personnes refusant les cookies mais pouvant payer et d'autres refusant les cookies et ne pouvant pas payer. L'alternative n'est donc pas équitable. Le règlement ePrivacy devrait sans doute pouvoir répondre aux interrogations concernant le paywall et offrir au consentement une meilleure place et une plus large protection qui dissuade de contournement.

Le dépôt de cookies peut donc présenter un vrai danger pour la protection de la personne concernée par le consentement tant celui-ci enfreint les critères de liberté et d'information pour se nicher entre la volonté des responsables de traitement à sciemment contourner leurs obligations et la fatigue informationnelle, la lassitude qui s'empare de la personne concernée. Le consentement perd alors de sa force protectrice pour devenir un fondement plus formel et souple, ce qui est inquiétant au regard de l'importance des cookies pour les acteurs privés.

B. Consentement, profilage et décision automatisée

52. Le profilage et la prise de décision automatisée sont étroitement liés. Le premier est défini par l'article 4 paragraphe 4 du RGPD comme étant « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ». Les lignes directrices WP251 du G29[115] précisent que le profilage est alors fondé sur trois éléments : c'est un « *traitement automatisé* » effectué sur les « *données à caractère personnel* »

[115] Groupe de Travail « Article 29 », WP251, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE)2016/679, 3.10.2017, p.7.

ayant pour objectif « *d'évaluer les aspects personnels d'une personne physique* ». Cette définition du profilage ne distingue pas selon que le traitement soit automatisé ou exclusivement automatisé, ce dernier régi par l'article 22 du RGPD. En tout état de cause, l'objectif du profilage est d'évaluer les caractéristiques individuelles pour ensuite placer la personne concernée dans une catégorie prédisant son comportement actuel ou futur. C'est un traitement individualisé et personnel.

La prise de décision automatisée est définie dans les lignes directrices WP251 du G29 comme étant « *la capacité de prendre des décisions par des moyens technologiques sans intervention humaine.* »[116] . Les données utilisées peuvent être fournies directement par les personnes concernées, des données observées à leur sujet ou des données dérivées. Ces décisions automatisées peuvent être en partie automatisée ou exclusivement automatisée. La question est alors de savoir si un être humain, le responsable de traitement, intervient à quelconque moment du processus décisionnel. Le contrôle du responsable de traitement doit être significatif dans le rendu de la décision pour que le traitement ne soit pas exclusivement automatisé. Dans le cas où la décision est exclusivement automatisée, alors le régime qui s'applique est plus sévère, d'où l'intérêt d'un contrôle humain. Ces décisions automatisées produisent un effet juridique (annulation d'un contrat, refus d'un avantage social particulier accordé par la loi, etc.) ou alors affecte la personne concernée « *de façon similaire* » (entraîne la discrimination de la personne, décision affectant l'accès à l'éducation, côte de solvabilité, etc.).

Les décisions automatisées peuvent être prises sans profilage, et vice versa. Or, il est très fréquent de rencontrer le cas où les deux domaines se chevauchent, étant donné l'importance du profilage dans le rendu d'une décision automatisée pertinente. Dans son corpus, le RGPD rattache l'activité de profilage à l'article 22 du RGPD qui encadre la prise de décision automatisée. Toutes deux seront donc traitées ensemble.

53. L'article 22 du RGPD énonce que la personne concernée « *[...] a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière similaire.* » L'article 22 est interprété comme une interdiction générale afin de renforcer la protection de la personne concernée, laquelle est dans ce cas automatiquement protégée et a le contrôle sur ses données.

Néanmoins, le considérant 71 du RGPD ainsi que le paragraphe 3 de l'article prévoient des cas où un tel traitement est autorisé : lorsque le traitement est nécessaire à l'exécution d'un contrat, lorsqu'il est permis par le droit de l'Union ou d'un État membre ou lorsque la personne concernée a donné son consentement explicite[117]. Dans ce cadre, le consentement remplit donc une fonction première de

[116] Idem, p.8.

[117] RGPD, Considérant 71, « *Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis [...], ou nécessaire à la conclusion ou à l'exécution d'un contrat [...] ou si la personne concernée a donné son consentement explicite.* » V. en ce sens Article 22.3 du RGPD.

dérogation. Bien que la forme du consentement explicite tende à faire valoir la protection de la personne concernée, son opacité ne rend encore une fois pas la tâche aisée.

La lettre de l'article 22 du RGPD cristallise le caractère libre du consentement en ce qu'il prévoit explicitement que les personnes concernées peuvent ne pas faire l'objet d'une décision automatisée ou d'un profilage si elles le souhaitent. De ce point de vue la liberté est garantie.

Or, comme l'énonce les lignes directrices WP251 du G29, « *le profilage peut être opaque* », ce qui menace la validité du consentement tel qu'étudié et commenté précédemment. La Convention 108+ dédiée au profilage prévoit alors qu'il est recommandé au responsable de traitement de permettre à la personne concernée de choisir entre les différentes finalités et les degrés de profilage[118]. Elle tient alors, dans le même temps, à garantir la spécificité du consentement. De plus, dans le cadre du *machine learning* et du *deep learning*, la question de la spécificité des données utilisées est essentielle au recueil d'un consentement explicite spécifique et éclairé.

Elle insiste aussi sur l'information de la personne concernée qui doit être « éclairée » depuis le RGPD. Tout comme pour les cookies, l'information de la personne concernée conditionne le caractère libre du consentement. En ce sens, il est recommandé au responsable de traitement en matière de profilage et de décisions automatisées de s'adonner à une information on ne peut plus complète qui renforce la confiance de la personne concernée. Ceci entre dans le champ de l'obligation d'information à laquelle le responsable de traitement est soumis et qui, en matière de consentement explicite, doit être renforcée. Cette information est nécessaire en la matière, étant donné que le profilage s'appuie beaucoup sur les données dites dérivées.

Cette obligation d'information, clé d'un consentement explicite permettant le profilage et la prise de décisions automatisées légitimes, est spécifique. En plus des informations traditionnelles afférentes au droit de la personne concernée et des finalités du traitement, le responsable de traitement doit informer la personne concernée de son droit à demander une explication sur la décision prise à un être humain ainsi que des modalités permettant de contester la décision prise. Le but de cette disposition est de ne pas légitimer une décision qui serait illicite, injuste ou disproportionnée sous prétexte que la personne concernée a consenti de manière explicite au traitement. Le consentement est ici certes une dérogation, mais il ne doit pas devenir un outil d'impunité et de discrimination.

Dans le sillage de cette information particulière, l'article 35 du RGPD impose dans des cas limitatifs la réalisation par le responsable de traitement d'une analyse d'impact à la protection des données (AIPD). Celle-ci est nécessaire à l'ensemble des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dès lors que ceux-ci ont recours à de nouvelles technologiques « *compte tenu de la nature, de la portée, du contexte et des finalités du traitement* ». Suivant l'article du RGPD, la CNIL, dans une délibération 2018-327[119], prévoit qu'une AIPD est obligatoire dès lors

[118] Convention 108, T.PD(2019)07BISrev2, *Profilage et la Convention 108+ : pistes pour une actualisation 2010(13) sur le profilage,* 18 juin 2020.
[119] CNIL, Délibération SAN-2018-327, 11 octobre 2018.

qu'un traitement avec profilage est réalisé. Le CEPD opte pour des critères plus larges en imposant une AIPD dès lors que deux critères de sa liste sont remplis. Parmi eux, la prise de décision automatisée et l'évaluation/scoring. Il semblerait que dans tous les cas, l'AIPD soit requise, ce qui est un bénéfice pour la protection de la personne concernée.
L'AIPD a un lien avec l'obligation d'information du responsable de traitement puisque cette analyse mène à rapport diligenté qui n'omet aucune information substantielle intéressant la personne concernée. L'AIPD est un outil de confiance pour le responsable de traitement puisque celui-ci est soumis à l'autorité nationale de protection des données. L'AIPD est alors un outil que la personne concernée peut utiliser pour donner son consentement. La spécificité de cet outil et sa mise à disposition par le responsable de traitement pourrait servir à qualifier le consentement d'explicite, à condition que cet outil soit bel et bien lu par la personne concernée. Cependant, il n'est pas fait obligation pour le responsable de traitement de divulguer un tel document qui ne traite pas seulement de l'utilisation des données personnelles collectées mais aussi des mesures de sécurité pour faire face aux risques que le traitement pose, ce qui est dommageable lorsque le traitement est fondé sur le consentement explicite. Au vu des études menées autour des taux de consentement, la probabilité d'obtenir le consentement de la personne concernée est moindre lorsqu'elle est totalement éclairée, ce qui est nécessaire à un consentement explicite. De ce fait, le responsable de traitement peut être réticent à l'idée de partager un tel document. Or, la mise à disposition de l'AIPD à la personne concernée, si elle n'est pas une obligation, participe grandement à la transparence, la loyauté du traitement de données à caractère personnel et au principe d'accountability. La personne concernée peut exercer un vrai contrôle sur ses données et accorder un consentement libre, éclairé et spécifique.

Le profilage et la prise de décisions automatisées peut mettre la protection de la personne concernée à rude épreuve dès lors que celle-ci est mal informée. Si les responsables de traitement refusent de s'adonner à une information claire, transparente, lisible et accessible sur tous les aspects du traitement, alors il convient de dire que le consentement, même explicite, n'est pas un fondement adapté à son traitement, alors même qu'il est le plus adapté à la personne concernée. Tout comme pour les cookies, fonder le profilage ou la prise de décision automatisée sur le consentement interroge la question de l'audience, laquelle sera abordée plus tard dans cette seconde partie.

II. Consentement et transfert de données à caractère personnel

54. Le consentement est aussi entendu comme une dérogation en matière de transferts de données. Faute de définition claire, le CEPD apporte trois critères permettant de définir ce qu'est un transfert de données. Pour caractériser un transfert de données à caractère personnel, il faut qu'une entité soumise au RGPD transmette les données ou les rende disponible à une autre qui ne se situe pas dans

l'UE. En principe, l'article 46 du RGPD prohibe les transferts de données à caractère personnel et ne l'autorise qu'en présence de garanties appropriées, d'une décision d'adéquation ou de présence de règles d'entreprises contraignantes.

En cas d'absence d'une de ces options, l'article 49 énonce que le transfert de données à caractère personnel peut se fonder, notamment, sur le consentement explicite de la personne concernée. Il énonce en ce sens que le transfert peut être réalisé lorsque la personne concernée « *[...] a donné son consentement explicite, après avoir été informée de risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées.* »[120] *In casu*, le consentement explicite de la personne concernée est rattaché à une obligation d'information précise qui pèse une nouvelle fois sur les épaules du responsable de traitement. La lettre de l'article 49 permet de dessiner les contours du consentement explicite et ce de manière plus satisfaisante, en laissant penser que la nature de l'information à communiquer, spécifique à la matière requérant un consentement explicite, permet de le modéliser. Le consentement explicite serait le consentement qui nécessite une information spécifique à une matière le requérant, toujours en respectant les exigences de forme et de fond spécifiées plus haut. Il y aurait alors un consentement explicite spécifique à chaque domaine.

En la matière, le consentement au transfert de données peut ne pas être une base adéquate. Le G29 dans ses lignes directrices le précise en disant du consentement que celui-ci s'avérerait être une « *fausse bonne solution* »[121]. Cette déclaration est juste à plusieurs égards.

D'abord, le consentement s'avère être une « *fausse bonne solution* » dès lors que la personne concernée a un droit de retrait. Lorsque celle-ci l'exerce, le responsable de traitement ne peut plus ni, traiter les données, étant donné que le fondement a disparu, ni les transférer pour la même raison. De ce fait, cela impose le responsable de traitement à modifier son fondement, ce qui interroge le choix initial du consentement et l'égard apporté à la personne concernée. Le consentement n'est donc pas une solution opportune pour le responsable de traitement sur ce point.

De plus, le consentement ne se révèle pas une solution opportune pour la protection de la personne concernée. D'abord, le consentement au transfert n'est pas spécifique. Les lignes directrices du CEPD concernant les dérogations au transfert précisent qu'il est difficile de faire preuve de spécificité pour le transfert de données, notamment au vu de la possibilité de ne pas connaître les circonstances particulières du transfert au moment du recueil du consentement[122]. Il se peut aussi que le transfert soit envisagé après la collecte de données et donc après l'obtention du consentement. Ce dernier peut être reconnu non valable rétroactivement.

L'exigence de spécificité du consentement est intimement liée au caractère éclairé de celui-ci, qui, *in casu*, soulève le plus de questions. La lettre de l'article 49 est claire : la personne concernée doit être

[120] RGPD, Article 49.1.a)

[121] Groupe de l'article 29*,* WP 114, *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995,* 25 nov. 2005, p.13.

[122] CEPD, Lignes Directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p.8.

informée « des risques que le transfert peut comporter ». Les lignes directrices du G29 sur le consentement ajoutent des informations tout aussi nécessaires à fournir à la personne concernée[123] : l'identité du responsable de traitement, la finalité du transfert, le type de données, l'existence du droit de retirer son consentement et l'identité ou les catégories des destinataires. Ceci participe à définir des informations spécifiques constituant l'obligation d'information du responsable de traitement qui s'expose à une faute s'il y faillit. À titre d'exemple, l'autorité norvégienne de protection des données dans une décision rendue à l'encontre du réseau Grindr est catégorique : le « *partage de données sans base légale à de graves répercussions* »[124]. En l'espèce, l'application de rencontre par affinité de genre partageait les données des utilisateurs sans leur consentement. La situation était d'autant plus critique qu'en sus de ne pas avoir recueilli leur consentement, Grindr partageait des données sensibles liées notamment à l'appartenance sexuelle de ses utilisateurs. Le site envoyait les données à des partenaires commerciaux contre un financement de leur plateforme. L'autorité norvégienne va plus loin en affirmant que les données personnelles des utilisateurs n'étaient pas de la monnaie d'échange et qu'en l'espèce, aucun consentement n'avait été donné ni au transfert, ni au ciblage commercial.

L'information concernant les acteurs du traitement est aisée à donner, mais l'information des risques l'est moins. Toujours dans un but d'obtenir un taux de consentement élevé et parvenir au transfert, il semble inadéquat pour le responsable de traitement de donner une information trop effrayante et décourageant la personne concernée. Or, tout comme pour le profilage, cette information est nécessaire à la qualification du consentement explicite. En l'espèce, il serait intéressant de rendre accessible à la personne concernée les Transfer Impact Assessment (TIA) réalisés. À la manière de l'AIPD, le TIA a pour objectif d'opérer une analyse de risques causés par le transfert de données à caractère personnel. Bien que la CJUE ne requiert le TIA uniquement lorsque le transfert est encadré par des garanties contractuelles[125], il semble étrange que celui-ci ne soit pas imposé lorsque le transfert est fondé sur le consentement. Le TIA garantit à la personne concernée une information intègre et réelle qui permet d'éviter toute asymétrie d'information ou de manquement de la part du responsale de traitement à son obligation d'information. Sans une information complète, il est difficile pour la personne concernée d'exercer l'ensemble de ses droits tel que l'opposition ou le retrait. Cela laisse planer autour de la personne concernée une illusion de contrôle de ses données, ce qui est dangereux et contraire à l'esprit du consentement, encore plus du consentement explicite. Les lignes directrices du CEPD sont claires : si l'information en matière de risque n'est pas correctement délivrée, alors la « *dérogation ne s'appliquera donc pas* »[126]. Le consentement n'est donc pas valable. Si la divulgation du TIA peut faire peur au responsable de traitement pour des raisons de stratégie commerciale, il n'empêche que sa mise

[123] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.15.
[124] Datatislynet, 20/02136-18, 13 décembre 2021. V. aussi, NYOB, « *NCC and nyob GDPR complaints: Grindr fined €6,3 Mio over illegal data sharing."*, 15 décembre 2021, www.nyob.eu
[125] CJUE, affaire C311/18, *Data Protection Commissionner/Maximilian Schrems and Facebook Ireland*, 16 juillet 2020.
[126] CEPD, Lignes Directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p.9.

à disposition participe au principe d'accountability et de transparence dans le traitement de données à caractère personnel, ce qui favorise la protection de la personne concernée par le consentement. De plus, cette mise à disposition du TIA permet à la personne concernée d'accepter les risques en pleine conscience, ce qui vient limiter la contestabilité des actions du responsable du traitement. La mise à disposition du TIA pourrait aussi s'inscrire dans une obligation générale de sécurité qui va au-delà des obligations de l'article 24 du RGPD prévoyant l'obligation pour le responsable de traitement de mettre en œuvre des mesures techniques organisationnelles. Les mesures inscrites dans le TIA visant à pallier les risques du transfert seraient contraignantes une fois mises à la disposition de la personne concernée ayant consenti, ce qui participerait aussi à préserver son consentement explicite.

Le consentement n'est pas toujours la base la plus pertinente pour la personne concernée en la matière eu égard du principe de liberté du consentement. Que faire lorsque la personne concernée responsable de traitement n'a d'autres choix que de transférer les données ? C'est dans ce cas précis que l'argument du G29 devient intéressant : le consentement étant une « *fausse bonne solution* », il est important pour le responsable de traitement de prévoir un autre fondement qui lui permet d'assoir sa pérennité.

SECTION 2 – LE CONSENTEMENT DANS LES DOMAINES CRITIQUES SPÉCIFIQUES

55. Le consentement fait aussi office de dérogation lorsqu'il s'agit pour un responsable de traitement d'opérer un traitement de données à caractère personnel dans les domaines dits « *critiques spécifiques* » par le G29. C'est dans ce cadre que se posent les questions de la protection de la personne concernée par le consentement dans ces domaines où celle-ci peut être soit, plus vulnérable (I), soit divulguer des données à caractère personnelles particulières (II).

I. Consentement et mineurs

56. Le traitement de données à caractère personnel de mineurs est aujourd'hui d'une grande importance pour les responsables de traitement. Avec la multiplication des jeux en ligne, de l'achat par leurs représentants légaux de terminaux qui leurs sont propres, de l'usage des réseaux sociaux et de l'enseignement à distance, les mineurs n'ont jamais été autant concernés par les données à caractère personnel que de nos jours. Du fait de leur vulnérabilité et de leur consommation, il est important de préserver leur protection, ce qui peut être difficile au vu du panorama légal actuel s'agissant du consentement.

57. L'article 8 du RGPD prévoit la possibilité pour le responsable de traitement de traiter des données personnelles d'un mineur dès lors qu'il a obtenu soit, le consentement ou autorisation du représentant légal, soit si le mineur a lui-même donné son consentement. Son consentement peut être recueilli dès lors qu'il a atteint l'âge légal pour, âge laissé à la discrétion des États membres. Le RGPD impose un plancher : le mineur ne peut valablement donner son consentement qu'à partir de 13 ans. La Loi Informatique et Libertés prévoit en son article 45 que le mineur de 15 ans peut consentir seul à un traitement de ses données personnelles. Cette marge de manœuvre laissée à la discrétion des États membres n'est pas amplement satisfaisante et peut engendrer des conflits étant donné les disparités entre États. Si un mineur de 14 ans résident en France consent seul au traitement de ses données à caractère personnel auprès d'une société belge dans le cadre de son activité, un conflit de loi s'installe : du point de vue de la Loi Informatique et Libertés, le mineur ne pouvait pas valablement agir seul, mais du point de vue de la loi belge, laquelle prévoit le consentement valable à l'âge de 13 ans[127], celle-ci s'applique du fait du traitement de données. Pour éviter ces conflits de loi, il aurait été préférable de faire preuve de plus d'harmonisation.

Avant de parvenir à un tel panorama, les dispositions de la Directive du 24 octobre 1995 ne se souciaient guère de la capacité juridique de la personne concernée à consentir. La protection de la personne concernée, si celle-ci était vulnérable, était régie par le droit commun. En droit civil français, cette protection est stricte tant à l'égard des mineurs que des majeurs protégés.

En principe donc, les droits de la personnalité du mineur sont exercés par les représentants légaux, très souvent, les parents. La lettre du RGPD s'inscrit dans cette volonté en précisant que le mineur qui n'a pas atteint l'âge minimal convenu par les États membres doit demander l'autorisation de son représentant légal ou celui-ci doit consentir pour lui. Dans une délibération précédant le RGPD, mais dont il est permis de penser que la position perdure, la CNIL précise qu'il revenait aux représentants légaux d'exercer pour le compte du mineur âgé de moins de 16 ans qui n'a pas sollicité leur autorisation l'ensemble de ses droits, tel que le droit d'accès ou de suppression.[128] L'acte du représentant légal dépasse la simple autorisation mais suppose un véritable exercice des droits et ce pour l'intérêt supérieur de l'enfant[129], décliné en droit interne comme l'intérêt de l'enfant. Bien que cette expression soit considérée comme une « *formule magique* » par le Doyen Carbonnier, les finalités de la notion s'entendent plus clairement. D'après Thomas Dumortier, l'intérêt de l'enfant est destiné à « *fonder un arbitrage entre deux revendications opposées, deux droits en conflit, tandis que dans d'autres cas, il permet de restreindre l'exercice d'un droit*.[130] » Ainsi, l'intérêt de l'enfant est une boussole qui permet

[127] Autorité belge de Protection des Données, *RGPD : la limite d'âge de 13 ans correspond à la pratique numérique*, 13 février 2018, www.autoriteprotectiondonnees.be

[128] CNIL, Délibération n°2012-020 du 26 janvier 2012 *portant recommandation relative à la mise en œuvre, par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers dans le cadre de leurs activités politiques*.

[129] Convention Internationale des Droits de l'Enfant (CIDE), 20 novembre 1989

[130] Thomas Dumortier, *L'intérêt de l'enfant : les ambivalences d'une notion protectrice,* in Le Journal du Droit des Jeunes, 2013/9, n°329, p.13 à 20, www.cairn.info

de prendre la décision la plus protectrice lorsque le responsable de traitement revendique son droit au traitement des données du mineur. La jurisprudence de l'ordre judiciaire a pu se prononcer en faveur de l'intérêt de l'enfant à plusieurs reprises et en des termes explicites rappelant aux représentants légaux le danger que peut représenter le traitement de données à caractère personnel d'un mineur. Bien que les juridictions énoncent que « *la publication de photographies de l'enfant et de commentaires relatifs à celui-ci sur le site Facebook ne constitue pas un acte usuel de l'autorité parentale* » [131], celles-ci ajoutent que « *la mère qui créé un compte pour son enfant de 10 ans met celui-ci en danger* »[132]. Elles ordonnent aussi la suppression d'un compte Facebook d'un mineur de 7 ans[133].

Ces interprétations de la jurisprudence et de la CNIL vont dans le sens de la protection du caractère éclairé du consentement. Comme expliqué précédemment, le caractère éclairé du consentement suppose une pleine conscience des informations distribuées et une capacité décisionnelle murie de ces informations. Un mineur peut être informé, mais sa capacité de discernement n'est pas assez large pour supporter l'ensemble de ces informations et agir en pleine conscience. En ce sens, recourir au représentant légal est l'initiative la moins susceptible de corrompre le rôle de protection qu'a le consentement.

Or, dans le même temps, il est possible d'interroger la question de la liberté du consentement et ce à deux égards. D'abord, le principe de liberté du consentement peut être mis à mal dès lors que le mineur n'utilise pas son propre terminal et que ses données entre en concurrence avec les données personnelles d'un autre utilisateur du terminal. Cet exemple est pertinent s'agissant des cookies sur un site web : le mineur consultant un site peut consentir à tous les cookies sur le terminal, alors même qu'un autre utilisateur du même terminal y aurait refusé. Le consentement du mineur peut engendrer le traitement de données qui ne lui sont pas personnelles, mais personnelles à d'autres utilisateurs du terminal. Ensuite, le mineur peut vouloir consentir au traitement de ses données personnelles pour accéder à une plateforme mais son représentant légal lui en interdit. La volonté du mineur ne serait donc pas respectée, ce qui peut le conduire à consentir en secret, alors même qu'il n'en a pas la capacité. Afin de protéger la liberté du mineur qui a le droit de bénéficier des services de la société d'information, il reste à déterminer le degré d'intervention du représentant légal : si le mineur souhaite consentir, le représentant légal doit-il se contenter d'obtenir les informations permettant un consentement éclairé et spécifique et exercer la volonté du mineur ? Il semble difficile pour le caractère libre du consentement de faire face à la volonté d'un mineur, étant donné que la liberté est incomplète : elle est dépourvue de conscience et dépourvue d'exercice propre.

Toujours dans le sillage de l'intervention du représentant légal, il est possible de s'interroger à proprement dit sur la lettre de l'article du RGPD. Alors que la jurisprudence antérieure disait de l'inscription sur un site internet qu'elle ne faisait pas partie d'un acte usuel d'autorité parentale, la lettre

[131] CA, Versailles, 2ème chambre, section 1, n°13/08349, 25 juin 2015.
[132] CA Agen, n°11/01886, 16 mai 2013.
[133] CA, Aix-en-Provence, n°13/19371, 2 septembre 2014.

de l'article 8 laisse penser que dorénavant, consentir pour le mineur est une obligation du représentant légal qui fait partie intégrante donc de l'autorité parentale. Au regard de la hiérarchie des normes, le RGPD en tant que norme internationale s'applique « au-dessus » de la loi nationale. De ce fait, si cette disposition du RGPD peut être lue comme une obligation, alors c'est une obligation qui se retranscrit naturellement dans l'ordre interne. Serait-il alors possible de présumer, lors du consentement donné par le mineur, que ses responsables légaux s'y sont conformés ? Est-ce une présomption simple, ou irréfragable ? Il est plus juste d'opter pour une présomption simple, tant pour le mineur que le responsable de traitement. L'inconvénient d'une présomption reste la charge de la preuve qui ici, incomberait au responsable de traitement : ce serait à lui de prouver que le responsable légal ne s'est pas conformé à son obligation.

58. Par suite, cette question autour de la responsabilité des représentants légaux fait naître une nouvelle obligation incombant au responsable de traitement, à savoir, de vérifier de manière certaine l'âge du mineur et l'intervention du représentant légal. La loi américaine dite Children's Online Privacy Protection Act oblige les responsables de site à obtenir une autorisation parentale qui soit véritablement vérifiable dès lors qu'ils collectent des données personnelles de mineurs de moins de 13 ans[134]. Ainsi, le texte dispose qu'un responsable de traitement doit fournir tous les efforts raisonnablement attendus de lui pour vérifier que le consentement d'un mineur de moins de 13 ans a été donné par son représentant légal, et ce grâce aux moyens techniques dont il dispose[135]. Cette vérification suppose et de vérifier que le consentement a été correctement donné par le représentant légal du mineur et que l'identité du responsable légal est la bonne. Le texte ajoute des modalités techniques par lesquelles le responsable de traitement peut y parvenir. En tout état de cause, la lettre du texte laisse peser sur le responsable de traitement une obligation de moyens et non une obligation de résultat, ce qui est dommageable. Si le RGPD devait s'inspirer de ces dispositions, alors il serait plus satisfaisant de faire peser une obligation de résultat sur les épaules du responsable de traitement afin de garantir l'intégrité du consentement donné. Sans ces vérifications menées par le responsable de traitement, alors le mineur se retrouve dans une position on ne peut plus vulnérable et où le consentement perd de sa dimension protectrice. Si l'obligation de vérification pesant sur le responsable de traitement n'est pas une obligation de résultat, alors il se peut que le consentement pourtant non valable ne soit pas sanctionné et que le traitement de données illégitime se poursuive.

[134] §312.5. A)1 et A)2, 15 USC §§6501 6506, Children's Online Privacy Protection Act.
[135] §312.5. B)1, 15 USC §§6501 6506, Children's Online Privacy Protection Act. Traduit de l'anglais, « *An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology.* »

II. Consentement et données particulières de l'article 9

59. Le traitement de données sensibles est en principe prohibé par l'article 9.1 du RGPD en ces termes : « *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits*. » Par exception, leur traitement est autorisé si le responsable de traitement a obtenu de la personne concernée son « *consentement explicite* ». L'énumération exhaustive présentée par le règlement permet de dissocier plusieurs catégories de données : les données liées à l'identité personnelle de la personne (les données révélant les origines raciales, ethniques, les opinions politiques, les convictions religieuses, philosophiques, l'appartenance syndicale, l'orientation et la vie sexuelle), les données génétiques, les données biométriques et les données concernant la santé. L'ensemble de ces données sont définies comme étant « *sensibles* » du fait de leur degré d'intimité pour la personne concernée. Ces données constituent toutes ensemble la personne concernée dans son entier, allant de son identité biologique à son identité personnelle. Le considérant 51 du RGPD précise que le traitement de ces données peut engendrer des risques pour les droits et libertés des personnes concernées, ce qui explique leur protection particulière.[136] C'est pourquoi celles-ci sont très liées au consentement : le traitement de ces données ne devrait qu'émaner de la volonté propre de la personne concernée.

La lettre de l'article 9 demande un « *consentement explicite* ». Les observations de Fabrice Mattita sont intéressantes et reprennent l'esprit des lignes directrices du G29. Selon lui, le consentement au traitement de données sensibles est particulier et indépendant de « *l'éventuel consentement au traitement* ». Il ajoute que l'absence de retour à l'article 6 au sein de l'article 9 laisse penser que le consentement aux données sensibles est différent du consentement comme fondement de traitement. De ce fait, il s'interroge sur l'éventuelle différence de régime entre le consentement aux données sensibles et le consentement de l'article 6, en ce sens que le premier serait exempté des critères du consentement tel que prévu par l'article 6[137]. Cette réflexion intéressante peut être réfutée du fait de la nature même des données étudiées. En effet, les données sensibles sont des données particulières demandant le plus haut degré de protection : il serait très dommageable que le consentement aux données sensibles ne doive pas respecter au moins les mêmes conditions que le consentement de l'article 6. De plus, l'article 9 évoque clairement le « *consentement explicite* ». Celui-ci est évoqué aussi pour les transferts de

[136] RGPD, Considérant 51 : « *Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits*. »

[137] Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales, p.4.

données, la prise de décision automatisée et le profilage. L'étude menée dans ces deux domaines a conduit à déterminer que chacun d'eux nécessitait la mise à disposition d'informations spécifiques à leur secteur pour permettre de qualifier le consentement d'explicite. *In casu*, le raisonnement peut s'appliquer à nouveau. Or, il n'est pas impossible que le consentement explicite soit, en plus d'être une base de traitement, une mesure supplémentaire que le responsable de traitement peut mettre en place afin de renforcer la sécurité de son traitement et la protection de la personne concernée. Il n'empêche que le consentement explicite se doit de respecter les conditions du consentement de l'article 6. Autrement, il perdrait de sa pertinence.

Pour le bien de cette étude, ne seront traitées que les données liées à l'identité personnelle de la personne ainsi que les données de santé dans le cadre de la recherche médicale, au vu des analyses convergentes que les autres catégories amènent.

A. Les données relatives à l'identité personnelle

60. Les données relatives à l'identité personnelle de la personne concernée font partie intégrante de son quotidien. Malgré leur fort degré d'intimité avec la personne concernée, ces données peuvent faire l'objet d'un traitement de données si elle donne au responsable de traitement son consentement explicite.

Le traitement des données relatives à l'identité personnelle de la personne concernée peut porter préjudice à sa protection par le consentement à deux égards. Le consentement au traitement de ces données particulières peut ne pas être suffisamment éclairé, ni suffisamment spécifique. En effet, la personne concernée qui consent au traitement peut ne pas avoir, au moment du recueil, tous les détails des données collectées et les finalités pour lesquelles elles le sont, le but pour le responsable de traitement étant d'obtenir un taux de consentement élevé. Il n'est pourtant pas rare que des données d'identification personnelles fassent l'objet d'un traitement : lorsqu'un site internet demande la réponse à une question prédéfinie en cas d'oubli de mot de passe, lorsqu'un site de prêt-à-porter se souvient ou conseille à la cliente une taille ou plus directement, lorsque la personne concernée s'inscrit sur un site de rencontre. Les sites de rencontre ont connu une croissance fulgurante dès les années deux mille. Aujourd'hui, ceux-ci se diversifient en spécifiant un public d'usager. Ainsi, Grindr est une application de rencontre par affinité de genres dont la majorité des utilisateurs appartiennent à la communauté LGBTQI+ tandis que Mektoub est un site de rencontre par affinité religieuse. Lorsque la personne concernée s'inscrit sur le site, la qualité des informations présentées peut ne pas permettre de garantir un consentement explicite, notamment sur les possibles transferts de ces données. C'est notamment le cas de la charte vie privée du site mektoub qui prévoit dans son Article 3 que lorsque la personne s'inscrit, celle-ci consent au transfert de ses données « *y compris de celles portant sur ses croyances et/ou son origine vers les autres États membres [...] les prestataires de mektboub.fr possiblement situés*

en dehors de l'Union Européenne »[138]. Hormis la qualité de cette information sur les transferts qui ne satisfait pas aux exigences de l'article 49 du RGPD puisque les destinataires ne sont pas spécifiquement adressés, le site annonce que les données sensibles qu'il collecte peuvent faire l'objet d'un transfert par la seule inscription de la personne concernée sur son site. Cette rédaction peut-être maladroite est dangereuse pour le responsable de traitement suite à la décision rendue par l'autorité norvégienne à l'encontre de Grindr[139]. En effet, le site s'adonnait à un partage de données sensibles (orientation sexuelle, origine ethnique, etc.) de ses utilisateurs sans leur consentement à des destinataires non identifiés qui s'avéraient faire du ciblage commercial. Dans le cas de mektoub, le site n'a pas recueilli de consentement explicite au transfert, ce qui équivaut à une absence de consentement. La personne concernée est alors on ne peut plus vulnérable. De même, la charte énumère un large nombre de données collectées et conservées, allant de la couleur des yeux jusqu'à l'origine ethnique, ce qui interroge le respect du principe de minimisation du traitement de données et la spécificité du consentement.

La question de l'information donnée à la personne concernée est essentielle, étant donné les conséquences dangereuses pouvant émaner du traitement de telles données. Il se peut que la collecte de ces données fonde une décision discriminatoire, motivée par des biais. C'est pourquoi, en plus d'un consentement éclairé, il est important pour la personne concernée de garder un contrôle sur ses données. Cela passe par une meilleure gestion du consentement, en laissant le choix à la personne concernée de consentir aux finalités qu'elle souhaite. Cela passe aussi par le respect par le responsable de traitement du principe de minimisation des données.

Concernant ce type de données, la question de l'audience qui les renseigne est aussi essentielle. Même s'il n'y a pas de règles spécifiques sur la capacité juridique si ce n'est l'âge requis d'un mineur, il revient au responsable de traitement de s'assurer que la personne concernée a le discernement nécessaire avant de traiter ce type de données. Ces vérifications peuvent être pour lui fastidieuses mais demeurent d'une importance capitale à la protection de la personne concernée.

B. Les données de santé et la recherche scientifique

61. La recherche scientifique est un domaine qui nécessite une grande quantité de données afin d'aboutir à un résultat souvent d'intérêt public, notamment dans le domaine médical. La recherche scientifique est interprétée au sens large par le règlement[140] et encore plus largement par le G29. Selon lui, la recherche scientifique s'entend comme le « *projet de recherche établi conformément aux normes méthodologiques et éthiques du secteur en question, conformément aux bonnes pratiques.* »[141]

---

[138] Mektoub, Charte vie privée, www.mektoub.fr

[139] Datatislynet, 20/02136-18, 13 décembre 2021. V. aussi, NYOB, « *NCC and nyob GDPR complaints: Grindr fined €6,3 Mio over illegal data sharing."*, 15 décembre 2021, www.nyob.eu.

[140] RGPD, Considérant 159 : « [...] *Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large. [...]* »

[141] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.32.

Tout comme les données relatives à l'identité de la personne, le responsable de traitement s'adonnant à de la recherche scientifique peut traiter des données sensibles de la personne concernée s'il obtient son consentement explicite. Cependant, la recherche scientifique peut porter atteinte à l'intégrité du consentement au regard de son critère spécifique et éclairé. En effet, il se peut que le responsable de traitement n'ait lui-même pas les aboutissants complets de sa recherche, celle-ci dépendant fortement du nombre de données collectées. Ainsi, celui-ci ne peut pas fournir à la personne concernée l'ensemble des détails nécessaires au recueil de son consentement totalement éclairé. Or, la qualité de l'information, en plus de la forme, est une composante importante du consentement explicite. Le considérant 33 du RGPD semble lui aussi conclure en ce sens et incite le responsable de traitement à laisser la personne concernée consentir au moins à « *certains domaines de la recherche, [...], dans la mesure où la finalité visée le permet.* » Cette disposition vient assouplir la condition de spécificité du consentement, un avantage pour le responsable de traitement mais un inconvénient pour la personne concernée. *In casu*, le consentement en tant que base de traitement ne suffit pas à protéger la personne concernée. Puisque le consentement est, d'une certaine manière, incomplet, alors le responsable de traitement peut n'avoir que peu de limites et aller au-delà de ce qui est nécessaire à ses fins sous prétexte que le consentement donné par la personne concernée est plus large et général. *In fine,* le consentement n'est pas explicite et devrait être non valable.

Pour protéger le responsable de traitement d'un consentement par nature non valable, l'article 89.1 du RGPD précise que, dans le cadre de la recherche scientifique notamment, le traitement « *est soumis [...] à des garanties appropriées pour les droits et libertés de la personne concernée.*[142]» Cette disposition suit le considérant 51 précédemment cité. Ainsi, le consentement de la personne concernée est agrémenté de mesures complémentaires spécifiques qui permettent de pallier aux carences informationnelles. Ces mesures peuvent d'abord être liées à l'éthique, afin de ne pas dépasser certaines limites à laquelle la personne concernée n'a pas consenti, lesquelles sont aussi encadrées par le Code de la santé publique. Le G29 évoque en ce sens la mise à disposition d'un « *plan de recherche* [143]» qui viendrait compenser la carence de certaines informations liées aux finalités du traitement. Pour garantir la force protectrice du consentement malgré ces différences, il revient au responsable de traitement de vérifier que la personne concernée a bien eu le plan à disposition avant de consentir. Le plan de recherche pourrait réciproquement être opposable au responsable de traitement par la personne concernée. Les mesures peuvent aussi être techniques et relatives à l'anonymisation des données ou encore à leur chiffrement. Ces mesures techniques font partie de l'obligation générale de mise en place de garanties appropriées prévues à l'article 21 du RGPD, ce qui correspond à une obligation de sécurité. Afin de renforcer la protection de la personne concernée, il n'est pas impossible pour le responsable de traitement de fournir de nouvelles informations au fur et à mesure de la recherche afin d'actualiser le

[142] RGPD, Article 89.1
[143] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.34.

consentement de la personne concernée. À la manière de l'AIPD et du TIA, il serait intéressant de mettre à la disposition de la personne concernée une analyse retraçant les risques de la recherche et comment le responsable de traitement y répond. Étant donné que le consentement est en l'espèce moins informé, cette mise à disposition tant du plan de recherche que de l'analyse de risque devrait être obligatoire.

Malgré ce cadre, des chercheurs restent insatisfaits des dispositions actuelles. En ce sens, les chercheurs Henri-Corto Stoeklé et Guillaume Vogt, chercheurs au Neglected Human Genetics, ont déclaré qu'en matière de recherche scientifique impliquant des données génétiques, un consentement écrit en la présence d'un médecin est requis en pratique, alors que selon eux, un « *consentement dynamique* » répondrait à l'exigence de protection de la personne concernée et faciliterait leurs recherches tout en accroissant le nombre de données collectées[144]. Le consentement dynamique est le consentement donné de manière dématérialisée et qui permet à la personne concernée d'obtenir un ensemble de mises à jour des finalités de la recherche via des liens, des podcasts ou des vidéos. Cette idée participe à la transparence du traitement de données et à la transparence de la recherche qui est très plébiscitée par les personnes concernées. Il obtient ses mises à jour grâce à un identifiant unique qui lui permet de se connecter à une plateforme sécurisée. Cette initiative est positive en ce sens qu'elle permet au fur et à mesure d'obtenir un consentement éclairé et spécifique que la personne concernée peut contrôler en temps réel.

L'atout majeur de la transparence pour le responsable de traitement est la diminution du risque de retrait du consentement. Pour rappel, lorsqu'un traitement de données à caractère personnel est fondé sur le consentement, celui-ci peut être retiré librement par la personne concernée. Bien que le consentement dans le cadre de la recherche scientifique puisse paraître plus souple, elle ne bénéficie « *d'aucune dérogation à cet égard* »[145]. Si la personne concernée retire son consentement pendant la recherche, alors le responsable de traitement doit en principe supprimer les données. Or, si les données de la personne concernée sont déterminantes à la recherche, il se peut que le responsable de traitement invoque son intérêt légitime ou l'intérêt public pour maintenir le traitement. Il serait alors préférable pour lui de prévoir une base de traitement de substitution pour continuer sa recherche ou de garantir l'anonymisation des données afin de protéger au maximum la personne concernée. Les comités d'éthique au sein des organisations de recherche ont alors un rôle central à jouer tant pour la protection de la personne concernée par le consentement que pour la garantie de la pérennité de la recherche.

Comme pour les données relatives à l'identité personnelle ou les mineurs, l'audience est ici potentiellement vulnérable. En ce sens, il revient au responsable de traitement de prévoir des garanties plus strictes pour protéger les plus vulnérables.

---

[144] Henri-Corto Stoeklé et Guillaume Vogt, *Tests génétiques, vers un consentement dynamique ?* in Le Figaro, 3 mars 2019, www.lefigaro.fr

[145] Groupe de Travail « Article 29 », WP259, Lignes directrices sur le consentement au sens du règlement 2016/679, 28.11.2017, p.35.

CONCLUSION

62. En définitive, la protection de la personne concernée par le consentement est tel un éventail. Elle a mis en exergue la distinction entre consentement standard et consentement explicite, lequel est lui aussi multiple. Grâce à une définition qui s'est renforcée à la lettre du RGPD, le consentement est une notion strictement encadrée qui laisse, malgré tout, place à une mise en œuvre souple et adaptée aux besoins du responsable de traitement. Le consentement explicite quant à lui reprend naturellement ses critères mais permet une protection accrue en ce qu'il exige une forme et une information sectorielle. Le consentement standard devient explicite.

En sus d'une notion bien encadrée, les critères exposés par le législateur européen permettent d'établir un champ d'obligations spécifiques au consentement auxquelles le responsable de traitement est soumis, permettant ainsi de renforcer la protection de la personne concernée. Il revient alors au responsable de traitement de mettre en œuvre toutes les diligences nécessaires en termes de forme et de fond, en apportant notamment des informations claires et accessibles permettant à la personne concernée de faire un choix en pleine conscience.

En pratique, la protection de la personne concernée par le consentement a elle aussi montré différentes couleurs. Qu'il s'agisse de domaines ordinaires ou de domaines critiques spécifiques, le consentement comme fondement d'un traitement de données à caractère personnel fait face à différents défis et offre différentes réponses. En tout état de cause, le consentement est un fondement propre à la personne concernée qui se rapproche le plus de la volonté du RGPD. Seulement, avec la montée exponentielle de l'économie digitale et l'importance pour les services numériques des données personnelles, celle-ci reste en danger. C'est pourquoi la protection de la personne concernée par consentement tel qu'observée à travers cette étude ne saurait être complète que par une réelle responsabilisation de la personne concernée dont les études montrent qu'elles ont un comportement passif. Ce comportement va à l'encontre de la définition même du consentement. Il revient donc au responsable de traitement mais aussi aux institutions, aux écoles, aux représentants légaux de mener une campagne de sensibilisation et de formation afin que chacun puisse exercer ses droits et consentir au traitement de ses données personnelles en pleine conscience et profiter d'une protection effective.

BIBLIOGRAPHIE

OUVRAGES

François Terre, Philippe Simler, Yves Lequette, François Chénedé, *Droit civil, Les obligations*, 12e éd., Précis Dalloz 2019.

Gérard CORNU, Association Henri Capitant, *Vocabulaire juridique,* PUF, 12ème édition mise à jour « Quadrige », 2018.

George RIPERT et Jean BOULANGER, *Traité élémentaire de droit civil d'après le traité de M. Planiol*, 2e éd., t. 1,

Nathalie MARTIAL BRAZ, Judith ROCHFELD*, Droit des Données Personnelles, les spécificités du droit français à l'égard du RGPD*, Dalloz, 2019.

ARTICLES ET PUBLICATIONS

Autorité belge de Protection des Données, *RGPD : la limite d'âge de 13 ans correspond à la pratique numérique*, 13 février 2018, www.autoriteprotectiondonnees.be

Oliver Cachard, CEJEM, *Validité et formation du contrat électronique dans la LCEN*, 9 octobre 2003, www.cejem.u-paris2.fr

CNIL, *Cookie walls : la CNIL publie des premiers critères d'évaluation*, 16 mai 2022, www.cnil.fr

CNIL, *Refuser les cookies doit être aussi simple qu'accepter : mise en conformité de tous les organismes mis en demeure et actions à venir de la CNIL,* 29 juin 2021, www.cnil.fr

CNIL,*Cookies : sanction de 50 000 euros à l'encontre de la SOCIÉTÉ DU FIGARO,* 29 juillet 2021, www.cnil.fr.

CNIL, *Cookie*, www.cnil.fr

CNIL, *Conformité RGPD, comment recueillir le consentement des personnes ?* 3 août 2018, www.cnil.fr

Conseil d'État, Communiqué de presse, *Cookies publicitaires, Google définitivement condamné à payer 100 millions d'euros,* 27 janvier 2022, www.conseil-etat.fr

Conseil d'État, Communiqué de presse, *Le Conseil d'État annule partiellement les lignes directrices de la CNIL relatives aux cookies et autres traceurs de connexion*, 19 juin 2020, www.conseil-etat.fr

Anne Debet, « *Le consentement dans le RGPD, rôle et définition* » in Communication Commerce Électronique, LexisNexis, 2018.

Thomas Dumortier, *L'intérêt de l'enfant : les ambivalences d'une notion protectrice,* in Le Journal du Droit des Jeunes, 2013/9, n°329, p.13 à 20, www.cairn.info

Gil Forbes, 2013, « *A very short history of Big Data* », www.forbes.com

Fair and Smart, *collecte des consentements sur internet : un état des lieux encourageant mais à améliorer*, 3 janvier 2019, www.fairandsmart.com

Mathilde Gérot, *Dossier thématique – Le renforcement des droits des personnes sur leurs données à caractère personnel,* Revue de Droit international d'Assas n°2, Décembre 2019, 3.

Fabrice Mattita, Administration/Citoyen, Étude, *Traitement de données à caractère personnel, détermination de la base de licéité et conséquences*, La Semaine Juridique Administration et Collectivités territoriales n°7, 18 février 2019.

Fabrice Mattita, Administration/Citoyen, Étude, *Pour en finir avec le mythe du consentement RGPD*, La Semaine Juridique Administration et Collectivités Territoriales n°16, 20 avril 2020.

Nathalie Metallinos, *Le RGPD apporte-t-il de réels changements sur la place du consentement ?* Communication Commerce Électronique n°7-8, Juillet 2018, comm.58.

NYOB, « *NCC and nyob GDPR complaints: Grindr fined €6,3 Mio over illegal data sharing."*, 15 décembre 2021, www.nyob.eu.

Romain Perray, Fasc.932-71, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel / Traitement reposant sur le consentement préalable de la personne concernée, Dispositions Générales*, JurisClasseur Communication, Lexis Nexis, 7 Décembre 2020.

Romain Perray, Fasc.932-72, *Données à caractère personnel, Bases juridiques applicables aux traitements de données à caractère personnel. Dispositions spécifiques imposant le recueil du consentement*, JurisClasseur Communication, Lexis Nexis, 7 décembre 2020.

Romain Perray et Hélène Adda, *Données à caractère personnel – L'arrêt Planet49 relatif aux cookies, pas de nouvelles recettes mais quelques pépites* in Revue Communication Commerce Électronique n°1, Janvier 2020, Lexis Nexis.

Henri-Corto Stoeklé et Guillaume Vogt, *Tests génétiques, vers un consentement dynamique ?* in Le Figaro, 3 mars 2019, www.lefigaro.fr.

Nathalie Weinbaum, *La preuve du consentement à l'ère de la Blockchain*, La Semaine Juridique, entreprises et affaires n°10, 2018, p.28-32.

TEXTES LÉGISLATIFS

Children's Online Privacy Protection Act of 1998, 15 U.S.C 6501/6505.

Code Civil.

Convention Internationale des Droits de l'Enfant (CIDE), 20 novembre 1989.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel n° L 281 du 23/11/1995.*

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *Journal officiel n° L201 du 31/12/2002*.

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

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), *Journal officiel n°L119/1 du 27/04/2016.*

LIGNES DIRECTRICES ET RECOMMANDATIONS

Conseil de l'Europe, Convention 108, STCE 108, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981.

Conseil de l'Europe, Convention 108, T.PD(2019)07BISrev2, *Profilage et la Convention 108+ : pistes pour une actualisation 2010(13) sur le profilage,* 18 juin 2020.

CEPD, Lignes Directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018.

CEPD, Lignes Directrices sur le consentement au sens du règlement EU 2016/697, 5 mai 2020.

Groupe de Travail de l'article 29, WP48, Avis 8/2001 *sur le traitement des données à caractère personnel dans le contexte du travail,* 13 septembre 2001.

Groupe de Travail « Article 29 », WP 114, *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995,* 25 novembre 2005.

Groupe de Travail de l'Article 29, WP187, Avis 15/2011 sur *la définition de consentement*, adopté le 13 juillet 2011.

Groupe de Travail de l'Article 29, WP249, Avis 2/2017 *sur le traitement de données sur le lieu de travail*, adopté le 8 juin 2017.

Groupe de Travail « Article 29 », WP251, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE)2016/679*, 3 octobre 2017.

Groupe de Travail « Article 29 », WP259, *Lignes directrices sur le consentement au sens du règlement 2016/679*, 28 novembre 2017.

ÉTUDES

Commanders Act, *Baromètre Privacy 2021*, 17 juin 2021, www.commandersact.com

Fair and Smart, *collecte des consentements sur internet : un état des lieux encourageant mais à améliorer*, 3 janvier 2019, reprenant le sondage Opinion Way en date de 2018, www.fairandsmart.com

Converteo, Livre Blanc 2021, *Baromètre, taux de consentement à mi-septembre 2021,* www.converteo.com

DÉCISIONS ET DÉLIBÉRATIONS

CA, Versailles, 2ème chambre, section 1, 25 juin 2015, n°13/08349.

CA Agen, 16 mai 2013, n°11/01886.

CA, Aix-en-Provence, 2 septembre 2014, n°13/19371.

Cass. Crim., 18 mars 1975, n° 74-92118.

CE, 19 juin 2020, n°434684.

CE, 28 janvier 2022, n°449209.

CNIL, Délibération n°2012-020 du 26 janvier 2012 *portant recommandation relative à la mise en œuvre, par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers dans le cadre de leurs activités politiques.*

CNIL, Délibération SAN-2018-327, 11 octobre 2018.

CNIL*, Délibération n°2019-093 du* 19 juillet 2019 *portant de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs),*

CNIL, délibération n°2019-160, 21 novembre 2019, portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel.

CNIL, Délibération n°2020-046, 24 avril 2020.

CNIL, délibération SAN-2020-012, 7 décembre 2020.

CNIL, délibération SAN-2021-023 du 31 décembre 2021.

CJUE, 1er octobre 2019, *Affaire C-673/19, Verbraucherzentrale Bundesverband eV contre Planet49 GmbH,.*

CJUE, 16 Juillet 2020, affaire C311/18, *Data Protection Commissionner/Maximilian Schrems and Facebook Ireland*.

CJUE, 11 novembre 2020, affaire C-61/19, *Orange Romania SA c/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal.*
Datatislynet, 13 décembre 2021, 20/02136-18.

Hellenic DPA's decision n°26/2019.

DIVERS

Alec Burnside, V. OCDE DAF/COMP/M(2016)2/ANN2/FINAL 8 juin 2017.

The Chicago History Museum, 1970, « *Arthur Miller and John O'Brien discuss privacy and surveillance* », Studs Terkel Radio Archive.

Privacy Policy des sites internet suivants :
- www.jeuxvideos.com
- www.allocine.fr
- www.tf.fr
- www.mektoub.fr