EXAMEN D'ACCÈS CRFPA

SESSION 2018

Lundi 3 septembre 2018

NOTE DE SYNTHÈSE

Durée de l'épreuve : **5 heures**

Coefficient : **3**

Documents autorisés : Néant

Dès que ce sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 31 pages numérotées de 1/31 à 31/31.

Rappel des recommandations de la Commission Nationale à destination des jurys et des correcteurs d'épreuve, relativement à l'épreuve d'admissibilité de "Note de synthèse rédigée en cinq heures" (article 5-1° de l'arrêté du 17 octobre 2016) :

Le dossier documentaire peut comprendre des documents divers (articles de doctrine, textes normatifs, arrêts, articles de presse, extraits d'ouvrages, cette énumération étant purement indicative). Le dossier ne devrait pas dépasser 20 documents et 30 pages, sans que ces limites soient impératives.

L'épreuve est destinée à apprécier, notamment, les capacités de synthèse du candidat : la limite de quatre pages ne doit pas être dépassée.

La qualité rédactionnelle est prise en compte (déficiences orthographiques et syntaxiques, impropriétés de termes, inélégance de style, obstacles divers à la lisibilité du texte sont sanctionnés).

Un plan apparent (avec des titres concis), dont la structuration est laissée à la libre appréciation du candidat, s'il n'est pas obligatoire, est fortement recommandé.

La note de synthèse doit consister en une synthèse objective des éléments du dossier documentaire, et seules les informations contenues dans le dossier peuvent être utilisées. La référence au numéro du document peut s'avérer nécessaire à la bonne compréhension de la synthèse et est recommandée.

Une brève introduction est possible mais non obligatoire, une conclusion n'est pas nécessaire.

À partir des documents joints, vous établirez une note de synthèse sur le sujet suivant :

CONSENTIR AU TRAITEMENT DE SES DONNÉES PERSONNELLES PAR LES RÉSEAUX SOCIAUX

Liste des documents :

Document 1 : 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 (règlement général sur la protection des données) (extraits)

Document 2 : Charte des droits fondamentaux de l'Union européenne, proclamée le 7 décembre 2000 et modifiée par le Traité de Lisbonne entré en vigueur le 1er décembre 2009 (extraits)

Document 3 : Jean-François KERLEO, « *La transparence en droit* », thèse de doctorat en droit Public, Lyon III, octobre 2012 (extrait, sans note de bas de page)

Document 4 : Adrien BASDEVANT et Jean-Pierre MIGNARD, « *L'empire des données* », Edition Don Quichotte, 2018 (extraits, sans note de bas de page)

Document 5 : Denis OLIVENNES et Mathias CHICHPORTICH, « Mortelle Transparence », éditions Albin Michel 2018 (extraits, sans note de bas de page)

Document 6 : Le Figaro, 12 avril 2018, « *Google et Twitter pourraient être également visés* » (extraits)

Document 7 : Anne DEBET, Professeur à l'université de Paris Descartes, « *Le consentement dans le RGPD : rôle et définition* » (extraits, sans note de bas de page)

Document 8 : « *RGPD : la protection des données à caractère personnel* », Lextenso 2018, par Aurélie BANK, juriste, Responsable pédagogique du DU PDO de Paris Nanterre (fiche 5, pages 21 à 23)

Document 9 : « *Protection des données personnelles* » éditions Législatives 2017, ouvrage collectif sous la direction de Laurent CHEVRY (pages 28 et 29 ; pages 200 à 203) (extraits)

Document 10 : « *La protection des données personnelles de A à Z* », éditions Bruylant (Bruxelles 2017), ouvrage collectif sous la direction de Alain BENSOUSSAN (pages 46 et 47 ; pages 109 et 110) (extraits, sans note de bas de page)

Document 11 : « *Droit de la donnée* », édition LexisNexis 2017, par Matthieu BOURGEOIS (extrait 1, sans note de bas de page)

Document 12 : « *Droit de la donnée* », édition LexisNexis 2017, par Matthieu BOURGEOIS (extrait 2, sans note de bas de page) (pages 97 et s)

Document 13 : Le Monde, 14 mai 2018, « *Le Parlement adopte le projet de loi sur la protection des données personnelles* »

Document 14 : Projet de loi relatif à la protection des données personnelles, texte définitif voté par l'Assemblée Nationale le 14 mai 2018

Document 15 : Code civil, Livre premier, Titre onzième : De la majorité et des majeurs protégés par la loi

Document 16 : Capital, 25 janvier 2015, « *Et si, demain, vous vendiez vos données personnelles à Facebook* ? » par Samuel CHALOM (extraits)

Document 17 : Article 544 du Code Civil (créé par Loi n° 1804-01-27 promulguée le 6 février 1804)

Document 18 : Article 9 du Code civil (créé par Loi n° 1803-03-08 promulguée le 18 mars 1803, modifié par Loi n° 1927-08-10, par Loi n° 70-643 du 17 juillet 1970 et par Loi n° 94-653 du 29 juillet 1994

Document 19 : Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (JORF n° 0235 du 8 octobre 2016) (extraits)

Document 20 : « *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information* », Rapport d'information n° 441 (2008-2009) de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, fait au nom de la commission des lois du Sénat, déposé le 27 mai 2009 (extraits)

Document 21 : Code civil, Livre troisième, Titre trois : Des sources d'obligations

DOCUMENT 1 : 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 (règlement général sur la protection des données) (extraits)

Considérant ce qui suit :

(1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental (...).

(2) (...) Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.

(...)

(6) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

(7) Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques.

(...)

(32) Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé.

(...).

(38) Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

(...)

(40) Pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la loi, soit dans le présent règlement soit dans une autre disposition du droit national ou du droit de l'Union, ainsi que le prévoit le présent règlement (...).

(42) Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement. En particulier, dans le cadre d'une déclaration écrite relative à une autre question, des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée. Conformément à la directive 93/13/CEE du Conseil, une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et elle ne devrait contenir aucune clause abusive. Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

(43) 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 du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.

(...)

(58) (...) Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre.

(59) Des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par le présent règlement, y compris les moyens de demander et, le cas échéant, d'obtenir sans frais, notamment, l'accès aux données à caractère personnel,

et leur rectification ou leur effacement, et l'exercice d'un droit d'opposition. Le responsable du traitement devrait également fournir les moyens de présenter des demandes par voie électronique, en particulier lorsque les données à caractère personnel font l'objet d'un traitement électronique. Le responsable du traitement devrait être tenu de répondre aux demandes émanant de la personne concernée dans les meilleurs délais et au plus tard dans un délai d'un mois et de motiver sa réponse lorsqu'il a l'intention de ne pas donner suite à de telles demandes.

(...)

(65) Les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et disposer d'un « droit à l'oubli » lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union ou du droit d'un État membre auquel le responsable du traitement est soumis. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant, ou encore lorsque le traitement de leurs données à caractère personnel ne respecte pas d'une autre manière le présent règlement. Ce droit est pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'est plus un enfant (...).

CHAPITRE I
Dispositions générales

(...)

Article 3
Champ d'application territorial

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

a)	à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
b)	au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

(...)

Article 4
Définitions

Aux fins du présent règlement, on entend par :

1) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une

«personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;
2) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

(...)

11) « consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ;

(...)

CHAPITRE II
Principes

(...)

Article 6
Licéité du traitement

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a)	la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
b)	le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
c)	le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
d)	le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
e)	le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
f)	le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

(...)

Article 7

Conditions applicables au consentement

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

(...)

Article 8

Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information

1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.
Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.
2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.
3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

Article 9

Traitement portant sur des catégories particulières de données à caractère personnel

1. 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.
2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :
a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

(...)

CHAPITRE XI
Dispositions finales

(...)

Article 99
Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
2. Il est applicable à partir du 25 mai 2018.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

DOCUMENT 2 : Charte des droits fondamentaux de l'Union européenne, proclamée le 7 décembre 2000 et modifiée par le Traité de Lisbonne entré en vigueur le 1er décembre 2009 (extraits)

Les peuples d'Europe, en établissant entre eux une union sans cesse plus étroite, ont décidé de partager un avenir pacifique fondé sur des valeurs communes.

Consciente de son patrimoine spirituel et moral, l'Union se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité ; elle repose sur le principe de la démocratie et le principe de l'État de droit. Elle place la personne au cœur de son action en instituant la citoyenneté de l'Union et en créant un espace de liberté, de sécurité et de justice.

L'Union contribue à la préservation et au développement de ces valeurs communes dans le respect de la diversité des cultures et des traditions des peuples d'Europe, ainsi que de l'identité nationale des États membres et de l'organisation de leurs pouvoirs publics aux niveaux national, régional et local; elle cherche à promouvoir un développement équilibré et durable et assure la libre circulation des personnes, des services, des marchandises et des capitaux, ainsi que la liberté d'établissement.

À cette fin, il est nécessaire, en les rendant plus visibles dans une Charte, de renforcer la protection des droits fondamentaux à la lumière de l'évolution de la société, du progrès social et des développements scientifiques et technologiques.

La présente Charte réaffirme, dans le respect des compétences et des tâches de l'Union, ainsi que du principe de subsidiarité, les droits qui résultent notamment des traditions constitutionnelles et des obligations internationales communes aux États membres, de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, des Chartes sociales adoptées par l'Union et par le Conseil de l'Europe, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'Homme. Dans ce contexte, la Charte sera interprétée par les juridictions de l'Union et des États membres en prenant dûment en considération les explications établies sous l'autorité du Praesidium de la Convention qui a élaboré la Charte et mises à jour sous la responsabilité du Praesidium de la Convention européenne.

La jouissance de ces droits entraîne des responsabilités et des devoirs tant à l'égard d'autrui qu'à l'égard de la communauté humaine et des générations futures.

En conséquence, l'Union reconnaît les droits, les libertés et les principes énoncés ci-après.

(...)

TITRE II
LIBERTÉS

(...)

Article 8
Protection des données à caractère personnel

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

DOCUMENT 3 : Jean-François KERLEO, "*La transparence en droit*", thèse de doctorat en droit Public, Lyon III, octobre 2012 (extrait, sans notes de bas de page)

587. Les dangers inhérents à la collecte et au traitement de données personnelles ne relèvent pas exclusivement de leur réutilisation commerciale. C'est toute la dimension de la protection de la vie privée et du droit à l'image qui est directement concernée par le développement des nouvelles technologies de l'information et de la communication. Les données personnelles sont le reflet d'une identité parfois intime qui mérite d'être maintenue dans l'opacité. Or, ces ressources représentent une manne économique pour des entreprises qui cherchent à cibler leur clientèle ou bien simplement à profiter des ressources disponibles pour en tirer un profit commercial. Les rapports annuels d'activité de la CNIL sont d'ailleurs l'occasion de souligner les dérives d'une commercialisation des données à caractère personnel. Ainsi la CNIL rappelle-t-elle que la publicité dire ciblée ainsi que les réseaux sociaux (Facebook, MySpace, Linkedin, Copainsdavant, etc.) représentent un risque de commercialisation des données personnelles qui, pour ce dernier cas, concerne les fournisseurs de contenus internet envers les annonceurs. La commercialisation tout comme l'utilisation à des fins de prospection commerciale passent soit par la collecte préalable des données par les opérateurs eux-mêmes, soit par une mise à disposition des données personnelles à l'initiative de personnes privées ou publiques. Certaines sociétés se sont spécialisées dans la commercialisation des données personnelles qu'elles se chargent de collecter préalablement pour d'autres sociétés dans des conditions parfois sanctionnées par la CNIL. Par conséquent, les usages de la transparence transforment les données personnelles en ressources économiques constituant une identité proprement économique de l'individu.

DOCUMENT 4 : Adrien BASDEVANT et Jean-Pierre MIGNARD, "*L'empire des données*", Edition Don Quichotte, 2018 (extraits, sans notes de bas de page)

Les algorithmes déterminent notre quotidien (...). Ces algorithmes sont nourris par des quantités illimitées d'un carburant nouveau, les data, pour anticiper ou orienter nos intérêts, déterminer les opportunités offertes et enfin nous guider. Mais qu'est-ce qu'une donnée ? Avant de pénétrer dans les problématiques et les disputes multiples, Wikipédia nous en propose une définition communément acceptée, énoncée par le professeur d'informatique Serge Abiteboul : "*Une donnée est une description élémentaire d'une réalité. C'est par exemple une observation ou une mesure. La donnée est dépourvue de tout raisonnement, supposition, constatation, probabilité. Etant indiscutable ou indiscutée, elle sert de base à une recherche, à un examen quelconque*".

Notre monde est ainsi devenu le monde des données. D'après l'Organisation des Nations unies (ONU), plus de données ont été créées en 2011 que dans toute l'histoire de l'humanité. Matière première du XXIe siècle, présentée parfois comme le pétrole, que l'on extrait, raffine, puis distribue, la data est le moteur de l'économie. Son volume disponible sous forme numérique connait une croissance considérable. En 2013, plus de 4,4 zettaoctets - c'est-à-dire 10^{21} octets de données ont été produits. En transcrivant ce contenu sur CD-Rom, on obtiendrait une pile mesurant les deux tiers de la distance entre la Terre et la Lune.

Cette masse de données double tous les deux ans et devrait atteindre 44 zettaoctets en 2020, soit plus de six fois la distance séparant la Terre de la Lune. Ces chiffres donnent le vertige. Qui n'a jamais éprouvé la sensation d'être dépassé par ce déluge de contenu ? Chaque minute, plus de deux cents millions de mails sont envoyés, cinq cent mille tweets partagés, trois milliards et demi de requêtes effectuées sur les moteurs de recherche, dix millions de vidéos visionnées, cent millions de photos chargées et cinquante mille sites Internet piratés. Ces indicateurs deviendront rapidement dérisoires, une fois que l'ensemble des objets de notre quotidien - brosse à dents, grille-pain, frigidaire, trottinette, oreiller - seront, eux aussi, intégralement connectés à nos activités par l'Internet des objets. En effet, selon une étude du cabinet IDC, il y aura quatre-vingts milliards d'objets connectés en 2020, contre quatre milliards seulement en 2010.

Cette croissance exponentielle du volume de données disponibles sous forme numérique est communément désignée par l'appellation big data, signifiant "*données massives*". Elle renvoie à la concordance de trois facteurs : la collecte volumineuse en temps réel de données provenant d'une variété de sources, la réduction drastique du coût du stockage, et la sophistication de nouvelles fonctionnalités d'analyse des données tournées vers l''action et la décision, permettant d'établir des liens et des inférences.

La transformation numérique, en raison de la massification de la collecte des données et de la diversification de leurs usages, bouleverse toutes les sphères de notre société.

(...)

DOCUMENT 5 : Denis OLIVENNES et Mathias CHICHPORTICH, "Mortelle Transparence", éditions Albin Michel 2018 (extraits, sans notes de bas de page)

(...)
Serions-nous devenus schizophrènes ? Une étude réalisée sur un panel de 1 587 citoyens français, allemands, anglais, italiens, américains et chinois souligne l'étendue du paradoxe : 75 % des personnes interrogées indiquent être préoccupées par le respect de leur vie privée, 66 % estiment n'avoir qu'un contrôle partiel sur leurs données personnelles et 95 % affirment leur défiance à l'égard des réseaux sociaux.

Est-ce pour autant un frein au partage de nos photographies de famille, de nos états d'âme ou de nos souvenirs de vacances ? Paradoxalement, non. 350 millions de photos sont partagées sur Facebook chaque jour, 150 millions sur Snapchat, 40 millions sur Instagram... 700 millions d'utilisateurs actifs pour cette dernière application tandis que Facebook poursuit, trimestre après trimestre, sa fulgurante progression pour frôler les 2 milliards d'utilisateurs. En France, la proportion des personnes connectées aux réseaux sociaux a plus que double en moins de six ans (...).

Comment préserver le droit à la vie privée sans entraver l'innovation ? Comment garantir la sécurité des citoyens sans verser dans la surveillance de masse ? Comment promouvoir les échanges sans sacrifier la protection des données personnelles des Européens ? (...)

DOCUMENT 6 : Le Figaro, 12 avril 2018, « *Google et Twitter pourraient être également visés* » (extraits)

Tandis que Mark Zuckerberg doit s'expliquer sous la lumière crue du Congrès américain, d'autres acteurs se réjouissent de rester dans l'ombre. Depuis le début de la crise, Google et Twitter se font très discrets. Les deux entreprises ont pourtant un modelé économique comparable en de nombreux points à celui de Facebook. Leurs outils de ciblage publicitaire ont également été détournés à des fins politiques durant les élections présidentielles américaines. «*Il ne faut pas être dupe, Facebook a beau être à nouveau dans l'œil du cyclone, le problème est beaucoup plus large que Cambridge Analytica*, souligne Jeremy Ghez, professeur d'économie et d'affaires internationales à HEC. *Tous les géants d'Internet sont en ligne de mire des législateurs américains, qui ont pris conscience du pouvoir d'influence de ces réseaux et veulent le réguler* ».

(...)

Miroir aux alouettes

Tout l'écosystème des réseaux sociaux suit peu ou prou le même modèle.

(...)

DOCUMENT 7 : Anne DEBET, Professeur à l'université de Paris Descartes, « *Le consentement dans le RGPD : rôle et définition* » (extraits, sans notes de bas de pages)

La place centrale du consentement est souvent présentée comme un des changements majeurs introduit par le RGPD dans le sens d'un renforcement du droit des personnes. Pourtant, le consentement peut avoir un rôle plutôt ambigu. Protecteur dans certains cas, il permet, dans d'autres, aux responsables de traitement de déroger à certaines règles posées par le Règlement (traitement des données sensibles et encadrement des transferts notamment). (...)

1 - Un des aspects du Règlement (UE) 2016/679 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 (ci-après RGPD), le plus fréquemment invoqué, est le renforcement des droits des personnes. Dans le cadre de ce renforcement, le rôle et les caractères du consentement tels qu'ils sont encadrés par le texte sont souvent envisagés. Et, il est fréquemment avancé que les individus ont un meilleur contrôle de leurs données – certains utilisent l'anglicisme *empowerment* – grâce notamment à la place centrale du consentement dans le RGPD. Or, cette affirmation doit être nuancée car le RGPD ne consacre pas un consentement préalable, un *opt in*, généralisé comme peuvent le croire aujourd'hui certains, ce qui angoisse inutilement beaucoup de responsables de traitement. Il est incontestable néanmoins que le consentement a eu un rôle croissant dans le droit de la protection des données.

(...)

Les rédacteurs du RGPD ont quant à eux beaucoup insisté sur le consentement. Il y a ainsi 68 occurrences du mot consentement dans le RGPD contre 12 dans la directive 95/46/CE (qui est un texte trois fois plus court). Alors même que la directive contenait une définition précise du consentement, le RGPD est encore plus détaillé sur le sujet. Des questions laissées en suspens par la directive – notamment la question du consentement des enfants – ont été précisées. Enfin, le consentement a gardé son rôle de fondement dérogatoire du traitement

des données sensibles et des transferts et est aussi devenu un fondement dérogatoire rendant possible la prise de décision automatisée. Il est donc aujourd'hui nécessaire de faire un bilan de ces changements pour voir si l'exigence du consentement justifie une telle anxiété de la part des responsables de traitement. Il faut, avant cet examen, préciser que le projet de loi intégrant le Règlement en droit français, actuellement en cours d'examen au Parlement, n'apporte pas vraiment de nouveautés sur le sujet – sauf en ce qui concerne le consentement des enfants. C'est donc essentiellement le RGPD qui sera l'objet de cette étude notamment au regard des positions récentes prises par la CNIL. Dans un ordre, un peu inversé par rapport aux constructions doctrinales classiques, il faudra s'intéresser au rôle du consentement (1) avant d'examiner la définition du consentement et ses caractéristiques (2).

1. Le rôle du consentement

2- Le consentement peut avoir un rôle plutôt protecteur, c'est le cas quand il sert de fondement au traitement (A). En revanche, il peut aussi être un élément sur lequel le responsable de traitement va déroger à des interdictions posées par le texte. Son rôle est alors non de protéger la personne mais d'ouvrir des possibilités au responsable de traitement (B).

A- Le consentement protecteur : le consentement comme fondement du traitement

3- L'article 6 RGPD sur la « Licéité du traitement » prévoit que le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques (a) ; le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles (b) ; au respect d'une obligation légale à laquelle le responsable du traitement est soumis (c) ; à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (d) ; à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (e) ; ou le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant (f). (...)

Il faut préciser et cela n'a pas peut être été très clair au moment de la transposition de la directive que le consentement n'est pas le fondement prioritaire des traitements et que ce n'est certainement pas forcément le plus adapté (...).

Les responsables de traitement ne doivent donc pas faire du recueil préalable du consentement une obsession. En effet dans le secteur privé, il est possible comme le soulignent les rapports Braibant et Gouzes préalablement cités de se fonder sur l'intérêt légitime ou sur la nécessité contractuelle. Toutefois, l'interprétation progressivement de plus en plus stricte de ces deux possibilités a eu comme conséquence le report de l'attention vers le consentement (...).

B- Le consentement source de dérogations aux règles posées par le RGPD

(...)

4- Le consentement peut être utilisé aussi pour fonder une possibilité de traitement ou de transfert par dérogation. Il n'est alors pas un instrument de protection de la personne. Grâce au consentement, le responsable de traitement va pouvoir faire quelque chose qui lui est sinon interdit. Il peut s'agir de traiter des données sensibles (art. 9), ce qui n'est pas très nouveau, faire un transfert (art. 49), ce n'est pas non plus une nouveauté mais on verra que la portée de cette dérogation interroge. Le responsable de traitement pourra aussi prendre à l'égard des

personnes, des décisions automatisées, interdites autrement et enfin traiter des données pour une finalité différente de celle pour laquelle elles ont été collectées. (...)

2. La définition et les caractéristiques du consentement

5- Le consentement est défini à l'article 4, 11° du RGPD. Il doit, comme nous l'avons vu plus haut, dans certains cas être explicite. Avant d'étudier l'ensemble de ces caractères (B), il faut dire un mot de l'identité de la personne qui doit consentir (A).

A- L'identité de la personne qui doit consentir : la question des enfants

6- Le traitement de données à caractère personnel des enfants, c'est-à-dire des personnes âgées de moins de 18 ans, est à l'origine de nombreux questionnements. Jusqu'au RGPD, les textes n'apportaient pas de solutions très claires sur ce point.

En principe, les règles de l'autorité parentale, figurant dans le Code civil, sont assez strictes en France. En effet, les droits de la personnalité de l'enfant sont exercés par les deux parents et l'accord des deux est nécessaire. Ainsi, l'inscription d'un mineur sur un réseau social n'est pas, selon les juridictions, un acte usuel de l'autorité parentale pour lequel l'accord d'un seul des deux parents serait suffisant. S'il faut l'accord des deux parents, a fortiori, ne pouvait-il pas s'agir d'un acte qu'un enfant pouvait faire tout seul.

La pratique était cependant plus souple et assez variable, certains sites fixant un seuil à 13 ans, d'autres à 16 ans pour collecter des données personnelles auprès des enfants et leur permettre d'accéder à des services. La CNIL, elle aussi, avait une position complexe sur le sujet. Elle acceptait parfois une collecte de données auprès d'enfants de 16 ans sans recueil du consentement des titulaires de l'autorité parentale, mais exigeait que les titulaires de cette autorité puissent exercer les droits d'accès, de rectification et d'opposition. La CNIL relève, d'ailleurs, lors de la mise en demeure d'un site de rencontres que le responsable du site n'avait pas obtenu le consentement du « tuteur légal » des mineurs.

Face aux incertitudes juridiques, le législateur européen devait trouver une solution. Quelques exemples étrangers montraient qu'il n'y avait pas sur cette question de consensus. La loi la plus fréquemment évoquée dans ce domaine est évidemment la loi américaine COPPA (Children's Online Protection Act) qui oblige les responsables des sites à obtenir une autorisation parentale vérifiable pour la collecte de données personnelles auprès d'enfants de moins de 13 ans. Les pratiques européennes à cet égard étaient très variables. Le RGPD pose donc une règle à ce sujet dans son article 8. Lorsque le consentement est le fondement du traitement, et seulement dans ce cas-là, ce qui n'est pas une hypothèse si fréquente que cela, pour les services de la société de l'information – la notion est très large – s'adressant aux enfants, un consentement parental est exigé avant l'âge de 16 ans, les États pouvant faire un choix moins protecteur et abaisser cet âge à 13 ans, le législateur français semblant vouloir faire le choix intermédiaire de 15 ans. Dans cette hypothèse, le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles. La preuve du consentement parental suscite cependant de nombreuses interrogations car elle suppose que le site recueille, a minima, l'e-mail des parents auprès du mineur ou même l'adresse si la solution de la voie postale, qui est plus sûre, est préférée, soit de nouvelles données à caractère personnel.

(...)

B- Les caractéristiques du consentement

7- Deux types de consentement sont présents dans le Règlement : "*le consentement normal*" (1°), celui exigé pour fonder un traitement ou pour traiter des données pour une finalité incomptable avec celle pour laquelle celles-ci ont été collectées et le consentement explicite (2°), celui exigé pour traiter des données sensibles, prendre une décision automatisée ou permettre un transfert.

1° Les caractéristiques du consentement « normal »

8 - Les caractéristiques de ce consentement figurent dans sa définition à l'article 4. 11 du RGPD. Il s'agit de toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement (...).

9- La liberté du consentement. – La première exigence à l'égard du consentement est la liberté de celui-ci (...).

Le consentement est, en outre, d'autant plus libre qu'il est révocable comme le montre l'article 7, 3° du RGPD et l'article 17, 1°, b) sur le droit à l'effacement qui peut être exercé quand le consentement est retiré (...).

10 - Le consentement spécifique et éclairé. – Le consentement doit aussi être spécifique et, là encore, les exigences sont très strictes. La règle était déjà posée dans la directive 95/46 et la CJCE avait eu l'occasion en 2010 de donner des précisions sur celle-ci dans l'arrêt Volker et Markus Schecke. Comme l'indique l'article 7, 2 du RGPD, le recueil du consentement ne peut pas être noyé dans les conditions générales du site. Il doit faire l'objet d'un recueil spécifique et séparé. (...)

Le consentement doit aussi présenter un autre caractère, il doit être éclairé, ce qui renvoie à la nécessité d'informer la personne. (...) Il ne faut pas noyer la personne dans les informations – l'information peut être fournie par strates – et s'adresser à la personne dans un langage clair, compréhensible et adapté, en particulier à son âge.

11 - Le consentement : une manifestation de volonté, acte positif clair ou déclaration univoque. – Le consentement doit être une manifestation non ambiguë des souhaits de la personne. Le 32e considérant du RGPD précise que cela peut « *se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité* » (...).

12- La preuve du consentement. – Le RGPD exige du responsable de traitement de pouvoir rapporter la preuve que la personne a consenti. Cette règle est clairement formulée dans le RGPD, mais on peut se demander si le droit antérieur ne la consacrait pas déjà dans l'exigence du caractère « indubitable » du consentement figurant à l'article 7 de la directive. Les responsables de traitement sont libres de choisir les modalités selon lesquelles ils vont recueillir le consentement (enregistrements oraux, registre des consentements, informations sur la session pendant laquelle le consentement est obtenu...).

Il résulte de tous ces développements qu'il va donc être souvent difficile pour un responsable de traitement d'obtenir un consentement « normal » et d'en apporter la preuve. Qu'en est-il dès lors s'agissant du consentement explicite ?

2° Les caractères du consentement explicite

13- Le consentement explicite permet, comme cela a été déjà envisagé, de traiter des données sensibles (art. 9), de prendre des décisions automatisées (art. 22), même dans le cas où ces décisions sont fondées sur des données sensibles et de faire un transfert (art. 49). Ni le RGPD, ni le G29 ne sont très prolixes sur cette exigence d'un consentement explicite. Il faut dire que celle-ci figurait déjà à l'article 8 de la directive 95/46/CE et il convient sans doute de se référer aux interprétations antérieures de ce texte. Le législateur français avait fait en 2004 le choix de mentionner un consentement exprès pour traiter des données sensibles mais tant les travaux préparatoires de la loi de transposition que l'avis du G29 de 2001 sur le consentement indique que ces mots explicites et exprès ont la même signification.

Pour mémoire, le Conseil d'État a adopté, avant 2004, une approche stricte de la notion d'accord exprès figurant à l'article 31 de la loi du 6 janvier 1978, suivie par la CNIL exigeant que l'accord soit nécessairement écrit. Cependant, la CNIL avait dû évoluer sur ce sujet, notamment dans le domaine de la santé, domaine dans lequel le fait de cocher d'une croix sur un formulaire électronique a été considéré comme un consentement 81, tant pour des raisons pratiques que juridiques.

Dans son avis sur le consentement datant du 13 juillet 2011, le G29 considérait, en effet, que, bien qu'un consentement explicite soit généralement donné par écrit, il n'était pas exclu qu'il puisse l'être oralement, ce que prouve d'ailleurs l'examen des travaux préparatoires de la directive 95/46. Une action positive peut ainsi être considérée comme un consentement explicite, par exemple en cochant une case ou en cliquant sur une icône. (...)

14 - En conclusion de cette étude relative au consentement, il est difficile d'avoir une opinion tranchée sur le rôle et la notion du consentement dans le RGPD. L'importance accrue du consentement comme fondement du traitement n'est pas forcément liée au changement des textes, mais plutôt à l'interprétation de plus en plus restrictive par les autorités de protection des données des autres fondements possibles des traitements. Les responsables de traitement, tenus de choisir un fondement au traitement, vont peut-être s'orienter vers un consentement plus rassurant que l'invocation d'un intérêt légitime susceptible d'être remis en cause dans le cadre d'une mise en balance parfois aléatoire des droits en présence. Il faut cependant les avertir. Le consentement prévu par le RGPD est un consentement exigeant, dont le caractère libre et spécifique ne sera pas toujours facile à garantir. Une réflexion de fond est donc nécessaire aujourd'hui avant de mettre en œuvre son traitement quant au fondement de celui-ci !

DOCUMENT 8 : « *RGPD : la protection à caractère des données personnelles* », Lextenso 2018, par Aurélie BANK, juriste, Responsable pédagogique du DU PDO de Paris Nanterre (fiche 5, pages 21 à 23)

LE CONSENTEMENT DES PERSONNES CONCERNEES

Tout traitement de données à caractère personnel doit pour être licite reposer sur un fondement (v. Fiche 2). Le consentement des personnes concernées donné « *pour une ou plusieurs finalités spécifiques* » est l'un de ces fondements.

Face à certaines pratiques consistant à pré-cocher des cases d'acceptation, à obtenir des consentements tacites ou à noyer des recueils de consentement au milieu de conditions générales illisibles, le législateur européen a souhaité rendre toute sa valeur au consentement de la personne concernée qui doit être « *une manifestation de volonté libre, spécifique, éclairée et univoque* » par laquelle un individu accepte que ses données fassent l'objet d'un traitement (art. 4, 11).

La notion de consentement intervient à plusieurs reprises dans le cadre du RGPD et des règles spécifiques s'y appliquent.

Les caractéristiques du consentement

- Libre

Ainsi, « *le consentement 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 du traitement, en particulier lorsque le responsable du traitement est une autorité publique* » (considérant 43). Le consentement ne pourra pas être libre si la personne n'est pas en mesure de refuser ou de retirer son consentement sans subir un préjudice (par exemple un coût supplémentaire, une diminution de la performance d'un service, etc.).

- Spécifique

Il doit être donné pour une finalité précise et de manière granulaire. Ainsi, il ne semble pas possible d'obtenir un seul consentement pour un groupe de traitement ayant des finalités distinctes.

- Éclairé

La personne concernée doit avoir été informée préalablement au recueil de son consentement afin de pouvoir le donner en toute connaissance de cause. Le G29 dans ses lignes directrices sur le consentement, publiées le 28 novembre 2017, considère qu'il convient a minima d'indiquer à la personne concernée :

- l'identité du responsable du traitement ;
- la finalité de chaque traitement de données pour lequel le consentement est recueilli ;
- les catégories de données collectées et utilisées ;
- l'existence d'un droit de retirer son consentement ;
- l'existence d'une prise de décision automatisée, incluant une mesure de profilage ;
- si le consentement concerne des transferts de données, les risques potentiels inhérents à un transfert vers un pays tiers en l'absence d'une décision d'adéquation ou d'une garantie appropriée.

Comme pour toute communication à l'intention des personnes concernées, ce message doit être communiqué dans un langage clair, accessible et compréhensible.

- Univoque

Il doit être « *donné par un acte positif clair* » (considérant 32). Il peut prendre la forme d'une déclaration écrite, orale, d'une case à cocher ou « *en optant pour certains paramètres techniques pour des services de la société de l'information* » (considérant 32). C'est donc la fin des cases cochées par défaut ou des consentements tacites résultant d'une inactivité de la personne concernée.

Les conditions applicables au consentement

Le responsable du traitement doit être en mesure de « *démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant* » (art. 7, 1). Le considérant 42 précise qu'il doit être « *en mesure de prouver que ladite personne a consenti à l'opération de traitement* ».

Il ne s'agit donc pas uniquement de démontrer que la procédure applicable comportait un recueil de consentement répondant aux caractéristiques prévues par le RGPD mais d'apporter la preuve qu'un individu donné a consenti.

À noter que la charge de la preuve incombe au responsable du traitement. Le G29 recommande d'enregistrer ces consentements avec leur date et leur mode de collecte et d'y associer l'information communiquée à la personne concernée.

Si le consentement doit être recueilli dans le « *cadre d'une déclaration écrite qui concerne d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions* » (art. 7, 2). Le consentement au traitement des données doit ainsi être distinct de l'acceptation d'un contrat. Le G29 précise clairement dans ses lignes directrices que l'acceptation de conditions générales ne saurait être considérée comme un acte positif clair exprimant un consentement à un traitement de données à caractère personnel.

La personne concernée a le droit de retirer son consentement à tout moment et il doit être aussi simple de retirer son consentement que de le donner (art. 7,3).

Le consentement a-t-il une durée de validité ? Le RGPD ne prévoit pas de durée de validité du consentement mais le G29 recommande de la renouveler à intervalle approprié.

Le consentement explicite

Le RGPD prévoit trois cas dans lesquels le consentement doit être renforcé :
- en cas de collecte de données relevant d'une catégorie particulière au sens de l'article 9 (v. Fiche 6) ;
- en cas de transfert de données vers un pays tiers ou une organisation internationale et en l'absence de mesures de protection appropriées dans le cadre de l'article 49 (v. Fiche 9) ;
- en cas de prise de décision individuelle automatisée, incluant un profilage (art. 22 ; v. Fiche 14).

Dans ces hypothèses, le consentement doit être explicite, ce qui sous-entend un renforcement de l'expression de la volonté de la personne concernée par rapport au consentement « *simple/ordinaire* » relevant de l'article 6. Dans la mesure où l'article 6 exclut les consentements tacites, l'interprétation de cette disposition peut poser certaines difficultés. Dans le cadre de ses lignes directrices, le G29 indique que ce consentement peut être recueilli via une déclaration écrite de la personne concernée ou un process d'authentification à deux facteurs (par mail et par SMS par exemple).

À noter que les autres conditions relatives au consentement s'appliquent également à ce consentement renforcé.

Le consentement et les enfants

Le RGPD prévoit des dispositions spécifiques pour protéger les personnes vulnérables, en particulier les enfants, c'est-à-dire les mineurs âgés de moins de 16 ans. Dans l'hypothèse où le consentement d'un mineur serait requis pour un traitement relatif à « *l'offre directe de services de la société de l'information aux enfants* », le traitement de leurs données ne sera pas licite si l'enfant est âgé de moins de 16 ans. Dans le cas contraire, il faudra recueillir le consentement ou l'autorisation du titulaire de l'autorité parentale.

Cet article n'est donc pas applicable à tout traitement de données concernant des enfants mais uniquement à ceux concernant l'offre directe de services de la société de l'information. Cette notion résultant de la Directive 2015/1535 couvre « *tout service fourni, normalement contre rémunération, à distance au moyen d'équipement électronique de traitement (y compris la compression numérique) et de stockage des données, à la demande individuelle d'un destinataire de services* ».

L'âge des mineurs fait partie des dispositions pour lesquelles les États membres peuvent adopter des spécificités locales, sous réserve de ne pas l'abaisser en dessous de 13 ans. Dans le cadre du projet de loi relatif à la protection des données personnelles, le gouvernement aurait choisi de ne pas faire usage de cette faculté. Les députés par voie d'amendement ont cependant choisi de l'abaisser à 15 ans (art. 14 A), disposition supprimée par le Sénat.

DOCUMENT 9 : « *Protection des données personnelles* » éditions Législatives 2017, ouvrage collectif sous la direction de Laurent CHEVRY (pages 28 et 29 ; pages 200 à 203) (extraits)

Pages 28 et 29 : Conditions applicables au consentement

- Conditions générales applicables aux personnes majeures

Le consentement de la personne concernée consiste en toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que les données à caractère personnel la concernant fassent l'objet d'un traitement (RGPD, art. 4). Son expression a été renforcée, en comparaison de la directive 95/46/CE qui visait toute manifestation de volonté, libre, spécifique et informée (art. 2), sans nécessité d'un acte positif clair. Il pouvait donc être implicite.

L'article 7 précise le régime applicable aux traitements reposant sur le consentement de la personne concernée. D'abord, le responsable du traitement assume la charge de la preuve du fait que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant (§ 1). Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples (§ 2). Il est donc exclu que la collecte du consentement soit noyée dans des conditions générales de vente ou d'utilisation. Le consentement exprimant l'acceptation d'un contrat ne se confond pas avec le consentement au traitement des données personnelles, il faut donc en recueillir deux distincts. Sur les sites internet, le procédé de collecte doit faire l'objet d'une expression (case cochée par exemple) séparée des autres conditions d'utilisation du service ou d'expression de conclusion du contrat. En cas de violation de ces dispositions du RGPD, la déclaration ne sera pas contraignante.

En outre, le paragraphe 3 confère à la personne concernée le droit de retirer son consentement à tout moment, sous une forme aussi simple que son recueil. Afin de garantir une sécurité juridique du traitement qui a été à l'origine illicite, ce retrait n'a pas pour effet de compromettre la licéité du traitement antérieurement fondé sur le consentement qui s'est alors exprimé valablement. La personne concernée en est informée avant de donner son consentement.

Le caractère libre du consentement est particulièrement difficile à apprécier, aussi le RGPD prévoit qu'il convient de regarder si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel et si ce traitement est nécessaire à l'exécution dudit contrat (§ 4). Il apparaît en effet que des contrats de services, souvent gratuits, peuvent être offerts, en échange de collecte de données dont certaines peuvent ne pas être nécessaires à l'exécution du service mais sont destinées à être valorisées pour compenser la gratuité du service. Le législateur européen, conscient de ces dérives du modèle économique de nombreux services en ligne, tente ici de les juguler.

- Conditions spécifiques applicables aux enfants en ce qui concerne la société de l'information

Le législateur européen a également conscience que de nombreux jeunes enfants ou adolescents accèdent à des services en ligne en ayant manifestement un consentement peu libre et éclairé. Aussi l'article 8 tend-il à les protéger. Lorsque la licéité du traitement repose sur le consentement de la personne concernée (art 6 § 1, a) en ce qui concerne l'offre directe de service de la société d'information aux enfants, le traitement des données est âgé au moins de 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné et autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant (art. 8, § .1).

Cependant, une marge de manœuvre est laissée aux États membres qui peuvent prévoir par la loi un âge inférieur sans aller en dessous de 13 ans. Il y a donc là aussi une variété de législations nationales à l'égard des enfants âgés de 13 à 16 ans. En outre, le droit général des contrats des États membres, notamment les règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant a aussi vocation à s'appliquer (art. 8, § 3). Il appartient au responsable de du traitement de s'efforcer raisonnablement de vérifier que le consentement est donné au autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant compte tenu des moyens technologiques disponibles (art. 8 § 2).

Pages 200 à 203 : Gérer le consentement des personnes concernées

1. Le consentement, une notion clé dans le RGPD

Le consentement préalable est l'une des conditions de licéité d'un traitement des données à caractère personnel (RGPD, art. 6, § 1, a). La place que lui accorde le RGPD est essentielle. Le terme « *consentement* » y est cité pas moins de 68 fois dans un très grand nombre d'articles et de considérants. A titre d'exemple, le considérant 32 indique ce qu'on doit entendre par « *consentement* » au traitement de données à caractère personnel.
(Reproduction du Considérant 32 du RGPD).
Dès lors qu'il est libre, éclairé, spécifique à une finalité et donné de manière univoque, le consentement est le « *sésame* » qui permet un grand nombre de traitements de données personnelles. En effet, on considère que ce consentement, ainsi délivré, matérialise le contrôle dont dispose la personne physique sur ses données personnelles et sur les traitements qui en sont faits.

Il existe, bien entendu, d'autres fondements juridiques aux traitements des données à caractère personnel : exécution d'un contrat, respect d'une obligation légale, sauvegarde des intérêts vitaux de la personne, mission d'intérêt public, exercice de l'autorité publique ou encore intérêt « légitime » du responsable du traitement (RGPD, art. 6, § 1, b a f ; v. « *Conditions de licéité du traitement* », p. 26). Toutefois, le consentement est par excellence ce qui doit autoriser, au sein de la *data economy*, un très grand nombre de traitements.

La notion de consentement est donc centrale au sein du RGPD, mais aussi dans le futur règlement *ePrivacy* qui reprend et adapte les principes du RGPD pour les services de communications électroniques et l'ensemble des technologies de *tracking* (Doc. COM (2017) 10 final, 10 janv. 2017).

La rigueur des dispositions relatives à la gestion du consentement démontre l'importance accordée par le régulateur européen à l'exercice de ce droit. Le texte européen renforce ainsi deux principes qui préexistaient dans la directive 95/46/CE du 24 octobre 1995 et dans la loi Informatique et Libertés qui l'a transposée : la transparence des traitements (RGPD art. 13) et l'expression du consentement (RGPD, art. 6 à 8) dont il est expressément prévu qu'il peut être révoqué (RGPD, art. 7). Ces principes sont intimement liés car la personne doit

nécessairement être informée des caractéristiques du traitement avant de pouvoir consentir à celui-ci de manière éclairée. L'information circonstanciée, si elle peut suffire certains traitements, constitue donc le préalable indispensable à l'expression d'un consentement éclairé (v. "*Informer les personnes concernées*", p. 205).

- Exigence de précision pour les finalités du traitement

Notons que les finalités pour lesquelles sont collectées les données doivent être énoncées de manière spécifique, c'est-à-dire détaillée et précise, non évasive, ni équivoque. Il n'est plus question de mentionner des finalités qui seraient trop génériques ou englobantes, car ce serait prendre le risque que l'autorité de contrôle (la CNIL en France) considère le consentement comme trompé par le caractère trop vague ou générique des objectifs poursuivis.
Il faut, comme à chaque fois lorsqu'il s'agit d'interpréter le règlement, se placer du côté de la personne concernée, afin d'analyser ce à quoi elle peut s'attendre en prenant connaissance des finalités exposées. Elle ne délivre en effet son consentement que pour les finalités qui lui sont clairement exposées ou qu'elle peut légitimement et raisonnablement croire incluses dans le traitement que lui est présenté. (...)

- Conditions applicables au consentement

L'article 7 du RGPD pose les conditions applicables au consentement qui est recueilli auprès de la personne concernée :
- le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement. Cela implique donc de tracer et conserver la preuve que le consentement a été donné, ainsi que de la (ou des) finalité(s) pour lesquelles il a été donné ;
- la demande de consentement doit être présentée sous une forme compréhensible, aisément accessible, en des termes clairs et simples (les formules de recueil du consentement doivent donc être sincères et limpides) ;
- il doit apparaître clairement que l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement ;
- la personne concernée doit être informée qu'elle a le droit de retirer son consentement à tout moment, en précisant qu'il est aussi simple de retirer que de donner son consentement.
REMARQUE : cela érige en pratique le droit au retrait du consentement en un droit supplémentaire qui doit être expressément indiqué dans la liste des droits dont dispose la personne concernée sur ses données, à côté des droits d'accès, de rectification, d'effacement, de limitation ou de portabilité (v. « *Gérer les droits d'accès, de rectification, à limitation et d'opposition* », p. 213 ; « *Gérer le droit à l'effacement* » ou « *droit à l'oubli* », p. 225; « *Gérer le droit à la portabilité* », p. 230).

- Cas particulier des mineurs

En particulier, les conditions applicables au consentement des mineurs sont fixées par l'article 8 du RGPD, puisqu'ils ne sont pas dotés de la pleine capacité juridique et qu'il serait donc illusoire de prétendre exiger d'eux le consentement libre et éclairé qui leur fait par ailleurs défaut s'il s'agit de nouer un contrat. Ainsi, pour les enfants de moins de 16 ans, le consentement doit être donné par le titulaire de l'autorité parentale. Les États membres peuvent prévoir un âge inferieur, pour autant qu'il ne soit pas en dessous de 13 ans, mais le principe est bien celui, à l'instar du droit des contrats, qu'un représentant légal réputé en pleine possession de ses moyens, est seul habilité par la loi à délivrer un consentement pour le compte du mineur. Cela pose donc la question de l'information circonstanciée qu'on doit délivrer à ce représentant légal sur le sort des données du mineur.

- Traitement de données pour des nouvelles finalités

En vertu du RGPD, chaque donnée est collectée dans l'optique d'une finalité et chaque traitement est mis en œuvre pour parvenir à cette finalité précisément. La problématique des finalités secondaires se pose donc avec notamment le risque des finalités incompatibles qui s'ajoutent dans le temps. Après des débats houleux et plusieurs versions du texte, le règlement a finalement adopté une approche restrictive : une donnée ne peut être utilisée que pour la finalité annoncée, et pas pour une autre, fût-elle intellectuellement proche. Cependant, le traitement pour une finalité autre que celle pour laquelle le consentement a été donné est autorisé si le responsable du traitement détermine que la nouvelle finalité est « compatible » avec la finalité initiale, en tenant compte notamment (RGPD, art. 6, § 4) :

- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données ont été collectées et les finalités du traitement ultérieur envisagé ;
- du contexte dans lequel les données ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données, en particulier si le traitement porte sur des catégories de données sensibles ou si des données relatives à des condamnations pénales et à des infractions sont traitées ;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

(...)

DOCUMENT 10 : « *La protection des données personnelles de A à Z* », éditions Bruylant (Bruxelles 2017), ouvrage collectif sous la direction de Alain BENSOUSSAN (pages 46 et 47 ; pages 109 et 110) (extraits, sans les notes de bas de pages)

Lettre C, consentement :

230. Définition générale. Le traitement de certaines données est soumis au consentement de la personne concernée, c'est-à-dire à la manifestation de sa volonté d'accepter que des données à caractère personnel la concernant fassent l'objet d'un traitement.

231. Définition juridique. Alors que la loi Informatique et libertés ne définissait pas cette notion, le règlement général sur la protection des données apporte une définition précise du consentement dans le contexte de la protection des données à caractère personnel.

232. Le consentement de la personne concernée s'entend de toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

233. Commentaires. Lorsqu'un traitement est fondé sur le consentement de la personne concernée, le responsable du traitement doit être en mesure de prouver que la personne a consenti à l'opération. La charge de la preuve repose donc sur le responsable du traitement.

234. D'après le règlement général sur la protection des données, le consentement doit être donné par un acte positif "clair" par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant.

235. Du point de vue de la forme, le règlement prévoit que le consentement peut être donné au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Par exemple, il peut être formalisé en cochant une case lors de la consultation d'un site

internet, en optant pour certains paramètres techniques appropriés d'un navigateur ou d'une autre application ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données personnelles.

236. En revanche, le silence, des cases cochées par défaut ou une inactivité ne sauraient valoir consentement au sens du règlement général sur la protection des données.

237. Pour que le consentement soit éclairé, un mécanisme opérationnel, lisible et compréhensible doit être privilégié. Le consentement doit également être donné spécifiquement, notamment au regard de la finalité du traitement.

238. Pour que le consentement soit donné librement, le règlement général sur la protection des données invite à s'interroger sur la question suivante : l'exécution d'un contrat et notamment la fourniture d'un service sont-elles subordonnées au consentement à un traitement de données à caractère personnel qui ne serait pas nécessaire à l'exécution dudit contrat ?

239. Un tel mécanisme, qui ne laisse pas de choix réel à la personne concernée, devrait être proscrit. En effet, le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

240. Sur ce point, le G29, groupe des autorités de contrôle européennes, a déjà souligné le fait que le consentement ne peut être valable "*que si la personne concernée est véritablement en mesure d'exercer un choix s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne don pas son consentement*".

241. Enfin, la personne concernée dispose d'un véritable droit de retirer son consentement, à de tout moment aussi simplement qu'elle a pu le donner.

242. Concernant le recueil du consentement des enfants, le règlement européen prévoit des règles particulières.

Lettre E, Enfants :

582. Définition générale. L'enfant est généralement défini comme un être humain, sans différenciation de sexe, dans les premières années de sa vie et avant l'adolescence.

583. Définition juridique. Juridiquement, la loi associe le plus souvent l'enfant et l'adolescent et les regroupe sous le terme de mineur. C'est ainsi que l'article 1er de la Convention des Nations unies relative aux droits de l'enfant 461 définit l'enfant comme " *tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu d'une loi qui lui est applicable*".

584. Commentaires.

585. Protection spécifique. En raison de la vulnérabilité des enfants, des conditions de licéité spécifiques sont mises en place pour le traitement des données à caractère personnel les concernant.

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

587. Il est notamment indiqué au titre de la protection spécifique qui leur est accordée que "*toute information et communication, lorsque le traitement les concerne, devraient être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre*".

588. Pour consentir à un traitement de données, un enfant doit être âgé d'au moins seize ans. En-dessous de cet âge, il sera nécessaire de recueillir l'autorisation du titulaire de la responsabilité parentale pour que la collecte soit licite.

589. S'agissant de l'âge à prendre en compte, le règlement prévoit la possibilité pour les États membres de fixer un âge inférieur à seize ans mais supérieur à treize ans. La possibilité d'augmenter cette limite n'est pas envisagée. Dans la loi informatique et libertés, la question des mineurs est envisagée uniquement au sens de la minorité française, c'est-à-dire comme personne physique de moins de dix-huit ans.

590. Enfin, le règlement précise que la protection spécifique accordée aux enfants n'affecte pas les législations nationales en matière contractuelle qui comprendraient des règles spécifiques concernant notamment la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

DOCUMENT 11 : « *Droit de la donnée* », édition LexisNexis 2017, par Matthieu BOURGEOIS (extrait 1, sans notes de bas de pages)

6° Le consentement

246 - Le consentement, comme fondement juridique a un traitement de données à caractère personnel, fait l'objet de règles générales et de règles spéciales.

a) *Règles générales*

247- A la différence des autres fondements, le traitement s'appuie ici sur la volonté de la personne concernée.

248 - La portée de cette volonté n'est néanmoins pas toute puissante, puisqu'elle ne permet pas de valider un traitement ne répondant pas à l'exigence de proportionnalité (qui sera développée infra, n°316 et s.).

249 - Pour être valable, le consentement doit être donné de manière univoque, libre, spécifique et éclairé.

1. Caractère univoque

250 - Cette exigence signifie qu'un simple silence - suivi d'aucun comportement particulier - ne peut constituer un consentement valable.

251 - Le consentement doit être exprimé positivement, c'est-à-dire :

- soit de manière tacite, autrement dit résultant d'un comportement comme le fait d'opter, « *pour certains paramètres techniques, pour des services de la société de l'information* », ou d'adopter « *un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données* ». La LIL a retranscrit ces principes en matière de cookies et autres tracteurs, en prévoyant des dispositions spécifiques qui sont développées plus loin (V. infra, n° 631 et s).

- soit de manière expresse (écrite ou orale) (...).

2. Caractère libre

256. Conformément aux principes généraux, seul un consentement donné librement (c'est-à-dire dans "*tromperie*", "*intimidation*", ou menace de "*coercition*" est valable (...)

3. Le caractère spécifique

269 -Le caractère « *spécifique* » signifie que le consentement ne peut pas être de portée générale, et doit nécessairement porter sur un traitement précis.

270 - En pratique, cela signifie que le dispositif du recueil du consentement ne peut pas viser plusieurs traitements à la fois. Chacun d'entre eux doit être individualisé. Ainsi la personne concernée pourra donner, pour toute ou partie de ces traitements, son consentement spécifique.

271- Tant que les données continuent d'être traitées pour la finalité spécifique sur la base de laquelle a été recueilli le consentement, nul n'est besoin de renouveler ce recueil (...).

4. Le caractère éclairé

Cette exigence signifie que la personne concernée doit avoir reçu les informations relatives aux caractéristiques essentielles du traitement, avant d'avoir exprimé son consentement. La délivrance de ces informations, qui relève des obligations à la charge du responsable du traitement, sera examinée *infra*, n° 589 (...).

5. Le caractère précaire

275 - La directive n° 95/46 ne prévoyait pas, explicitement, la possibilité pour la personne concernée de retirer son consentement lorsque le traitement était fondé sur celui-ci.

276 - C'est désormais chose faite avec l'article 7.3 du RGPD qui prévoit :
« *La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement* ».
277 - Il résulte de ce texte que :
- en principe, le retrait du consentement n'a d'effet que sur le traitement futur des données, et non sur les opérations de traitement réalisées antérieurement à ce retrait : ainsi, les processus engagés dans le passé « *ne peuvent donc pas être purement et simplement annulés* » ;
- en revanche, toutes les opérations de traitement réalisées postérieurement au retrait du consentement devront cesser, à moins que le responsable ne puisse appuyer son traitement sur un autre fondement juridique que le consentement.

b) *Règles spéciales*

278 - Des dispositions spéciales s'appliquent lorsque le consentement sert de fondement a un traitement à des fins de prospection commerciale par voie électronique, ainsi que lorsqu'il porte sur les données d'un mineur.

(...)

1. Le consentement en cas de traitement à des fins de prospection commerciale par voie électronique

(...)

2. Consentement des mineurs

283 -La directive n° 95/46 ne posait aucune règle particulière relative au consentement des mineurs. Le G29 s'en était saisi et avait recommandé une harmonisation au niveau communautaire, notamment concernant les « *conditions permettant à des personnes incapables, d'exercer leurs droits* », ainsi qu'en ce qui concerne « *l'âge minimum* » de ces personnes pour que leur consentement soit considéré valable.

284 - C'est désormais une lacune qui vient d'être comblée avec le RGPD, dont l'article 8 prévoit un âge minimum (seize ans) au-dessus duquel le recueil du consentement de l'enfant est réputé valable, et en dessous duquel le traitement « *n'est licite que* [s'il] (...) *est donné ou autorisé par le titulaire de la responsabilité parentale* ».

285 - Le RGPD aménage la possibilité, pour les États membres, de « *prévoir par la loi un âge inferieur* » qui ne devra néanmoins pas être « *en dessous de treize ans* ».

286 - Lorsque le traitement concerne des mineurs d'un âge inferieur à ce seuil, le responsable du traitement devra alors s'efforcer « *raisonnablement de vérifier* (...) *que le consentement est donné* (...) *par le titulaire de la responsabilité parentale*".

DOCUMENT 12 : « *Droit de la donnée* », édition LexisNexis 2017, par Matthieu BOURGEOIS (extrait 2, sans notes de bas de pages) (pages 97 et s)

2) Régime

382 - Le traitement de données sensibles est interdit. Ce principe souffre néanmoins d'exceptions qu'il est possible de regrouper en neuf catégories de traitements.
a) Les traitements fondés sur le consentement exprès de la personne concernée

383 - Le traitement de données sensibles est possible lorsque la personne concernée a donné son « *consentement exprès* » (« *explicite* » indique le RGPD), sauf s'il existe une disposition spéciale, de droit national ou communautaire, privant d'effet le consentement en présence d'un traitement de données sensibles.

384 - C'est, par exemple, le cas de l'article L. 1111-18, alinéa 2 du Code de la sante publique, qui interdit l'accès par le professionnel (une compagnie d'assurance notamment) au dossier médical partagé lors de la souscription, par le client, d'un contrat relatif à une protection complémentaire en matière de frais de santé, ainsi qu'à l'occasion de tout autre contrat exigeant l'évaluation de l'état de santé de l'une des parties. Hormis ce cas, il sera possible de traiter des données sensibles avec le consentement des personnes concernées à la condition que celui-ci soit exprès, libre, spécifique et éclairé.

385 - « *Exprès* », c'est-à-dire exprimé par une action positive et explicite. Ainsi, en pratique, il conviendra de recueillir cet accord sous une forme écrite, par exemple au moyen d'une signature sur un formulaire ou une case à cocher (lorsqu'il s'agit d'un formulaire en ligne).

386 - « Libre », c'est-à-dire que la personne concernée ne doit subir aucune sanction en cas de refus. Ainsi, dans une délibération rendue à propos du service « *web médecin* », mis en œuvre pour permettre aux praticiens de santé de transmettre les données nécessaires au

remboursement des actes par l'assurance maladie, la CNIL a relevé que le refus, par le bénéficiaire, de remettre sa carte Vitale, n'emportait « aucune conséquence en matière de remboursement ».

387 - « *Spécifique* », ce qui signifie que le consentement ne peut concerner qu'un usage précisément défini des données (en l'occurrence des finalités claires et déterminées).

388 - « *Éclairé* », car la personne doit avoir reçu l'ensemble des informations exigées par les textes (V. infra, n°' 590 et s.).

DOCUMENT 13 : Le Monde, 14 mai 2018, « *Le Parlement adopte le projet de loi sur la protection des données personnelles* »

Onze jours à peine avant l'entrée en vigueur du règlement général sur la protection des données (RGPD), les dispositions de ce texte européen ont été inscrites dans la loi française, après un vote à l'Assemblée nationale, lundi 14 mai. Adopté en 2016 par le Parlement européen, le texte - qui régit la manière dont les entreprises et les administrations peuvent faire usage des données personnelles des utilisateurs - n'avait pas encore été transcrit en droit français. En France, ces pratiques étaient, pour l'instant, encadrées par la loi informatique et liberté de 1978 (modifiée par la directive européenne de 1995).

Malgré la procédure accélérée lancée par le gouvernement en décembre 2017, le texte s'est enlisé dans un fastidieux va-et-vient entre l'Assemblée nationale et le Sénat, dont les vues divergeaient sur de nombreux points. Le Senat réclamait, en particulier, un régime dérogatoire temporaire pour les collectivités territoriales. Il s'est également opposé à l'Assemblée sur des points plus spécifiques du texte, dont l'âge de la majorité numérique, à partir duquel un adolescent peut de lui-même donner son consentement au traitement de ses données personnelles.

DOCUMENT 14 : Projet de loi relatif à la protection des données personnelles, texte définitif voté par l'Assemblée Nationale le 14 mai 2018

(...)

Article 20
La section 1 du chapitre II de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 7-1 ainsi rédigé :
« *Art. 7-1. – En application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans* ».
« *Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur* ».
« *Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne.* » (...)

Article 28
En application de l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsque le traitement repose sur le consentement de la personne concernée, le responsable de traitement doit être en mesure de démontrer que les contrats qu'il conclut portant sur des équipements ou services incluant le traitement de données à

caractère personnel ne font pas obstacle au consentement de l'utilisateur final dans les conditions définies au 11 de l'article 4 du même règlement.
Peut en particulier faire obstacle à ce consentement le fait de restreindre sans motif légitime d'ordre technique ou de sécurité les possibilités de choix de l'utilisateur final, notamment lors de la configuration initiale du terminal, en matière de services de communication au public en ligne et aux applications accessibles sur un terminal, présentant des offres et des conditions d'utilisation de nature équivalente selon des niveaux différenciés de protection des données personnelles.

DOCUMENT 15 : Code civil, Livre premier, Titre onzième : De la majorité et des majeurs protégés par la loi

Article 414 : La majorité est fixée à dix-huit ans accomplis ; à cet âge, chacun est capable d'exercer les droits dont il a la jouissance.

DOCUMENT 16 : Capital, 25 janvier 2015, « *Et si, demain, vous vendiez vos données personnelles à Facebook* ? » par Samuel CHALOM (extraits)

Pouvoir se réapproprier nos données personnelles sur le web, c'est l'idée d'un rapport publié ce jeudi 25 janvier par le think tank libéral Génération Libre. Entretien avec sa directrice adjointe, Delphine Granier.

Le sujet est au cœur de notre vie quotidienne et, pourtant, nous n'y portons pas forcément attention. Que l'on s'inscrive sur Facebook, sur Instagram, ou encore sur Snapchat, nous acceptons d'y laisser nos données personnelles sans véritables contreparties des plateformes, si ce n'est d'accéder gratuitement aux services proposés. Dans un rapport publié jeudi 25 janvier, le think tank libéral Génération Libre, dirigé par le médiatique philosophe Gaspard Koenig, plaide pour la création d'un droit de propriété sur nos données personnelles (...).

Capital : Génération Libre, votre think tank, publie un rapport sur les données personnelles. De quel constat êtes-vous parti ?

Delphine Granier : Le point de départ, c'est que nous, internautes, sommes tous désemparés face aux GAFA (Google Apple Facebook Amazon). Nous nous en servons quotidiennement, mais nous n'avons aucun moyen de dire non au pillage des données. Tous les contrats et clauses que l'on signe n'ont en fait que peu d'importance. À partir de là, nous nous sommes demandé quelles solutions il était possible d'imaginer pour sortir de ce modèle.

Il y a trois possibilités. Soit on soutient que les données sont une sorte de bien public, et c'est donc à l'État d'en négocier directement l'usage avec les entreprises. Soit on adopte la logique des droits et obligations dans l'esprit de ce que fait déjà la Cnil dans l'Hexagone, et la Commission européenne avec le RGPD. Soit, enfin, on institue un droit de propriété de chaque usager sur ses données, ce qui est l'option des libéraux.

Et donc la vôtre, puisque Génération Libre est un think tank libéral...

Exactement. Nous considérons que puisque chaque personne génère des données, ces dernières doivent lui appartenir. Il faut donc introduire dans notre arsenal juridique un véritable droit de propriété sur nos données.

Très concrètement, si on prend l'exemple de Facebook qui, on le sait, se sert à l'envie de nos données, comment cela marcherait ?

L'idée est de pouvoir être payé pour ses données ou au contraire payer le service rendu par Facebook afin de pouvoir garder ses données privées. Concrètement, dans le cas de Facebook, on peut très bien imaginer à l'avenir que l'inscription sur le réseau social de Mark Zuckerberg laisse deux possibilités. Soit je (ne veux pas céder) mes données, et dans ce cas-là je paie l'accès à la plateforme. Soit je les vends à Facebook et suis rémunéré en fonction d'un prix de marché. On peut imaginer le même système avec les GPS et les applications qui utilisent nos données de géolocalisation.

Mais la possibilité laissée à tous de vendre ses données ne pose-t-elle pas des questions en termes de droit ?

En effet, le droit pose le principe selon lequel nous ne sommes pas propriétaires de nous-même. Or, dans notre conception, les données sont une extension de nous-même puisque nous seuls pouvons les générer. Afin de pouvoir introduire dans le droit cette notion de patrimonialité des données, nos juristes proposent de considérer la donnée comme un "objet" relevant du droit commun des biens, donc comme quelque chose d'appropriable.

(...)

Qu'attendez-vous de la publication de votre rapport ?

Nous sommes pragmatiques, nous savons très bien que nos propositions sont radicales et que donc, elles ne pourront pas être mises en œuvre dès demain. Nous souhaitons surtout créer un débat de société, comme cela a pu être le cas avec le revenu universel, que nous avions défendu dans un précédent rapport. L'idée progresse : aux Etats-Unis, elle est portée par certains chercheurs de la Silicon Valley comme Jaron Lanier. Il est temps d'ouvrir le débat en France aussi.
Nous espérons, ensuite, que nos propositions entreront un jour dans le droit français, puis dans le droit européen. Sur ce dernier point, nous nous réjouissons déjà de l'entrée en vigueur dès le mois de mai prochain du règlement général sur la protection des données (RGPD), qui pose comme principe que les GAFA et autres entreprises du Net ne sont pas les propriétaires de nos données, mais seulement les gardiennes. C'est l'esprit des articles du RGPD sur la portabilité des données ou sur le droit à l'oubli. C'est une première pierre vers une véritable réappropriation de notre data. Reprenons enfin le contrôle de nos données !

DOCUMENT 17 : Article 544 du Code Civil (créé par Loi n° 1804-01-27 promulguée le 6 février 1804)

La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements.

DOCUMENT 18 : Article 9 du Code civil (créé par Loi n° 1803-03-08 promulguée le 18 mars 1803, modifié par Loi n° 1927-08-10, par Loi n° 70-643 du 17 juillet 1970 et par Loi n° 94-653 du 29 juillet 1994)

Chacun a droit au respect de sa vie privée.

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telle que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de sa vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.

DOCUMENT 19 : Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (JORF n° 0235 du 8 octobre 2016) (extraits)

Chapitre II : Protection de la vie privée en ligne

Section 1 : Protection des données à caractère personnel

Article 54 :

L'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est complété par un alinéa ainsi rédigé : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

DOCUMENT 20 : « *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information* », Rapport d'information n° 441 (2008-2009) de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, fait au nom de la commission des lois du Sénat, déposé le 27 mai 2009 (extraits)

a) La notion de droit de propriété sur ses données personnelles : une fausse bonne idée

À plusieurs reprises, la reconnaissance d'un droit de propriété sur ses données personnelles a été avancée. L'idée, séduisante, serait de faire de chaque individu le véritable maître de son identité numérique. Chacun pourrait gérer ses données en les louant, prêtant, récupérant, etc. Toutefois, le concept de propriété n'apporte pas de réponses adéquates et pourrait poser plus de problèmes encore. Notre conception de la vie privée place sa protection sur le terrain de la dignité humaine. En se référant au concept de propriété, le risque de marchandisation de ses données personnelles est évident. La propriété comprend aussi le droit de céder la chose. Or, comment pourrait-on céder une donnée qui peut aussi être un attribut de sa personnalité ? Faut-il imaginer des droits d'exclusivité ?

Il pourrait être objecté que le droit à l'image est d'ores et déjà un droit patrimonial et peut donner lieu à l'établissement de contrats.

Mais ce régime juridique est inadapté aux enjeux d'Internet. Comment y faire valoir ses droits de propriété quand on a soi-même diffusé une donnée personnelle ? Quant aux informations relatives à sa vie publique, il ne peut être question d'un droit de propriété à moins de remettre en cause fondamentalement la liberté d'expression.

Enfin, lorsque le rapport de force entre des contractants est inégal, quelle valeur donner au consentement à contracter ?

DOCUMENT 21 : Code civil, Livre troisième, Titre trois : Des sources d'obligations

Article 1128 (Ordonnance n° 2016-131 du 10 février 2016, art. 2 en vigueur le 1er octobre 2016)

Sont nécessaires à la validité d'un contrat :

1° - Le consentement des parties
2° - Leur capacité de contracter
3° - Un contenu licite et certain