François Barrière et Natalia Rotaru

Journée européenne de la protection des données

Dans un contexte de généralisation de l'outil informatique, de développement exponentiel des nouvelles technologies et de l'intelligence artificielle, le droit à la protection des données à caractère personnel est aujourd'hui considéré comme étant un droit humain fondamental[1]. Cela s'explique notamment par les nombreuses interactions et liens d'interdépendance qu'entretient ce droit avec d'autres droits fondamentaux, tels que le droit au respect de la vie privée et familiale, du domicile et des communications, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, ainsi que le droit à la diversité culturelle, religieuse et linguistique. La Charte des droits fondamentaux de l'Union européenne[2], ainsi que le Traité sur le fonctionnement de l'Union européenne[3] disposent que toute personne a droit à la protection de ses données à caractère personnel.

Chaque jour, des données nous concernant (nom, adresse, données de localisation, etc.) font l'objet de multiples opérations de traitement (collecte, enregistrement, diffusion, etc.), tel est par exemple le cas lorsque nous procédons à un achat sur un site Internet ou utilisons notre abonnement pour accéder aux transports en commun, ou encore lorsque nous mettons à jour notre profil LinkedIn. Les mérites et utilités de ces opérations dans la vie courante sont incontestables mais tels sont également les risques et dangers qu'elles génèrent. Les opérations de traitement de données à caractère personnel présentent en effet des risques importants d'atteinte à la vie privée[4] dans toutes ses déclinaisons, tels que les risques de traçabilité, de discrimination, de vol ou d'usurpation d'identité, etc. Or, selon la loi dite « Informatique et Libertés »[5], "*l'informatique doit être au service de chaque citoyen. […] Elle [l'informatique] ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*".

Deux séries de règles juridiques – l'une européenne, l'autre française – sont venues instaurer un cadre protecteur des données à caractère personnel. Au niveau de l'Union européen, c'est notamment le Règlement

---

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant (1).

2 Article 8, paragraphe 1.

3 Article 16, paragraphe 1.

4 Le droit au respect de la vie privée est notamment protégé par l'article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948, l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et l'article 17 du Pacte international relatif aux droits civils et politiques du 16 décembre 1966.

5 L. n° 78-17, mod. par Ord. n° 2018-1125, 12 déc. 2018, art. 1er.

général sur la protection des données du 27 avril 2016[6] (« RGPD ») et la directive (UE) du 27 avril 2016 relative aux traitements de données personnelles en matière pénale[7] qui constituent le socle de la protection des données personnelles. En droit français, cette protection est notamment assurée par la loi du 6 janvier 1978 dite « Loi Informatique et libertés »[8], telle que modifiée par la loi du 20 juin 2018[9]. Ces dispositions visent à garantir la protection des personnes physiques lorsque leurs données à caractère personnel font l'objet d'une opération de traitement.

Les données à caractère personnel visées par cette réglementation sont toutes les informations qui se rapportent à une personne physique susceptible d'être identifiée, directement ou indirectement[10]. Sont notamment des données à caractère personnel les nom, prénom, numéro de carte d'identité, adresse, numéro de téléphone, données de localisation, adresse de protocole internet (IP), cookies, voix, image d'une personne ou élément(s) spécifique(s) propre(s) à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Quant à l'opération de traitement[11] des données, elle s'entend de toute opération effectuée sur des données à caractère personnel, de manière automatisée ou manuelle telles que, notamment, la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la consultation, la transmission, la diffusion, l'effacement ou la destruction. Constituent, par exemple, des opérations de traitement l'envoi des courriels promotionnels, l'enregistrement de vidéosurveillance, la conservation des adresses IP ou encore la publication d'une photo d'une personne sur un site internet.

Le champ d'application territorial de cette réglementation est assez étendu, elle protège toutes les personnes physiques se trouvant sur le territoire de l'Union européenne (qu'elles soient ou non ressortissantes d'un Etat membre) et s'applique à toutes les opérations de traitement réalisées sur le territoire de l'Union. D'un point de vue matériel, le champ d'application de ces dispositions est également particulièrement large et s'applique à toute opération de traitement de données à caractère personnel, à l'exception de celles réalisées par une personne physique au cours d'activités strictement personnelles ou domestiques.

---

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

7 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

8 L. n° 78-17, mod. par Ord. n° 2018-1125, 12 déc. 2018, art. 1er.

9 LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

10 Article 4, paragraphe 1 du RGPD.

11 Article 4, paragraphe 2 du RGPD.

L'esprit général de cette règlementation est de mettre en œuvre une approche par les risques. Il appartient en effet au responsable du traitement[12] d'identifier les risques d'atteinte à la vie privée des personnes concernées et de mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel faisant l'objet du traitement.

Quelle que soit l'étendue des risques identifiés par le responsable du traitement, le RGPD et la Loi Informatique et Libertés prévoient une série de principes généraux applicables en toutes circonstances (I), ainsi qu'une liste de droits expressément reconnus aux personnes dont les données à caractère personnel font l'objet d'un traitement (II).

I. Principes généraux du traitement des données à caractère personnel

Un traitement de données à caractère personnel ne peut être légalement mis en œuvre que s'il est fondé sur l'une des six bases légales prévues par le RGPD[13], à savoir :

- le consentement : la personne concernée consent de manière libre, éclairée, spécifique et expresse au traitement de ses données. Le recueil du consentement préalable est particulièrement nécessaire en matière de cookies[14] (et autres traceurs) liés à l'affichage publicitaire (personnalisée ou non) ou à des fins de partage sur les réseaux sociaux[15], qui ne peuvent être déposés ou lus sur un terminal, tant que la personne concernée n'a pas donné son consentement[16]. Le responsable du traitement (éditeur du site web, régie publicitaire, réseau social, etc.) doit donc permettre à l'utilisateur de consentir par un acte positif préalable à l'utilisation de cookies mais aussi de choisir les cookies qu'il autorise ou non en fonction de leurs finalités[17].

---

12 Défini comme toute personne morale quelle que soit sa forme ou sa taille, une entreprise, une association ou un organisme public et, dans certaines conditions, un particulier, qui détermine les finalités et les moyens d'un traitement des données à caractère personnel est considéré comme responsable de traitement (article 4, paragraphe 7 du RGPD).

13 Article 6 du RGPD.

14 Les cookies sont des fichiers texte déposés par le navigateur sur un ordinateur lors de visites sur des sites Internet afin de conserver les informations de navigation sur ces sites. Les cookies permettent ainsi de sauvegarder les login et mot de passe, de retrouver son panier sur un site de shopping ou encore de se connecter à un site directement via un réseau social sans rentrer à nouveau les informations d'identification.

15 Article 5 du RGPD ; Article 82 de la Loi Informatique et Libertés.

16 Les traceurs strictement nécessaires à la fourniture d'un service de communication en ligne ou permettant la transmission de la communication par voie électronique ne nécessitent cependant pas le recueil du consentement préalable de la personne concernée.

17 Délibération CNIL n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ». Délibération CNIL n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

- le contrat : 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 sa demande ;
- l'obligation légale : le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'un tiers ;
- la mission d'intérêt public : 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 ; ou
- l'intérêt légitime : le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers sauf si les intérêts, libertés et droits fondamentaux de la personne concernée prévalent, notamment lorsque la personne concernée est un enfant.

Chacune de ces bases légales est soumise à des conditions spécifiques et entraine des conséquences différentes sur l'étendue des droits de la personne concernée. Néanmoins, quelle que soit la base légale du traitement, celui-ci devra impérativement respecter plusieurs autres principes fondamentaux, tels que rappelés ci-après.

A. Limitation des finalités

Tant le RGPD[18] que la Loi Informatique et Libertés[19] disposent, dans les mêmes termes, que pour être licite, le traitement de données à caractère personnel doit être assorti d'une finalité. Cela signifie que la collecte de données ne peut pas être une finalité en soi et qu'elle doit viser un objectif précis identifié en amont.

Aux termes des dispositions précitées, la finalité du traitement doit être déterminée, explicite et légitime. Elle est considérée comme déterminée lorsque les objectifs de la collecte sont précisément identifiés, sans recours à des formulations vagues ou trop générales. Pour être explicite, la finalité du traitement doit être formulée clairement et de manière accessible afin de permettre à la personne concernée de comprendre les utilisations de ses données qui sont incluses ou exclues du traitement. La finalité du traitement ne serait par ailleurs légitime que si elle repose sur l'une des six bases légales évoquées *supra*. Constituent par exemple des finalités de traitement déterminées, explicites et légitimes la gestion de la clientèle, la gestion du compte retraite, la mise en place d'une enquête de satisfaction, etc.

La finalité ainsi déterminée doit être communiquée à la personne concernée en amont de la collecte et doit être respectée pour tout traitement ultérieur. En effet, les données collectées ne peuvent pas être traitées ultérieurement d'une manière incompatible avec la finalité initiale, étant précisé que le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales.[20]

---

18 Article 5, paragraphe 1, b) du RGPD.
19 Article 6, 2° de la Loi Informatique et Libertés.
20 Article 6 Loi Informatique et Libertés.

B. Loyauté, licéité et transparence de la collecte de données

Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée[21].

La condition de licéité exige que le traitement ne soit pas prohibé par un texte et qu'il repose sur l'une des six bases légales évoquées *supra*.

S'agissant du caractère loyal du traitement, celui-ci est plus délicat à définir et repose sur le respect par le responsable du traitement de plusieurs obligations dont, notamment, l'obligation de collecter les données directement auprès de la personne concernée. Est par conséquent prohibé le traitement de données collectées de manière indirecte, à l'insu de la personne concernée. Dans un arrêt du 14 mars 2006[22], la Cour de cassation a ainsi jugé déloyal un procédé consistant à « *recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet* ».

Quant à l'obligation de transparence, elle est intrinsèquement liée à celle de loyauté et impose d'informer la personne concernée de l'identité du responsable du traitement, des finalités du traitement et des droits en lien avec ce traitement. Cette information doit en outre être rédigée en des termes clairs et simples et être facilement accessible et compréhensible pour la personne concernée.

C. Proportionnalité et minimisation des données

Tant le RGPD[23] que la Loi Informatique et Libertés[24] disposent que les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Le responsable du traitement est ainsi tenu au respect d'un principe de proportionnalité qui est en réalité composé de plusieurs obligations :

- la collecte doit être limitée à une quantité minimale de données, strictement nécessaires à l'opération de traitement envisagée ;
- les données à caractère personnel collectées doivent être en lien avec la finalité du traitement ; et
- les données collectées doivent être utiles au regard de la finalité définie en amont de la collecte.

Le respect du principe de proportionnalité s'apprécie via une mise en perspective de la finalité du traitement avec la nature des données collectées. A titre d'exemple, la CNIL indique que le recueil d'information sur la situation professionnelle de l'entourage d'un candidat n'est pas justifié dans un fichier de recrutement, ces données étant non pertinentes et excessives au regard de l'objectif poursuivi.

---

21 Article 5-a du RGPD.
22 Cass. Crim. 14 mars 2006, n°05-83-423.
23 Article 5-c du RGPD.
24 Article 6, 3° de la Loi Informatique et Libertés.

D. Détermination de la durée de conservation des données

Les données doivent être conservées par le responsable du traitement sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.[25] En vertu de cette disposition, la durée de conservation des données collectées doit être limitée au strict minimum et ne peut en aucun cas être illimitée. Ce principe a pour corolaires le droit au déférencement et le droit à l'effacement des données, qui sont deux composantes du « *droit à l'oubli numérique* »[26].

La durée de conservation doit être fixée par le responsable du traitement au regard de la finalité du traitement mais aussi du risque d'atteinte à la vie privée de la personne concernée. En pratique, la détermination du délai de conservation est délicate et repose sur une estimation subjective du responsable du traitement qui peut, à cette fin, reposer sur les délibérations de la CNIL ou les usages professionnels dans le secteur concerné.

A l'expiration de la durée de conservation fixée par le responsable du traitement, les données doivent être supprimées. Elles ne pourront être conservées pour des durées plus longues que dans des cas limités, prévus par la loi, à savoir, (i) à des fins archivistiques dans l'intérêt public, (ii) à des fins de recherche scientifique ou historique ou (iii) à des fins statistiques, et pour autant que les droits de la personne concernée continuent à être garantis[27].

E. Sécurité et confidentialité des données

Le traitement doit être mis en œuvre de façon à garantir une sécurité et intégrité appropriées des données à caractère personnel, y compris pour prévenir le traitement non autorisé ou illicite, la perte, la destruction ou les dégâts d'origine accidentelle[28]. Cette obligation de sécurité est fondamentale pour garantir le droit au respect de la vie privée des personnes dont les données sont collectées.

L'obligation de sécurité incombe principalement au responsable du traitement qui doit mettre en œuvre toutes les mesures techniques ou organisationnelles appropriées au regard de la nature des données et des risques présentés par le traitement. Ces mesures de sécurité peuvent par exemple consister en la pseudonymisation et le chiffrement des données à caractère personnel, la mise en place de moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ou la mise en place d'une procédure visant à tester, à analyser et à évaluer

25 Article 5-e du RGPD.
26 V. ci-dessous pour plus de détails.
27 *Ibid.*
28 Article 5-f du RGPD ; Article 34 de la loi Informatique et Libertés.

régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement[29].

F. Encadrement des transferts de données en dehors de l'Union européenne

Aux termes du RGPD[30], le responsable du traitement est autorisé à exporter et importer librement des données à caractère personnel au sein de l'Union européenne, sans avoir à accomplir de formalités spécifiques. Cependant, le transfert de données hors l'Union européenne et l'Espace économique européen (EEE) ne peut intervenir qu'à condition d'assurer un niveau de protection des données suffisant et approprié et conformément à la réglementation applicable.

Le RGPD propose différents outils juridiques à cet effet, tels que l'existence d'une décision de la Commission européenne constatant que le pays tiers de destination des données assure un niveau de protection adéquat[31], la stipulation de clauses contractuelles type adoptées par une autorité de contrôle et approuvées par la Commission européenne[32], la mise en œuvre d'un plan de conduite approuvé par le destinataire des données[33], etc.

G. Interdiction de collecter certaines catégories de données

Le risque d'atteinte à la vie privée d'une personne physique est particulièrement élevé lorsque les données collectées révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ou lorsque le traitement concerne 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

---

29 Article 32 du RGPD.

30 Article 44 et sv. du RGPD.

31 Dans un arrêt dit Schrems II du 16 juin 2020, la Cour de justice de l'Union européenne (CJUE) a cependant invalidé le régime de transfert de données entre l'Union européenne et les Etats-Unis dit « Privacy shield », en estimant que le droit américain n'assure pas un niveau de protection essentiellement équivalent à celui prévu par le RGPD (V. notamment https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf). Le transfert de données entre l'Union européenne et les Etats-Unis pourrait toutefois intervenir sur la base des Clauses Contractuelles Types (CCT) de la Commision européenne.

32 Les Clauses Contractuelles Types (CCT) de la Commision européenne ont été mises à jour suite à l'arrêt Schrems II précité, dans lequel la CJUE indique qu'en règle générale, les CCT peuvent toujours être utilisées pour transférer des données vers un pays tiers (qu'il s'agisse des États-Unis ou d'un autre pays tiers). Cependant, elle souligne qu'il incombe à l'exportateur et à l'importateur de données d'évaluer en pratique si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l'UE et les garanties fournies par les CCT (V. aussi https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne).

33 La CNIL conseille à cet effet aux responsables de traitements de mettre en place des règles d'entreprise contraignantes (BCR), qui constituent un outil d'encadrement global des transferts de données hors UE : https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr

physique. Aux termes de l'article 9 du RGPD, ces données dites « sensibles » font l'objet d'un régime de protection renforcé – leurs collecte et traitement sont en principe interdits.
Cette interdiction de principe est néanmoins assortie de plusieurs exceptions[34], dont notamment :

- la personne concernée a donné son consentement explicite au traitement de ses données ;
- les données sont rendues publiques par la personne concernée ;
- le traitement de ces données est nécessaire à la sauvegarde de la vie humaine ;
- le traitement est justifié par l'intérêt public et autorisé par la CNIL ; ou
- le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

Une autre catégorie de données dites « sensibles », soumise à un régime protecteur renforcé concerne les données relatives aux infractions, condamnations et mesures de sûreté. Aux termes de l'article 10 du RGPD, le traitement de ces données ne peut être effectué que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

II. Droits de la personne concernée

La personne concernée par le traitement dispose de plusieurs droits qui lui permettent de garder le contrôle et la maîtrise de ses données. Les conditions d'exercice et la portée de chacun de ces droits ne sont pas identiques, néanmoins, ils répondent tous à quelques caractéristiques communes[35] :

- quel que soit le droit en cause, la personne concernée doit s'adresser au responsable du traitement, qui est le principal débiteur pour satisfaire ses demandes ;
- aucun frais ne doit être mis à la charge de la personne concernée dans le cadre de l'exercice de ses droits, sauf si le responsable du traitement prouve que les demandes sont infondées ou excessives, « *notamment en raison de leur caractère répétitif* »[36] ;
- le responsable du traitement est tenu de traiter la demande de la personne concernée dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à 3 mois compte tenu de la complexité et du nombre de demandes ;
- exceptionnellement, l'organisme pourra demander à vérifier l'identité de la personne concernée s'il existe un doute raisonnable sur son identité, sans toutefois pouvoir demander la fourniture de pièces justificatives abusives, non pertinentes ou disproportionnées ;[37]
- en cas d'inertie ou de réponse insatisfaisante du responsable du traitement dans un délai raisonnable, la personne concernée peut saisir la CNIL pour obtenir satisfaction de sa demande.

[34] Article 9, paragraphe 2 du RGPD.
[35] Article 12 du RGPD.
[36] Article 12, paragraphe 5 du RGPD.
[37] Article 12, paragraphe 6 du RGPD.

A. Droit à l'information sur l'utilisation des données

La personne concernée a le droit d'être informée de l'existence et de la portée de l'opération de traitement portant sur ses données à caractère personnel ainsi que des modalités d'exercice de ses droits en lien avec ce traitement.[38] Le droit à l'information est ainsi une condition nécessaire et préalable à l'exercice des autres droits.

La personne dont les données sont collectées a le droit de demander et d'obtenir du responsable du traitement la communication des informations relatives, notamment, (i) aux coordonnées du responsable du traitement, de son représentant et de son délégué à la protection des données, (ii) à la durée de conservation des données, (iii) aux intérêts légitimes poursuivis par cette collecte, (iv) au transfert éventuel de ses données vers un pays hors Union européenne, (v) à l'existence d'une prise de décision automatisée et, de manière plus générale, (vi) à l'ensemble de ses droits tels que décrits ci-après.[39]

Ces informations doivent être présentées de façon « *concise*, *transparente*, *compréhensible et aisément accessible* » pour la personne concernée[40], qui doit être mise en mesure de comprendre ces informations sans difficulté et sans avoir besoin d'être un expert dans ce domaine.[41] Lorsque le traitement de données concerne des personnes vulnérables, l'information doit être d'autant plus adaptée, tel est notamment le cas lorsque la collecte est réalisée auprès d'un mineur de moins de 15 ans.[42]

B. Droit d'opposition au traitement des données

Le droit d'opposition a pour objet que de faire cesser l'utilisation de données à caractère personnel pour une finalité précise sans nécessairement aboutir à leur suppression (laquelle pourrait néanmoins être obtenue via le droit à l'effacement).

Ce droit d'opposition peut être exercé par la personne concernée à tout moment et par tout moyen (courrier, formulaire électronique, adresse mail, compte en ligne, etc.). L'opposition ne pourra cependant aboutir que si elle est justifiée par des motifs tenant à la « *situation particulière* »[43] de la personne concernée. Une telle justification n'est toutefois pas nécessaire en cas de prospection commerciale, à laquelle la personne

38 Articles 12, 13 et 14 du RGPD ; Article 48 de la Loi Informatique et Libertés.
39 Article 13 du RGPD.
40 Article 12, paragraphe 1 du RGPD.
41 Site de la CNIL, Comprendre mes droits, Le droit d'information : https://www.cnil.fr/fr/le-droit-detre-informe-sur-lutilisation-de-vos-donnees-0
42 Article 12, paragraphe 1 du RGPD ; Article 48, al. 2 de la Loi Informatique et Libertés.
43 Article 21, paragraphe 1 du RGPD.

concernée peut s'opposer sans avoir à invoquer un motif particulier, la simple manifestation de l'opposition étant suffisante.[44]

En cas d'opposition à une opération de prospection commerciale, le responsable du traitement n'a aucune marge d'appréciation et doit cesser le traitement des données concernées dans les meilleurs délais. Dans les autres cas d'opposition, le responsable du traitement dispose cependant d'une marge d'appréciation et pourra refuser la demande d'opposition en justifiant (i) soit de motifs légitimes et impérieux[45], (ii) soit de la nécessité du traitement pour la constatation, l'exercice ou la défense de droits en justice[46], (iii) soit d'une obligation légale lui imposant ce traitement[47], (iv) soit encore de l'existence d'un contrat liant la personne concernée au responsable du traitement ou (v) lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'un tiers[48]. Ce droit d'opposition ne pourra par ailleurs pas être exercé si la personne concernée a déjà donné son consentement à l'opération de traitement, auquel cas elle devrait procéder à un retrait de consentement (via le droit à l'effacement), plutôt qu'à une opposition.

C. Droit d'accès aux données

Le droit d'accès vient compléter le droit à l'information (qui est exercé en amont du traitement) et permet à la personne concernée d'obtenir des informations en temps réel sur une opération de traitement afin de pouvoir, le cas échéant, exercer ses droits subséquents, tels que les droits de rectification ou d'effacement.

Le droit d'accès aux données comprend le droit d'obtenir confirmation de l'existence d'un traitement, le droit d'obtenir communication des données personnelles concernées ainsi que le droit d'obtenir des informations relatives à l'opération de traitement elle-même.[49]

Sur demande de la personne concernée, l'organisme responsable du traitement (que ce soit un site Internet, un assureur, une banque, etc.) devra lui fournir gratuitement une copie des données qu'il a collectées, dans un format compréhensible et sans que la personne concernée n'ait à justifier sa demande. Il devra en outre renseigner la personne concernée sur les modalités du traitement (finalité, durée de conservation, l'existence d'une prise de décision automatisée, etc.).

Le droit d'accès n'est soumis à aucune condition dès lors que la demande n'est pas manifestement abusive. Cette affirmation ne vaut cependant pas en ce qui concerne les données contenues dans certains fichiers de

---

44 Article 21, paragraphe 2 du RGPD ; Article 56 de la Loi Informatique et Libertés.
45 Article 21, paragraphe 1 du RGPD.
46 *Ibid.*
47 Article 56 de la Loi Informatique et Libertés.
48 Site de la CNIL, Comprendre mes droits, Le droit d'opposition : refuser l'utilisation de vos données : https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees
49 Article 15 du RGPD ; Article 49 de la Loi Informatique et Libertés.

police ou intéressant la sûreté de l'Etat, pour lesquelles le droit d'accès ne peut être mis en œuvre directement que par l'intermédiaire de la CNIL et à condition que la demande ne soit pas infondée ou abusive.[50]

D. Droit de rectification des données

Dans le cas où les données personnelles collectées par l'organisme responsable du traitement seraient inexactes (numéro de téléphone erroné, par exemple) ou incomplètes (année de naissance sans indication du jour et mois, etc.), la personne concernée peut obtenir que ses données soient corrigées ou complétées[51]. Ce droit permet ainsi à la personne concernée de s'assurer que les données faisant l'objet du traitement sont à tout moment exactes, complètes et si nécessaire, mises à jour, compte tenu des finalités du traitement.

L'exercice du droit de rectification n'est soumis à aucune condition autre que la preuve du caractère inexact, incomplet, périmé ou équivoque de l'information. Le droit de rectification n'est toutefois pas absolu et ne peut pas être exercé lorsque le traitement porte sur des données journalistiques, artistiques ou littéraires.[52] Un régime spécial de rectification est en outre prévu pour les données contenues dans les fichiers de police, de renseignement, de gendarmerie et de FICOBA[53], pour la rectification desquelles l'intervention d'un magistrat de la CNIL est nécessaire[54].

E. Droit à l'effacement des données

La personne concernée a le droit de demander au responsable du traitement l'effacement des données à caractère personnel la concernant, sous certaines conditions.[55] Pour pouvoir aboutir, la demande d'effacement doit obligatoirement être fondée sur l'un des motifs suivants :

- les données sont utilisées à des fins de prospection ;
- les données ne sont plus nécessaires au regard des objectifs pour lesquels elles ont été collectées ou traitées ;
- la personne concernée retire le consentement au traitement de ses données ;
- la personne concernée s'oppose au traitement et le responsable du traitement ne démontre pas l'existence d'un motif légitime impérieux pour le traitement ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;

---

50 Site de la CNIL, Comprendre mes droits, Le droit d'accès : connaître les données qu'un organisme détient sur vous, https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous

51 Article 16 du RGPD ; Article 50 de la Loi Informatique et Libertés.

52 Site de la CNIL, Comprendre mes droits, Le droit de rectification : corriger vos informations : https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations

53 Fichier national des comptes bancaires et assimilés.

54 Site de la CNIL, Comprendre mes droits, Le droit de rectification : corriger vos informations : https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations

55 Article 17 du RGPD ; Article 51 de la Loi Informatique et Libertés.

- les données ont été collectées par une société de l'information (par exemple un forum ou réseau social) alors que la personne concernée était mineure au moment de la collecte ;[56]
- les données à caractère personnel doivent être effacées pour respecter une obligation légale.

Si l'organisme a rendu publiques les données avant l'exercice de ce droit d'effacement, il est tenu de prendre des mesures raisonnables pour informer tout autre responsable de la demande d'effacement de ces données[57].

Même en présence d'un motif légitime, le responsable du traitement peut cependant refuser de procéder à l'effacement des données lorsque le traitement de ces données est nécessaire à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ainsi qu'à des fins de constatation, de l'exercice ou de la défense de droits en justice.[58]

F. Droit au déréférencement d'un contenu dans un moteur de recherche

Le droit au déréférencement permet à la personne concernée de demander à un moteur de recherche (tels que Google ou Yahoo), de supprimer certains résultats de recherche associés à ses nom et prénom lorsque ceux-ci lui portent préjudice. Ce déréférencement aboutit à la suppression des liens vers des pages web qui contiendraient des données à caractère personnel, sans pour autant supprimer ces informations du site Internet source[59] (dont le contenu original reste inchangé et est toujours accessible en utilisant d'autres critères de recherche) qui ne peut être obtenue qu'auprès de l'éditeur du site Internet (en vertu du droit à l'effacement)[60].

Le droit au déréférencement, ensemble avec le droit à l'effacement des données, constituent les deux composantes du « *droit à l'oubli numérique* » consacré pour la première fois au niveau européen par l'arrêt Google Spain c/ AEPD et Costeja Gonzales du 13 mai 2014. Dans cette affaire, la Cour de justice de l'Union européenne (CJUE) énonce que, si la personne concernée se prévaut d'un motif légitime, « *l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne* ». La CJUE a donc accepté de faire primer le droit à la protection

56 Article 17 du RGPD. Article 51, paragraphe II de la Loi Informatique et Libertés.
57 Article 17, paragraphe 2 du RGPD.
58 Article 17, paragraphe 3 du RGPD.
59 Site de la CNIL, Comprendre mes droits, Le droit au déréférencement : https://www.cnil.fr/fr/le-dereferencement-dun-contenu-dans-un-moteur-de-recherche
60 CJUE, grde ch., 13 mai 2014, aff. C-131/12, Google Spain et Google : JurisData n° 2014-009597

de la vie privée de la personne concernée sur l'intérêt économique de l'exploitant du moteur de recherche mais aussi sur l'intérêt du public à accéder à l'information déréférencée[61].

Ce droit n'est toutefois pas absolu puisque l'opportunité de la suppression des données pourra être appréciée au cas par cas par le moteur de recherche en fonction de la nature de l'information, de sa sensibilité au regard de la vie privée et de son intérêt pour le public.[62]

G. Droit à la portabilité des données

Le droit à la portabilité permet aux personnes concernées de récupérer leurs données à caractère personnel faisant l'objet d'une opération de traitement, soit afin de les transmettre à un autre responsable de traitements, soit pour en faire une utilisation personnelle[63]. Ces données doivent être fournies par le responsable du traitement dans un format « *structuré, couramment utilisé et lisible par une machine* »[64]. La personne concernée peut même demander la transmission directe de ses données entre les deux responsables de traitements sans qu'elle n'ait à intervenir, à moins que l'organisme à l'origine du traitement ne justifie de l'impossibilité technique de cette transmission.

L'exercice du droit à la portabilité est cependant sujet à 3 conditions cumulatives. Premièrement, la portabilité ne peut porter que sur les données fournies directement par la personne concernée (nom, téléphone, adresse, etc.) ou générées par celles-ci (par exemple, historique des achats enregistrés grâce à une carte de fidélité), à l'exception des données dérivées ou inférées à partir de ces informations (par exemple, analyse de risque de crédit réalisée par une banque). Deuxièmement, le droit à la portabilité ne peut être exercé que si les données sont traitées de manière automatisée et sur la base du consentement de la personne concernée ou dans le cadre de l'exécution d'un contrat. Troisièmement, l'exercice du droit à la portabilité ne doit pas porter atteinte aux droits et libertés des tiers. Lorsque ces conditions ne sont pas réunies, la personne concernée conserve néanmoins un droit d'accès à ses données.

H. Droit à l'intervention humaine face au profilage ou à une décision automatisée

Le « profilage » constitue une forme de traitement de données à caractère personnel d'un individu en vue d'analyser et prédire son comportement, notamment en ce qui concerne sa performance au travail, sa situation financière, sa santé, ses intérêts, ses habitudes d'achats, sa localisation, ses déplacements, etc.[65]

---

61 V. également CJUE, grde ch., 24 septembre 2019, aff. C-507/17, Google c/ CNIL, et les 13 arrêts du Conseil d'Etat du 6 décembre 2019 : n° 391000 ; n° 393769 ; n° 395335 ; n° 397755 ; n° 399999 ; n° 401258 ; n° 403868 ; n° 405464 ; n° 405910 ; n° 407776 ; n° 409212 ; n° 423326 ; n° 429154.

62 G. Desgens-Pasanau, *RGPD. Mettre en œuvre le droit à l'oubli numérique et le droit au déréférencement*, Fiche pratique n° 2154, Lexis Nexis.

63 Article 20 du RGPD ; Article 55 de la Loi Informatique et Libertés.

64 *Ibid.*

65 Article 4 du RGPD.

Ce profilage pourrait ensuite être utilisé par un responsable de traitements afin de prendre des décisions automatisées à l'égard de la personne concernée, c'est-à-dire des décisions qui ne résultent que d'une application d'algorithmes et qui ne requièrent aucune intervention humaine. Ces décisions automatisées peuvent avoir des conséquences considérables sur la situation de la personne concernée (par exemple en cas de refus automatique d'un stage, de fixation automatique du montant de la prime d'assurance ou de refus automatique d'une prestation sociale).[66]

Afin d'éviter le risque de décisions arbitraires, émanant uniquement des machines, le RGPD reconnaît à la personne concernée un droit à une intervention humaine, c'est-à-dire à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé de ses données personnelles, si elle justifie que ce traitement produit des effets juridiques à son égard ou l'affecte de manière significative.[67] Même en présence d'une telle justification, la personne concernée pourra continuer à faire l'objet d'une décision entièrement automatisée si celle-ci a été autorisée par des dispositions légales, si elle est nécessaire à la réalisation du contrat conclu avec le responsable du traitement ou si la personne concernée y a donné son consentement explicite.[68]

Enfin, même en cas de décision automatisée, il sera toujours possible pour la personne concernée de demander à être informée de la logique utilisée pour cette prise de décision, de contester cette décision automatisée ou encore de demander le réexamen de la décision par un être humain.[69]

I. Droit à la limitation du traitement des données

Le droit à la limitation du traitement des données est l'accessoire des autres droits, tels que mentionnés ci-dessus. Il permet en effet à la personne concernée qui a demandé l'exercice de l'un de ses droits (opposition, rectification, etc.) de limiter l'utilisation de ses données pendant le délai d'examen de sa demande par le responsable du traitement. A l'inverse, cette limitation peut permettre à la personne concernée de conserver ses données alors que le responsable du traitement souhaiterait les effacer, par exemple dans le cadre d'une procédure judiciaire.

La limitation du traitement correspond en effet à un « gel » temporaire de l'utilisation des données : le responsable du traitement ne devra plus utiliser les données mais devra les conserver.[70] Durant cette période, les données concernées pourront cependant être utilisées dans quelques cas limités, à savoir : avec le

66 Site de la CNIL, Comprendre mes droits, Le droit à l'intervention humaine : https://www.cnil.fr/fr/vos-droits-lintervention-humaine-face-votre-profilage-ou-une-decision-automatisee
67 Article 22 du RGPD.
68 Article 22, paragraphe 2 du RGPD.
69 Article 22, paragraphe 3 du RGPD.
70 Article 18 du RGPD ; Article 53 de la Loi Informatique et Libertés.

consentement de la personne concernée, pour la constatation, l'exercice ou la défense de droits en justice, pour la protection des droits d'un tiers ou pour des motifs d'intérêt public.

***

La question de la protection des données à caractère personnel nous accompagne dans de nombreuses démarches au quotidien et est d'autant plus importante dans le contexte actuel.

La protection des données à caractère personnel est en effet essentielle dans le cadre de l'utilisation constante des réseaux sociaux. La perte de contrôle des données transmises sur les réseaux mène malheureusement trop souvent à des fuites, vols ou usurpations d'identité qui peuvent entrainer des conséquences dramatiques, allant du scandale au cyberharcèlement. Le RGPD constitue ainsi un bouclier en ce qu'il permet de demander efficacement la suppression des données mises en ligne et vient protéger plus particulièrement les mineurs[71], qui sont les premiers touchés par ces problématiques. C'est précisément cette volonté de protéger les mineurs qu'a conduit l'autorité italienne pour la protection des données personnelles à interdire, le 22 janvier dernier, au réseau social TikTok d'exploiter les données des utilisateurs dont l'âge n'a pas été établi avec une sécurité absolue, cette décision faisant suite au décès d'une fillette qui participait au « jeu du foulard » (consistant à bloquer ou à couper sa respiration jusqu'à l'évanouissement afin de connaître des sensations fortes) sur ce réseau social[72].

En outre, la pandémie de Covid-19 a mis à l'épreuve du RGPD les problématiques de collecte des données dans le cadre de la gestion de la crise sanitaire et de la recherche scientifique, ainsi que les questions liées à la protection du quotidien numérique des salariés, employeurs et enseignants amenés à travailler depuis chez eux.

Si des limitations à l'application du RGPD et de la Loi Informatique et Libertés sont permises afin d'assurer la protection de la santé publique dans un contexte d'urgence sanitaire, et sous réserve que ces mesures soient nécessaires et proportionnées[73], le respect des principes généraux de protection des données demeure incontournable.

La CNIL a ainsi été consultée sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la pandémie de Covid-19[74]. Plus particulièrement, la mise en place d'une application

---

71 Article 8, paragraphe 1 du RGPD.

72 *L'Italie bloque l'accès à TikTok pour quiconque n'est pas en mesure de justifier de l'âge minimal requis,* Le Monde, 22 janvier 2021.

73 Article 23 du RGPD ; Article 67 de la Loi Informatique et Libertés.

74 CNIL, Délibération n° 2020-087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à août 2020).

de « *tracking* » de la population pour surveiller les contaminations au Covid-19 a suscité de nombreuses problématiques en matière de protection des données à caractère personnel (position géographique, informations médicales, consentement des utilisateurs, etc.). La création de l'application « StopCovid » (devenue « TousAntiCovid ») a notamment fait l'objet de plusieurs délibérations de la CNIL[75], allant jusqu'à une mise en demeure du ministère de la Santé qui a dû se plier à ses recommandations en adaptant les mesures de protection proposées[76]. Plusieurs pays asiatiques ont eu des approches différentes, plus strictes en terme de traçage des personnes contaminées ou cas contacts : si la protection des données personnelles a pu sembler mise à mal, l'efficacité pour maîtriser la pandémie a été un argument. Céder toutefois devant la protection des libertés personnelles reste problématique, notamment car une fois le pas franchi, il est pour le moins difficile de revenir en arrière.

Dans un monde globalisé, l'approche reste encore divergente entre pays (et entre cultures) en matière de protection des données personnelles. Les nouvelles générations apparaissent parfois moins sensibilisées à ces aspects. Les données personnelles peuvent devenir un bien ayant de la valeur, une marchandise en quelque sorte dont il est dangereux qu'elle puisse être vendue ou achetée, voire monétisée, même avec le consentement de la personne en question. La protection des données personnelles apparaît donc toujours fondamentale, car l'absence de protection de celles-ci est de nature à induire des risques portant atteinte aux droits fondamentaux, dont les conséquences ne sont le plus souvent appréhendées qu'a posteriori, qu'une fois qu'il est souvent trop tard.

[75] CNIL, Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » ; Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid ».

[76] CNIL, Décision n°2020-015 du 3 septembre 2020 - Clôture de la décision n° 2020-015 du 15/07/2020 mettant en demeure le ministère des Solidarités et de la Santé.