QU'EST-CE QU'UN TRAITEMENT « ILLICITE » DE DONNEES ?

Fiche pratique publié le **23/11/2023**, vu **911 fois**, Auteur : Murielle Cahen

Toute personne, de sa naissance à sa mort, génère des données à caractère personnel ou « données personnelles », c'est-à-dire des informations qui concernent cette personne et permettent de l'identifier.

C'est l'élément de base de notre vie privée.

Avec l'entrée en application du Règlement Général sur la protection des Données le 25 mai 2018, la définition retenue est la suivante : « toute information se rapportant à une personne physique identifiée ou identifiable ».

Les données personnelles sont au centre des enjeux du RGPD. C'est pour assurer la protection des données à caractère personnel qu'une telle régulation a été mise en place, tant leur utilisation impacte profondément la vie privée de chacun.

Le « traitement » est 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. Art 4.2 RGPD

Le 7 mai 2019, un demandeur d'asile a déposé une demande de protection internationale auprès de l'Office fédéral allemand.

Sa demande a été rejetée en se basant sur les informations contenues dans le dossier électronique « MARIS ». Ce dossier, compilé par l'Office fédéral, contient des données personnelles relatives aux demandeurs, telles que leur identité, leurs antécédents et les motifs de leur demande de protection.

Suite à ce rejet, le demandeur a décidé de contester la décision devant le tribunal administratif de Wiesbaden, en Allemagne. Dans le cadre de cette procédure, le dossier électronique « MARIS » a été transmis au tribunal.

Cependant, la légalité de cette transmission a été remise en question par le tribunal, car l'Office fédéral n'a pas été en mesure de prouver qu'il respectait les obligations prévues par le RGPD, notamment en ce qui concerne :

(1) la tenue d'un registre des activités de traitement (art. 30 RGPD) et

(2) l'établissement d'un accord pour une responsabilité conjointe (art.26 RGPD).

Le tribunal s'interroge au premier chef sur les conséquences de ces potentielles violations : le traitement en devient-il illicite au sens de l'article 17 d) RGPD, entrainant dès lors l'effacement des

données ?

Avant de nous prononcer sur la l'illicéité d'un traitement de données personnelles (II), examinons la question de la licéité du traitement (I).

I. La licéité du traitement des données personnelles

A. La « base légale » d'un traitement de données personnelles ?

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement.

Quelles sont les bases légales prévues par le RGPD ?

Il est permis de traiter des données personnelles lorsque le traitement repose sur une des 6 bases légales mentionnées à l'article 6 du RGPD :

le consentement : la personne a consenti au traitement de ses données ;

le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;

l'obligation légale : le traitement est imposé par des textes légaux ;

la mission d'intérêt public : le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;

l'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées ;

la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.

Lorsqu'un même traitement de données poursuit plusieurs finalités, c'est-à-dire plusieurs objectifs, une base légale doit être définie pour chacune de ces finalités. En revanche, il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule.

Exemple : un fichier « clients et prospects » d'une entreprise peut poursuivre plusieurs finalités, qui doivent chacune reposer sur une base légale : le contrat pour la gestion des commandes, des livraisons ou du service après-vente ; l'obligation légale pour la tenue de la comptabilité ; le consentement pour les opérations de prospection commerciale par voie électronique ; etc.

B. Licéité et consentement

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

Le consentement n'est pas un concept nouveau, puisqu'il était déjà inscrit dans la loi Informatique et Libertés. Le RGPD complète néanmoins sa définition et précise cette notion sur certains

aspects, afin de permettre aux personnes concernées d'exercer un contrôle réel et effectif sur le traitement de leurs données.

Le consentement est une des 6 bases légales prévues par le RGPD autorisant la mise en œuvre de traitements de données à caractère personnel.

Le responsable de traitement doit être en mesure de démontrer la validité du recours à cette base légale.

Tout changement important des conditions de mise en œuvre du traitement (finalité, données, durées de conservation, etc.) est susceptible d'avoir une incidence sur la validité de la base légale retenue : la démarche d'évaluation de cette validité doit donc, dans ce cas, être réitérée.

4 critères cumulatifs doivent être remplis pour que le consentement soit valablement recueilli. Le consentement doit être :

Libre : le consentement ne doit pas être contraint ni influencé. La personne doit se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus.

Le caractère libre du consentement doit faire l'objet d'une attention particulière dans le cas de l'exécution d'un contrat, y compris pour la fourniture d'un service : refuser de consentir à un traitement qui n'est pas nécessaire à l'exécution du contrat ne doit pas avoir de conséquence sur son exécution ou sur la prestation du service.

Par exemple, un opérateur de téléphonie mobile recueille le consentement de ses clients pour l'utilisation de leurs coordonnées par des partenaires à des fins de prospection commerciale. Le consentement est considéré comme libre à condition que le refus des clients n'impacte pas la fourniture du service de téléphonie mobile.

Spécifique : un consentement doit correspondre à un seul traitement, pour une finalité déterminée.

Dès lors, pour un traitement qui comporte plusieurs finalités, les personnes doivent pouvoir consentir indépendamment pour l'une ou l'autre de ces finalités. Elles doivent pouvoir choisir librement les finalités pour lesquelles elles consentent au traitement de leurs données.

Par exemple, un organisateur d'évènements culturels souhaite recueillir le consentement des spectateurs pour deux types de prestations : la conservation de leurs coordonnées de paiement (carte bancaire) afin de faciliter leurs prochaines réservations ; la collecte de leur adresse électronique pour leur adresser des courriels concernant des prochaines représentations. Pour que le consentement soit valide, les spectateurs doivent pouvoir consentir librement et séparément pour chacun de ces deux traitements : la conservation des coordonnées bancaires et l'utilisation de leur adresse électronique.

Eclairé : pour qu'il soit valide, le consentement doit être accompagné d'un certain nombre d'informations communiquées à la personne avant qu'elle ne consente.

Au-delà des obligations liées à la transparence, le responsable du traitement devrait fournir les informations suivantes aux personnes concernées pour recueillir leur consentement éclairé :

l'identité du responsable du traitement ;

les finalités poursuivies ;

les catégories de données collectées ;

l'existence d'un droit de retrait du consentement ;

selon les cas : le fait que les données seront utilisées dans le cadre de décisions individuelles automatisées ou qu'elles feront l'objet d'un transfert vers un pays hors Union européenne.

Univoque : le consentement doit être donné par une déclaration ou tout autre acte positif clairs. Aucune ambiguïté quant à l'expression du consentement ne peut demeurer.

Les modalités suivantes de recueil du consentement ne peuvent pas être considérées comme univoques :

les cases pré-cochées ou pré-activées

les consentements « groupés » (lorsqu'un seul consentement est demandé pour plusieurs traitements distincts)

l'inaction (par exemple, l'absence de réponse à un courriel sollicitant le consentement)

II. L'illicéité du traitement

La notion de licéité apparait ici et là dans le règlement, sans que l'on perçoive toujours la portée exacte du terme. On sent l'importance de la notion, transversale, mais moins bien sa portée exacte.

Si l'on adopte une approche restrictive, la licéité du traitement se limite à respecter les conditions de l'article 6 intitulé … « licéité du traitement ». Dans cette approche restrictive, l'illicéité du traitement viserait les hypothèses de violation de l'article 6.

Si l'on adopte à l'inverse une approche large, dans laquelle est illicite tout ce qui ne respecte pas la règle de droit ou la norme de bon comportement, l'illicéité du traitement viserait la violation de n'importe quelle disposition du RGPD.

La question est importante, non seulement par rapport aux dommages et intérêts ou aux mesures correctrices que l'autorité peut prendre, mais aussi par rapport aux dispositions du RGPD qui visent spécifiquement les hypothèses d'illicéité. La première d'entre elles étant l'article 17 d) consacré au droit à l'oubli lorsque « les données à caractère personnel ont fait l'objet d'un traitement illicite. »

A. Le rejet de l'approche restrictive

On savait déjà que l'approche restrictive n'est pas celle retenue par la CJUE.

Dans l'arrêt Google Spain, la Cour a considéré que le caractère illicite peut résulter « non seulement du fait que ces données sont inexactes mais, en particulier, aussi du fait qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédante celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques ».

Il en découle :

d'une part, que la Cour élargit la notion d'illicéité au-delà de la violation du seul article 6 et y englobe l'article 5 ; et

d'autre part, que la Cour semble considérer qu'une illicéité fondée sur l'article 5 peut naitre de la violation de n'importe quel principe énoncé au 1er paragraphe de cette disposition : licéité, loyauté, transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité.

La Cour rejetait donc clairement une approche restrictive qui limiterait le concept d'illicéité aux seules violations de l'article 6.

B. Le rejet d'une approche (trop) extensive

En substance, la question préjudicielle posée par le tribunal administratif allemand porte sur l'élasticité du concept d'illicéité : une violation des articles 26 et 30, consacrés respectivement à l'établissement de règles entre responsables conjoints du traitement et à l'obligation de tenue d'un registre, constituerait-elle une illicéité au sens de l'article 17 d) (droit à l'oubli) ?

La logique du juge allemand n'est pas dénuée de logique. Puisque la CJUE a elle-même élargi la notion d'illicéité à tous les principes énoncés à l'article 5.1, pourquoi ne pas aller au bout de la logique et considérer que toute violation du RGPD est une violation du principe de responsabilité énoncé à l'article 5.2 et, dès lors, une illicéité au sens de l'article 17 d) ?

La CJUE s'y refuse.

Avant de se consacrer à l'illicéité visée à l'article 17 d), la Cour commence par s'intéresser à la notion de licéité.

Elle rappelle tout d'abord sa jurisprudence selon laquelle « tout traitement de données à caractère personnel doit être conforme aux principes relatifs au traitement des données énoncés à l'article 5, paragraphe 1, de ce règlement et satisfaire aux conditions de licéité du traitement énumérées à l'article 6 dudit règlement [voir, notamment, arrêts du 6 octobre 2020, La Quadrature du Net e.a., C?511/18, C?512/18 et C?520/18, EU:C:2020:791, point 208 ; du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C?439/19, EU:C:2021:504, point 96, ainsi que du 20 octobre 2022, Digi, C?77/21, EU:C:2022:805, points 49 et 56] ».

La Cour ajoute ensuite une précision importante pour la suite du raisonnement : les articles 7 à 11 du RGPD, qui figurent, à l'instar des articles 5 et 6 de celui-ci, dans le chapitre II relatif aux principes, ont pour objet de préciser la portée des obligations incombant au responsable du traitement en vertu de l'article 5, paragraphe 1, sous a), et de l'article 6, paragraphe 1.

Il s'ensuit, selon la Cour que « le traitement de données à caractère personnel, afin d'être licite, doit également respecter, ainsi qu'il ressort de la jurisprudence de la Cour, ces autres dispositions dudit chapitre qui concernent, en substance, le consentement, le traitement de catégories particulières de données personnelles à caractère sensible et le traitement de données

personnelles relatives aux condamnations pénales et aux infractions ».

Ayant posé les bases, la Cour s'attache enfin à l'hypothèse spécifique d'une violation des articles 26 et 30 : pareille violation, à la supposer établie, est-elle une illicéité au sens de l'article 17 d) qui autorise la personne concernée à exiger l'effacement de données, le lien entre les deux étant le concept de responsabilité (accountability) énoncé à l'article 5.2 ?

Elle répond par la négative, soulignant que :

Les articles 26 et 30 ne font pas partie du chapitre 2 consacré aux « principes » ;

La distinction opérée entre le chapitre 2 et le reste du règlement se reflète dans les dispositions relatives aux amendes administratives et aux mesures correctrices, qui varient selon le niveau de gravité des violations constatées ;

Cette interprétation est également corroborée par l'objectif du règlement qui est de garantir un niveau élevé de protection aux personnes concernées. Or relève la Cour, autant une violation des principes est susceptible de mettre en cause cet objectif, autant on ne peut affirmer de manière générale qu'une violation des articles 26 et 30 porte, en tant que telle, atteinte à cet objectif.

En conséquence, la Cour juge qu'une violation des articles 26 et 30 n'est pas une illicéité au sens des articles 17.1 d) (oubli) et 18.1 b) (limitation) dès lors qu'une telle méconnaissance n'implique pas, en tant que telle, une violation par le responsable du traitement du principe de « responsabilité » tel qu'énoncé à l'article 5, paragraphe 2, dudit règlement, lu conjointement avec l'article 5, paragraphe 1, sous a), et l'article 6, paragraphe 1, premier alinéa, de ce dernier.

Sources :

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=FR&mo

https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

https://www.cnil.fr/fr/les-bases-legales/consentement