« Les idées reçues sur la protection des données personnelles : les pièges à éviter » :

Intervention du 6 mai 2022 dans le cadre du 2e Printemps de la donnée UBFC, par Clémence Bourgeois, étudiante en Master Droit du numérique – UFR SJEPG, Université de Franche-Comté.

En collaboration avec Delphine Martin, MCF de droit privé, UFR SJEPG, Université de Franche-Comté.

Lorsque nous parlons de données à proprement parler, il convient de préciser d'emblée qu'il s'agit de données ***personnelles***. Cette précision est déterminante dans les propos qui suivront.

Une donnée dite personnelle est définie comme une information se rapportant à une personne physique identifiée ou identifiable. Ainsi, si les nom, prénom, ou la date de naissance d'un particulier sont concernés à l'évidence par cette définition, son champ d'application est plus vaste et inclut par exemple, une donnée de santé, une empreinte biométrique, une donnée de géolocalisation ou encore une adresse IP.

Exemple : collecte de données opérée dans le cadre d'un projet de recherche visant la réalisation d'un plan de déplacement d'entreprise. Les noms et prénoms des personnes ne sont pas collectés (ces informations ne sont pas nécessaires) mais des données sur les déplacements des personnes, leurs employeurs, leurs catégories socio-professionnelles et leur lieu de résidence permettent une identification des personnes physiques concernées. Ces informations sont donc des données à caractère personnel.

Aujourd'hui, notre société est toujours plus connectée et nos données sont donc la cible d'enjeux de plus en plus grands, notamment économiques et sécuritaires. Leur protection doit demeurer le centre des préoccupations de tous les acteurs de plus en plus dépendants des nouvelles technologies.

La protection des données personnelles est encadrée légalement en France depuis l'adoption de la loi Informatique et Libertés du 6 janvier 1978[1]. En raison de la massification du traitement des données une protection des données personnelles à l'échelle européenne s'est avérée nécessaire et a conduit à l'adoption du Règlement général sur la protection des données le 27 avril 2016 (RGPD), entré en vigueur le 25 mai 2018[2].

Pour appréhender les différentes problématiques liées à la protection des données personnelles notre propos aura pour objet une présentation du RGPD et des fausses idées relatives à ses conditions d'application.

Le RGPD a pour objet d'harmoniser les règles de protection des données personnelles en responsabilisant les responsables de traitement tout en accordant une place privilégiée au consentement des personnes dont les données sont collectées et traitées.

Pour ce faire, il convient tout d'abord d'apporter des précisions sur son champ d'application.

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

[2] Règlement (UE) 2016/679 sur la protection des données.

I. L'exclusion de la vie privée du champ d'application du RGPD

L'idée de protéger des données personnelles qui se rapportent donc spécifiquement à une personne physique conduit à se demander si la protection prévue par le RGPD s'étend jusqu'à la vie privée de toute personne.

Sur ce point il convient d'opérer une distinction entre les notions de données personnelles et de vie privée.

- La protection des données personnelles s'appuie sur les dispositions du RGPD dont l'objet est de protéger des informations permettant l'identification directe ou indirecte de la personne dont les données sont collectées. La donnée personnelle est donc une information.
- La notion vie privée protège tout ce qui a trait à l'intimité d'une personne : vie familiale, image de la personne, vie sexuelle, domicile, et, dans une certaine mesure vie professionnelle (possibilité pour les salariés d'identifier des fichiers sur leur poste de travail comme « personnels »). La protection de la vie privée a pour fondement l'article 9 du Code civil.

Illustration de la distinction entre les deux notions : par un arrêt de du 9 septembre 2020, la Cour de cassation a jugé que la divulgation, sans le consentement de l'intéressée, d'informations relatives aux circonstances précises dans lesquelles des infractions ont été commises est un fait distinct constitutif d'une atteinte à sa vie privée, qui peut être sanctionné sur le fondement de l'article 9 du Code civil[3]. En revanche, l'utilisation d'une donnée médicale sans le consentement de la personne concernée ou sans finalité légitime, ou encore l'utilisation d'une donnée de géolocalisation sera considérée comme une violation des données personnelles.

Dans le cadre d'une atteinte à la vie privée, l'auteur de l'atteinte engage sa responsabilité personnelle et peut être condamné au versement de dommages-intérêts en réparation du préjudice moral et/ou éventuellement matériel subi sur le fondement de l'article 1240 du Code civil. De plus, au titre de l'article 9 du Code civil *« les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée (…) ».*

Dans le cadre d'une atteinte à la protection des données personnelles, le responsable de traitement est sanctionné sur le fondement du RGPD. Dans ce cas, des sanctions peuvent être infligées par la CNIL ou par un juge aux responsables de traitement (amendes administratives ou judiciaires jusqu'à 20 000 000 euros ou 4% du CA de l'exercice précédent pour une entrepris, le montant le plus élevé étant retenu)[4]. La société SPARTOO a par exemple été condamnée par la CNIL le 5 août 2020 au paiement de la somme de 250 000€ pour avoir méconnu le RGPD, en particulier le principe de finalité dans la collecte des données car elle procédait à leur traitement systématique sans objectif suffisamment circonscrit et le principe de limitation de la conservation des données dont la durée maximale est, dans cette hypothèse, de cinq ans.

[3] Cass. Civ. 1ère, 9 septembre 2020, n°19-16415.
[4] Articles 83 et 84 RGPD.

II. Le périmètre d'application du RGPD : qui est concerné ?

Au niveau interne, la CNIL créée par la loi Informatique et Libertés assure le contrôle de l'application du RGPD.

Tout d'abord, le RGPD doit s'appliquer à toute organisation publique et privée, quelle que soit sa taille, qui traite de données personnelles pour son propre compte ou non. Contrairement à ce qui est parfois supposé, le RGPD ne concerne donc pas que les entreprises de plus de 250 salariés celles-ci étant concernées en revanche par l'obligation de tenir un registre de traitement des données.

Parmi les organismes publics concernés, sont concernés les Etats, les collectivités, les établissements publics etc.

Ensuite, le RGPD doit être appliqué par l'organisme établi sur le territoire de l'Union européenne. Mais, le RGPD doit également être appliqué si l'organisme cible directement des résidents européens. Tout organisme public ou privé est donc visé peu importe sa taille, le lieu de son implantation ou encore la nature de son activité. Ainsi, les GAFAM sont pleinement visés par l'application du RGPD puisque celle-ci peut donc être extraterritoriale. Ce point constitue d'ailleurs une force du texte européen.

Exemple : dans un arrêt du 28 avril 2022, la Cour de justice de l'Union européenne s'est prononcée sur la question de la recevabilité de l'action des consommateurs qui invoquaient la violation des données personnelles par la société META, société mère de Facebook, dont l'activité consiste à transférer des données personnelles de l'UE vers les E-U. L'association de consommateurs a été considérée comme légitime à agir la CJUE ayant jugé que le RGPD « *ne s'oppose pas à une réglementation nationale qui permet à une association de défense des intérêts des consommateurs d'agir en justice (…) dès lors que le traitement de données concerné est susceptible d'affecter les droits que des personnes physiques identifiées ou identifiables tirent de ce règlement »* et alors que le responsable du traitement des données est situé hors UE[5].

III. La finalité du traitement, condition préalable à tout traitement de données personnelles

Par application de l'article 6 le traitement de données personnelles doit être licite, fondé sur une base légitime et respecter un certain nombre de principes tels que le principe de finalité, de proportionnalité et de pertinence, le principe d'une durée de conservation limitée, le principe de sécurité et de confidentialité. Or, une collecte de données personnelles dans le cadre d'un projet de recherche pourrait être considérée comme d'emblée légitime et s'affranchir des contraintes qui pèsent sur le responsable de traitement en particulier s'agissant du consentement de la personne concernée, or, il n'en est rien.

Par application du principe de finalité, les données doivent être collectées pour des finalités déterminées, explicites et légitimes. De plus, un traitement ultérieur incompatible avec ces

[5] CJUE 68/2022, 28 avril 2022,

finalités est interdit sauf exceptions dans le cas d'un traitement ultérieur à des fins archivistiques, scientifiques, historiques ou statistiques par exemple.

Exemple : étude sociolinguistique de la variation du langage utilisé sur Twitter. Dans le cadre de cette étude la finalité est d'étudier le langage utilisé sur Twitter pour en identifier les spécificités, ce qu'il traduit ou encore son impact sur l'évolution du langage. Pour atteindre cet objectif il faudra identifier d'abord les données personnelles nécessaires qui peuvent être des données d'état civil, économiques, ou encore de géolocalisation. Une fois les données identifiées dans le respect de minimisation qui consiste à ne collecter que les données nécessaires il faudra ensuite recueillir le consentement des personnes concernées après une information claire et loyale (dans le cadre de la géolocalisation une analyse d'impact peut s'avérer nécessaire, les données de géolocalisation étant considérées comme des données sensibles). L'absence d'une finalité commerciale ne dispense donc pas le responsable de traitement de respecter le RGPD, de même qu'un objectif scientifique n'est pas considéré comme un motif d'ordre public permettant de le contourner.

Si la poursuite d'un objectif à caractère scientifique peut être considérée comme une finalité légitime, il ne permet pas d'écarter les principes applicables à la collecte de données personnelles, en particulier la nécessité du consentement des personnes concernées.

IV. Le consentement

La volonté du législateur européen a été de renforcer le principe du consentement des personnes dont les données sont collectées et de privilégier un principe de loyauté au moment de la collecte. Pour autant le consentement de la personne concernée n'est pas toujours exigé et il convient de distinguer deux situations différentes :

Premier cas de figure : le traitement repose sur le consentement de la personne. Le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de ses données[6].

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 doit être présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible donc en des termes clairs et simples.

De plus, 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 doit être informée de son droit de retrait.

Deuxième cas de figure : le traitement de données personnelles ne repose pas sur l'exigence d'un consentement de la part de la personne concernée[7].

Selon le RGPD, le consentement de la personne dont des données sont enregistrées dans un fichier n'est pas nécessaire lorsque ces données sont collectées :

- Pour l'exécution d'un contrat (Ex : contrat de vente, de location, de travail, etc.) ou de mesures précontractuelles (ex : un devis, des pourparlers, etc.).

[6] Articles 4 et 7.
[7] Article 6.

- Parce qu'un texte légal rend obligatoires certains fichiers (ex : le recensement de la population par l'INSEE, le registre unique du personnel, etc.).
- Pour l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique (ex : constitution de fichiers de police, de l'administration fiscale, etc.).
- Pour sauvegarder les intérêts vitaux d'une personne (ex : en cas d'épidémie, dans les situations de catastrophe naturelle ou d'origine humaine, etc.).
- Pour un intérêt légitime (ex : la prévention de la fraude, les transferts au sein d'un groupe, la sécurité des réseaux, etc.) sauf si les intérêts ou les libertés fondamentales de la personne concernée prévalent.

Néanmoins, en dehors de ces cas, le consentement de la personne concernée est obligatoire. C'est le consentement qui confère alors au fichier projeté son caractère licite, en application de l'article 7.

A titre de remarque et pour conclure sur la nécessité du consentement de la personne concernée, le fait de cocher une case justifiant qu'elle donne son consentement à la collecte de ses données peut être critiquable tandis qu'une case pré-cochée ne traduit pas la réalité du consentement.

Exemple : dans le cadre d'une collecte de données opérée par CARREFOUR auprès de clientes qui ont transmis des données personnelles telles que leur nom et leur âge. CARREFOUR avait pour objectif ensuite de transmettre ces données à des enseignes qui vendent des produits d'hygiène, notamment des protections hygiéniques mais sans que les clientes concernées n'aient été informées du traitement prévu pour ces informations. Outre le fait que leurs données personnelles sont détenues par CARREFOUR, ces personnes ont-elles bien pris conscience que l'ensemble de ces données pourra être réutilisé en matière dans un objectif commercial ? Ainsi, en l'absence de prise de conscience véritable et d'information totalement transparente des personnes concernées, il est permis de douter de la réalité de leur consentement.

V. Vis-à-vis des clients et des usagers, comment cela se passe-t-il MAIS surtout vis-à-vis des salariés et fonctionnaires

Tant dans le secteur privé que dans le secteur public, il convient de rappeler que la problématique de la protection des données personnelles concerne tant la clientèle que les salariés d'une entreprise, mais aussi des usagers dans un organisme public.

Cependant, la collecte de données peut être opérée pour des finalités différentes et plus ou moins lisibles.

Par exemple, un traitement de données peut être opéré dans le cadre de l'organisation interne d'une entreprise ou d'un organisme public. Dans ce contexte il convient de garder à l'esprit que les données sont susceptibles d'être conservées par les services RH de l'entreprise ou de l'organisme public pour être utilisées à des fins différentes :

- Gestion administrative personnelle, utilisation par exemple des coordonnées des personnes à prévenir

- Organisation du travail : exemple de la photo de l'employé qui sera utilisée pour réaliser un organigramme et avoir une vue d'ensemble sur les employés ou les fonctionnaires dans le cadre d'un organisme public
- Exercice de de l'action sociale, par exemple, pour obtenir des informations sur les ayants droits de l'employé.

Donc finalement dans cette idée de conservation et de collecte de données personnelles l'article 6 du RGPD reste applicable et le traitement devra avoir une base légale.

Néanmoins il y a deux nuances à apporter car dans le cadre du recrutement il s'agit de données qui seront conservées mais :

- L'accès à ces données conservées reste limité → il ne s'agira que des personnes du processus de recrutement c'est à dire les délégués du personnel mais également les autres institutions comme le comité d'entreprise les délégués syndicaux
- L'accès à ces données est contrôlé → ce contrôle de l'accès sera garanti par le fait que l'employeur doit assurer la sécurité des informations et garantir que seules les personnes habilitées en prennent connaissance.

Exemple 1 : lors de la crise liée au COVID-19, les employeurs ont été amenés à collecter certaines données personnelles de salariés relatives à leur santé, notamment dans les établissements soumis à la présentation du pass vaccinal. Les dispositions législatives relatives à la crise sanitaire donnent la possibilité aux salariés/agents des établissements soumis à l'obligation de présentation du pass vaccinal, de présenter à leur employeur un justificatif de statut vaccinal et d'autoriser celui-ci à conserver la preuve de cette vérification jusqu'à la fin de l'application du dispositif.

Exemple 2 : l'employeur peut accéder aux données personnelles des salariés pour contrôler leur activité sur le lieu de travail. Pour ce faire la consultation des e-mails reçus sur la boîte mail professionnelle du salarié fait partie des prérogatives de contrôle de l'employeur bien qu'il ait été rappelé à plusieurs reprises par la Cour de cassation que les e-mails spécifiquement identifiés comme personnels ne peuvent pas être lus par l'employeur.

Enfin, le statut de salarié n'exclut pas l'application des droits reconnus par le RGPD et en particulier du droit d'accès. L'exercice du droit d'accès permet à une personne de savoir si des données qui la concernent sont traitées puis d'en obtenir, si elle le souhaite, la communication dans un format compréhensible. Cette démarche permet notamment de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer. L'employeur est alors tenu de faire droit à la demande du salarié sauf cas particulier : courriels contenant des informations qui porteraient atteinte à la sécurité nationale ou à un secret industriel. Ces arguments ne pourront pas être invoqués par l'employeur sans justification étayée auprès du demandeur.

VI. Le rôle clé du responsable de traitement

D'après les dispositions de l'article 4 du RGPD, le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Au sein d'une entreprise, le rôle du responsable de traitement sera principalement joué par l'employeur.

Le RGPD impose deux obligations au responsable de traitement-: une obligation d'information et une obligation de sécurité et de confidentialité.

Au CNRS, pour les unités mixtes de recherche, le directeur d'unité est responsable de traitement (RT). Il doit donc s'assurer du respect de la règlementation sur la protection des données personnelles et désigner un délégué à la protection des données. Il s'appuie pour cela sur les responsables scientifiques des projets conduits au sein de l'unité. Le plus souvent, lorsque le directeur d'unité est employé par le CNRS, il désigne le Délégué à la protection des données du CNRS.

VII. Le DPO : une fonction émergente

Le DPO (Data Protection Officer) obligatoire pour le secteur public. L'article 37 du RGPD dispose que la désignation d'un délégué à la protection des données s'applique dès lors que le responsable du traitement opère un traitement régulier, systématique et à grande échelle des personnes concernées par le traitement. Au regard des lignes directrices du G29 (groupe des CNIL européennes) la notion de suivi régulier et systématique fait référence à un évènement continu ou se produisant à intervalles réguliers au cours d'une période donnée. La nomination du DPO ne dépend donc pas de la taille de la structure mais de la régularité et de l'envergure des traitements. Autant dire que toute entreprise opérant un suivi régulier de ses clients par la tenue d'un CRM par exemple sera potentiellement concernée par la désignation d'un DPO, quelle que soit sa dimension. Dans les grandes entreprises un seul DPO peut être désigné et donc pas nécessairement un DPO par service, c'est même préférable pour une meilleure coordination et un meilleur pilotage. Ce choix de nommer un ou plusieurs DPO relève de l'organisation interne.

Contrairement aux idées reçues, même concernant les entreprises, il n'y a pas de seuil minimal pouvant la désignation d'un DPO. De plus, il ne s'agit pas d'un salarié lambda même si dans les textes rien ne s'y oppose, mais d'un juriste averti qui entretient un lien de confiance particulier avec l'employeur (pour une entreprise).

Les ETI (entreprises de taille intermédiaire) et les grands groupes sont donc concernés, de même que les entreprises qui font du commerce électronique car une telle activité implique une collecte de données en quantité importante.

Le DPO conseille sur le respect de la règlementation, coopère avec l'autorité de contrôle, s'assure du respect de la règlementation sur la protection des personnes. La désignation est à effectuer auprès de la CNIL.

- Le DPO a un rôle d'information et de conseil auprès du responsable de traitement
- Il a un rôle de contrôle.
- Il a un rôle de formation et de sensibilisation du personnel.
- Il a un rôle d'intermédiaire auprès de la CNIL

Le DPO est au carrefour de plusieurs compétences. La CNIL le comparaît à un chef d'orchestre. D'une certaine manière, c'est ce qu'il est. Non seulement, doit il être capable d'analyse

juridique et de comprendre a minima les enjeux et problèmes techniques, mais il doit être capable de mobiliser l'ensemble des acteurs sur ce sujet.

Dans les grandes structures, grandes administrations par exemple, le DPO est aussi bien expert, que coordonnateur, pilote et doit être en mesure de sensibiliser les personnes clés dans l'organisme à ces questions. Il ne peut agir seul et doit pouvoir compter sur un responsable de traitement compétent. Raison pour laquelle chaque dossier que le dpo examine est aussi l'occasion pour lui de sensibiliser ses interlocuteurs.

Sur un traitement lambda, le DPO a bien souvent à faire au responsable, pilote du produit, le responsable de la sécurité des systèmes d'information compétent, le prestataire du pilote, et ses équipes informatiques. Son premier travail est de comprendre ce dont il est question. Le RGPD ne se limite en effet pas au seul examen de la donnée traitée. La donnée est l'entrée, ce qui notamment fait qu'il est fait application du RGPD. Mais au-delà, il y a les finalités du traitement, la manière dont la donnée est traitée, par qui, où, comment. Ces questions sont importantes. Elles déterminent aussi le niveau de sensibilité du traitement, et les mesures à prendre.

Sur ce point, l'une des fausses idées concernant la donnée est son niveau de sensibilité. Toutes les données personnelles ne requièrent pas le même niveau de traitement, ni n'imposent au responsable de traitement les mêmes exigences. La donnée compte beaucoup bien sûr, mais on n'a pas tout dit une fois que l'on a qualifié le niveau de sensibilité de la donnée.

Concernant le positionnement du DPO, sa tâche est généralement compliquée de ce qu'il est vu comme l'expert. Ce biais a une conséquence, le responsable de traitement a tendance à le suivre et s'en remettre à lui. Aussi le DPO doit-il toujours rappeler qu'il n'est pas responsable de traitement, juridiquement parlant, et présenter toutes les options possibles au responsable. Par ailleurs, si le dpo jouit d'un statut d'indépendance au sein de son organisme, il en est tout de même partie. Son travail est aussi d'aider le responsable de traitement à la réalisation de ses objectifs et non d'endosser le rôle de gendarme au sein de sa structure.

Enfin, le DPO est bien souvent juriste avant d'être technicien. Pourquoi ? Simplement parce que le RGPD est juridique avant d'être technique. Et savoir ce qu'il est possible de faire techniquement ou comment le faire pour être conforme à la législation est un point de passage obligé. Si le DPO est consulté trop tard dans l'avancement du projet, c'est courir le risque de s'engager dans une voie qui n'est pas conforme et donc s'exposer à des coûts supplémentaires, des retards de mise en production, etc.

Le DPO a donc un rôle central et sa désignation se fera le plus souvent sur la base de ses compétences juridiques plus que techniques.

VIII. Qu'en est-il de la création de données à travers la recherche

Dans la pratique, des questions peuvent être soulevées concernant le cycle de vie des données mais également la protection des données à caractère personnel dans le cadre de projets de recherche.

A ce titre, l'Union européenne conformément à un objectif de qualité de libre accès aux données de la recherche demande à ce qu'un plan de gestion des données soit réalisé pour

tout projet financé. Le plan de gestion des données est un document qui explicite la manière dont sont obtenues et traitées les données tout au long de leur cycle de vie, de leur collecte à leur archivage Il indique quel est le traitement des données de recherche avant pendant et après la fin du projet, les données qui seront collectées, traitées et générées ; si les données sont partagées, rendues accessibles, comment les données seront organisées, conservées, y compris à la fin du projet. Enfin, le plan de gestion des données garantit la qualité de la recherche et contribue à rendre les données facilement accessibles, identifiables et reproductibles. C'est donc un document qui a toute son importance dans le cadre de la recherche.