« Le traitement des données sensibles dans le cadre de la recherche »

Intervention du 13 mai 2022 dans le cadre du 2e Printemps de la donnée UBFC par Manon Anselme, Anaelle Ranguis, Louis Zimberlin, étudiants en Master Droit du numérique, UFR SJEPG – Université de Franche-Comté.

En collaboration avec Delphine Martin, MCF de Droit privé, Université de Franche-Comté

INTRODUCTION : De quoi parle-t-on ?

En droit français, selon l'article 2 de la loi informatique et libertés, une donnée à caractère personnel est une *« information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »*[1]. Ces données doivent être collectées et traitées conformément au Règlement européen sur la protection des données adopté le 27 avril 2016 et entrée en vigueur le 25 mai 2018 (RGPD)[2].

Une personne physique peut être identifiée par ses données soit :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, nombre d'enfants, couverture sociale.

Le RGPD définit le traitement comme : *« 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 »*[3]*.* Plus simplement un traitement de données c'est un ensemble d'opérations réalisées sur des données personnelles.

Parmi les données personnelles, le RGPD distingue les données sensibles soumises à des règles de traitement particulières[4]. Les données sensibles sont définies comme des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses (pratique d'un culte par exemple) ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques (empreinte digitale, gabarit facial, vocal, empreintes palmaires…) aux fins d'identifier une personne physique de manière unique, des données concernant la santé (comportement de prévention, renoncement à des soins, traitements médicaux) ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite loi LIL.
[2] Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données
[3] Article 4 RGPD.
[4] Article 9 RGPD.

Le format des données collectées est sans incidence sur la qualification de données sensibles : il peut s'agir d'images (photographies, tableaux, scanner médicaux), de vidéos (enregistrements de vidéosurveillance), d'une partie du corps (empreinte digitale, rétinienne ou veineuse).
Cette définition permet de mettre en exergue la différence entre une donnée sensible et une information confidentielle. Par exemple, le secret industriel ou le secret de l'instruction ne sont pas considérés comme des données sensibles au sens du RGPD. De même que les données hautement confidentielles ne sont pas des données sensibles bien qu'elles fassent l'objet de règles similaires en termes d'évaluation des risques pour les droits et libertés fondamentales (les données bancaires sont par exemple qualifiées de hautement confidentielles).

Les données sensibles portent en elles un risque d'atteinte aux droits fondamentaux tels que le respect de la vie privée et nécessitent donc la plus grande vigilance lorsqu'elles sont collectées puis traitées. A noter que cette vigilance doit rester constante dans la mesure où, la qualification juridique de la donnée collectée est susceptible d'évoluer. Ainsi une donnée personnelle non sensible peut le devenir lorsqu'elle est croisée avec d'autres données.

Exemples :

-Des recherches portant sur la géolocalisation des véhicules pourraient révéler des convictions politiques réelles ou supposées, des convictions religieuses et/ou des données relatives à la santé par l'étude des habitudes de déplacement et du stationnement sur le parking de lieux particuliers (locaux d'un parti politique, fréquentation de lieux de culte, etc.).

-Le nom et le prénom d'une personne ne sont pas des données sensibles, mais lorsqu'ils sont associés aux opinions politiques de la personne elles deviennent des données sensibles au sens de l'article 9.

Le principe général est l'interdiction de collecte et de traitement des données sensibles en raison du risque d'atteinte que ces deux opérations représentent pour les droits fondamentaux des personnes concernées[5].

Ainsi par exemple :

-un traitement de données sensibles dans le cadre de la recherche peut porter atteinte aux libertés fondamentales s'il a pour objet le traitement de données relatives à l'origine ethnique ou la prétendue « race » des personnes concernées dans le cadre d'une étude sur la mesure de la diversité des origines. En revanche, la langue parlée ou l'origine géographique au sein d'un territoire nationale sont des données non sensibles.

- un projet de recherche visant à étudier des pages de personnalités publiques sur les réseaux sociaux qui contiennent des propos rattachés à certaines opinions politiques peut contenir des données sensibles.

[5] Article 9.

- un projet de recherche visant à développer un algorithme de reconnaissance faciale (données biométriques dans ce cas).

Il existe cependant des exceptions à cette interdiction de principe de collecte et de traitement des données sensibles :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ; tel est le cas par exemple des opinions publiques exprimées par un candidat à une élection lors d'une émission télévisée
- si elles sont nécessaires à la sauvegarde de la vie humaine (données médicales)
- si leur utilisation est justifiée par l'intérêt public (recherche médicale).

Parmi les hypothèses de données sensibles nous prendrons l'exemple des données médicales les plus facilement associées aux données sensibles, mais sans prétention à l'exhaustivité, ces données faisant l'objet de règles particulières qui ne seront pas toutes abordées. Dans le cadre de la recherche médicale, les données à caractère personnel sont l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Ces données peuvent être objectives, comme le groupe sanguin, le numéro de sécurité sociale (NIR), ou subjectives, comme des avis ou des appréciations. A noter que s'agissant du NIR, le principe est l'interdiction de traitement sauf dans des cas précisément mentionnés par décret-cadre actualisé chaque année : couverture sociale par exemple, service de paie, mutuelle…

Les données médicales ne peuvent être collectées que dans certains cas, encadrés par la loi, par exemple pour le dossier médical informatisé d'un patient hospitalisé. Dans ce contexte, il est, notamment, nécessaire de remettre un document spécifique au patient, de prévoir une information par affichage dans la structure de soin, le cryptage des pièces sensibles qui sont envoyées par mail, de subordonner la lecture des fichiers transmis à un mot de passe….

A titre illustratif, pour le cas du Sida, les données ont été considérées comme extrêmement sensibles en médecine, puisque l'identité du patient était reliée aux données traitées, le fichier étant nominatif.

Il convient de souligner que les règles applicables au traitement des données sensibles s'appliquent à la recherche tant publique que privée.

Traiter une donnée, pourquoi faire ?

Les données sont collectées dans un but déterminé et légitime par le chercheur. La finalité du traitement est ce qu'on appelle l'objectif principal de l'utilisation de données personnelles. Elles ne doivent pas être traitées ultérieurement de façon incompatible avec cet objectif initial sauf cas particuliers (traitement ultérieur à des fins statistiques, de recherche ou archivistiques).

Ce principe de finalité limite la manière dont le chercheur peut utiliser ou réutiliser ces données dans le futur. Il est essentiel dans la définition des données qui seront collectées pour en minimiser la quantité, dans la détermination de la procédure applicable à la collecte et au traitement et de la durée de conservation, celle-ci étant particulière dans le domaine médical.

Exemples de finalité dans le cadre de la recherche scientifique :

Les traitements à finalité de recherche scientifique ne rentreront pas dans le champ d'application de la réglementation en matière de protection des données personnelles dans les hypothèses suivantes :

- si le traitement mis en œuvre ne contient aucune donnée personnelle (exemple : l'étude du métabolisme chez les oiseaux migrateurs ou encore des recherches menées sur les satellites de la planète Jupiter) ;
- si le traitement mis en œuvre concerne exclusivement des données anonymisées, car elles ont perdu leur « caractère personnel » et en principe sortent du champ d'application du RGPD ;
- si le responsable de traitement n'est pas établi sur le territoire de l'UE et si les recherches menées concernent des personnes qui ne se trouvent pas sur le même territoire de l'UE.

Le RGPD souligne explicitement l'importance et l'intérêt pour la société des traitements effectués à des fins de recherche scientifique ou historique. Comme il sera évoqué un peu plus tard, la recherche médicale fait exception au principe d'objectif limité dans la mesure où, beaucoup de travaux sont archivés et sont d'intérêt public.
Tout l'enjeu consiste donc à cerner la portée des objectifs et à établir ce qu'ils permettent exactement aux chercheurs de faire, afin de sécuriser le traitement des données.

Traiter une donnée sensible, comment ça marche ?

Qui peut traiter une donnée ?

Dès qu'un chercheur collecte des données personnelles, le responsable du traitement doit faire en sorte que les droits des personnes concernées soient respectés.

Le responsable du traitement est, selon le Règlement général sur la protection des données, *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».* Donc le responsable de traitement est celui qui définit les objectifs ou finalités et les moyens du traitement[6]. Il ne s'agit pas nécessairement de la personne qui collecte ou accède aux données, (la personne qui collecte les données peut être un chercheur, un centre de recherche, un ingénieur de recherche, ou encore un étudiant).

Existe-t-il des conditions pour pouvoir traiter une donnée ?

[6] Articles 24 et s.

OUI. Le RGPD prévoit une série de droits que les personnes peuvent faire valoir auprès des responsables de traitements. S'agissant des traitements poursuivant des finalités de recherche, les droits suivants sont applicables :

1) droit à la transparence des informations, de communications (art. 12 du RGPD) : il faut que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples par exemples illustré à l'aide d'éléments visuels

2) droit à l'information (art. 13 et 14 du RGPD) : obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

3) droit d'accès (art. 15 du RGPD) : les personnes doivent être informées qu'elles peuvent demander à un organisme s'il détient des données sur elles (site web, magasin, banque...) et demander à ce que les leur communique pour en vérifier le contenu.

4) droit de rectification (art. 16 du RGPD) : Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

5) droit à l'effacement aussi appelé droit à l'oubli (art. 17 du RGPD) : permet à toute personne d'obtenir d'un responsable de traitement la suppression des données à caractère personnel qui la concerne

6) droit à la limitation du traitement (art. 18 du RGPD) : une personne a le droit de demander à un organisme de geler temporairement l'utilisation de certaines des données

7) droit à la portabilité des données (art. 20 du RGPD) : droit pour une personne de récupérer une partie de ses données dans un format lisible. Libre à la personne stocker ailleurs ces données portables ou les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins.

8) droit d'opposition (art. 21 du RGPD) : droit pour une personne de refuser l'utilisation de ses données

Pour faciliter la recherche scientifique, les données à caractère personnel peuvent être traitées à des fins de recherche scientifique sous réserve de conditions et de garanties appropriées prévues dans le droit de l'Union ou le droit des États membres.

Comme pour les traitements réalisés à des fins archivistiques ou statistiques, un équilibre doit être opéré entre la finalité scientifique et la protection des droits et libertés des personnes concernées

Toutefois, l'interdiction de traitement des données sensibles est un principe qui fait l'objet d'exceptions. Elles sont prévues par le paragraphe 2 de l'article 9 du RGPD. Il s'agit notamment des cas suivants :

- **Si la personne concernée a donné son consentement exprès** : Par exemple ça pourra être → « J'accepte que mon image et mes propos soient diffusés dans le cadre de colloques scientifiques, séminaires ou dans toute forme de valorisation du projet XXX »

- **si les informations sont manifestement rendues publiques par la personne concernée** : concerne notamment les contenus se rapportant à la personne qui les a délibérément divulgués. Par exemple, on pourrait estimer que cela ne concerne pas les commentaires publiés par un tiers sur un réseau social.

Exemple : des opinions politiques tenues par un candidat à une élection lors d'une émission télévisée constituent des données manifestement rendues publiques par la personne concernée.

→ A savoir que la présence d'un seul élément peut ne pas toujours suffire à établir que les données ont été « manifestement » rendues publiques par la personne concernée. En pratique, une combinaison de plusieurs éléments est prise en compte pour considérer que la personne concernée a manifesté clairement l'intention de rendre ses données publiques.

- **La recherche est nécessaire pour des motifs d'intérêt public importants**

Cette exception concerne principalement les recherches mises en œuvre par les autorités publiques. Elle peut néanmoins autoriser la mise en œuvre de traitements par des organismes privés s'ils poursuivent une mission d'intérêt public ou sont dotés de prérogatives de puissance publique.

Le responsable de traitement devra démontrer :

-la condition de « nécessité » pour la mission d'intérêt public ;
-la présence de motifs d'intérêt public importants ;
-qu'il s'agit d'un intérêt public au sens du droit national ou du droit européen.

Pour mobiliser cette exception, la loi Informatique et Libertés exige un texte, par exemple un décret en Conseil d'État après avis de la CNIL.

- **L'utilisation des données est nécessaire à la recherche publique**

Certaines utilisations de données peuvent être nécessaires à la recherche publique, sous réserve que des motifs d'intérêt public importants les rendent nécessaires (nécessite un avis de la CNIL). Pour être considérée comme une recherche publique, celle-ci doit respecter certains critères précisés dans le code de la recherche comme par exemple le financement par des fonds publics.

La recherche privée, qui ne rentre pas dans les critères définis dans le code de la recherche, ne peut donc pas mobiliser cette exception prévue par la loi Informatique et Libertés. Par conséquent, pour ces traitements, des données sensibles ne pourront être collectées seulement dans le cadre des exceptions mentionnées plus haut. En effet, l'article 9.2 du RGPD relatif à la recherche tant publique que privée n'est pas encore adapté dans la loi française : il n'est donc pas possible de mobiliser cet article.

Pour ce qui est de l'application du principe de finalité il convient, par exemple, d'indiquer → que « Le traitement a pour objet : préciser l'objectif principal de la recherche et le cas échéant, détailler les sous-finalités ».

Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique.
Les chercheurs disposent donc d'une certaine marge de manœuvre pour formuler les finalités des traitements de données collectées d'une manière moins précise que ce qui est exigé en principe par le RGPD.

Enfin, la donnée sensible en recherche doit être traitée dans une durée « n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ». Le RGPD précise même que la durée de conservation devrait être limitée au « strict minimum »[7]. On en déduit que les données peuvent être conservées au-delà de la durée nécessaire pour atteindre la finalité de recherche (par exemple, au-delà de la durée d'un projet de recherche déterminé) du moment qu'elles sont ensuite conservées uniquement pour être utilisées à des fins de recherche.

Il en résulte que les projets de recherche doivent prévoir une durée déterminée de conservation des données qu'ils collectent, en lien avec la finalité retenue. Mais une fois cette durée écoulée, les données peuvent être confiées à un service d'archives disposant de la compétence légale pour procéder à un passage des documents en archives définitives, après une opération de tri. Ce sont ensuite ces archives définitives, constituées à partir des matériaux de recherche, qui permettent une conservation au-delà de la durée initiale. Cette hypothèse correspond à celle d'un traitement ultérieur de données, par exception autorisé, comme le traitement ultérieur à des fins statistiques ou historiques.

Exemple de mention d'information :

Cas d'une enquête par questionnaire

→ Nous attendons de vous que vous participiez à une enquête par questionnaire durant laquelle nous vous poserons des questions sur « *rappeler les finalités du projet* ». Le questionnaire devra « *préciser la durée de passation* ». *S'il s'agit d'une enquête longitudinale, préciser la durée de participation et les périodes de collecte.*

[7] Articles 5 et s.

« Quels principes respecter pour traiter des données sensibles ? » :

Pour se conformer aux règles du RGPD, le responsable du traitement des données personnelles ou son représentant doit préalablement et jusqu'à la fin du traitement, respecter six principes généraux auxquels s'ajoutent des règles particulières lorsqu'il s'agit de données sensibles[8].

Ces principes d'ordre général s'imposent notamment dans le cadre des programmes pédagogiques intégrant le recueil et le traitement de données personnelles.

1- Licéité, loyauté et transparence du traitement. Les données personnelles doivent être « traitées de manière licite, loyale et transparente au regard de la personne concernée ». Cela signifie que les données ne doivent pas avoir été collectées ni traitées, sans que la personne concernée en ait connaissance. Ce principe nécessite de fournir aux personnes concernées plusieurs informations, sur la finalité du traitement, mais aussi sur les droits qu'ils peuvent exercer après la phase de collecte des données (droit d'accès, droit de rectification, droit à la portabilité).

2- La limitation des finalités. Les données personnelles doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ». Le RGPD prévoit toutefois que des données personnelles peuvent être traitées « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques », même si elles n'avaient pas été initialement collectées à cette fin ; un tel traitement ultérieur n'est pas incompatible avec la finalité initiale de la collecte. C'est ce qui permet aux chercheurs de consulter des fonds existants contenant des données personnelles, sans enfreindre ce principe de limitation des finalités, et sous réserve de respecter certaines règles, comme, par exemple, les délais de consultation des archives publiques.

Néanmoins pour ce qui est de la recherche scientifique, le texte instaure une forme de présomption aux termes de laquelle le changement de finalité sera systématiquement réputé compatible avec la finalité initiale du moment que le traitement ultérieur est effectué à des fins de recherche scientifique

3- La minimisation des données. Seules doivent être collectées les données strictement nécessaires à la finalité du traitement.

4- L'exactitude des données. Les données personnelles collectées doivent être « exactes et, si nécessaire, tenues à jour » ; elles doivent sinon être rectifiées ou effacées.

[8] Article 5.

5- La limitation de la conservation. Les données personnelles ne doivent pas être conservées au-delà de la durée nécessaire à la finalité du traitement. Le principe de limitation de la conservation implique que les personnes collectant soient en mesure de définir une durée de conservation proportionnée à la finalité poursuivie. Ce délai doit être présenté préalablement au recueil des informations et des données personnelles sollicitées. Dans le cadre de travaux ponctuels, cette durée ne pourrait excéder la durée de présentation des travaux dans le cadre académique, à savoir une année au maximum. En outre, les représentants du responsable du traitement des données personnelles devront procéder à la suppression ou à l'archivage, le cas échéant dans les conditions prévues par le Code du patrimoine, des données en question à l'issue de la recherche, sauf justification particulière. A cet égard, le cycle de conservation des données peut être divisé en trois phases

- la base active : elle correspond à la durée d'utilisation courante des données (en l'espèce, à la durée nécessaire à la réalisation des recherches)

- l'archivage intermédiaire : les données peuvent être conservées pour une durée plus longue en archivage intermédiaire, qui est distinct de la base active, et seulement pour un accès restreint (par exemple, s'il existe une obligation légale de conserver les données, si les données présentent un intérêt administratif ou, sous réserve de garanties appropriées, si les données sont traitées à des fins de recherche scientifique)

- l'archivage définitif : dans les conditions du Livre 2 du Code du patrimoine, l'intérêt public peut parfois justifier que certaines données ne fassent l'objet d'aucune destruction.

6- L'intégrité et la confidentialité des données. Le responsable du traitement doit prendre « les mesures techniques ou organisationnelles appropriées » pour garantir la sécurité des données personnelles, y compris la protection contre le traitement non autorisé ou la perte des données. Cette obligation de prendre les mesures techniques ou organisationnelles appropriées est la pierre angulaire du RGPD. Le responsable du traitement doit, pour garantir l'intégrité et la confidentialité des données personnelles traitées, vérifier que l'organisation (humaine) et les moyens techniques (souvent informatiques) mis en œuvre sont suffisamment sûrs pour protéger les droits et libertés des personnes concernées. Dans certains cas (les données sont sensibles, le traitement de données est mené à grande échelle…), le RGPD exige que soit également menée une étude d'impact approfondie Privacy Impact Assesment (PIA).

Lorsqu'il s'agit de données sensibles, les principes sont posés par l'article 35 du RGPD qui s'articulent avec les critères posés par le G29 devenu le CEPD. L'idée générale est qu'il faut dans cette hypothèse évaluer le risque d'atteinte aux libertés fondamentales et éventuellement demander ensuite l'avis de la CNIL après avoir réalisé une analyse d'impact. Le but de l'analyse d'impact est d'évaluer le risque lié à la collecte et le traitement de données pour en déduire les mesures de sécurité adaptées. Par cette analyse d'impact on souhaite passer d'un risque élevé à un risque résiduel

Qu'est-ce qui justifie cette analyse d'impact ? Il y a 3 raisons principales :

- La nature des données
- La quantité des données
- Les traitements automatisés de données

Plus précisément l'AIPD est obligatoire dans trois hypothèses selon l'article 35 :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire (perte d'un droit par exemple) ;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. La notion de traitement à grande échelle est définie par le Considérant 91 du même règlement, il s'agit d'un traitement d'un volume considérable de données au niveau régional, national, supranational.

c) la surveillance systématique à grande échelle d'une zone accessible au public (utilisation de la vidéosurveillance).

Les hypothèses de l'article 35 doivent être articulées avec les 14 préconisations de la CNIL (par exemple en cas de traitement de données génétiques, les données biométriques, données de santé, données de géolocalisation) et les 9 critères posés par le G29 (comme le croisement de données, le traitement de données de personnes vulnérables).

Selon la CNIL une AIPD doit obligatoirement être menée quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernée*s* ».

-Soit le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données :

Exemples :

Exemple 1 :

-Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médicosociaux pour la prise en charge des personnes. Il s'agit dans ce cas de données sensibles et qui concernent des personnes vulnérables donc de la réunion de 2 critères dégagés par le G29. Une AIPD est nécessaire pour les traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) :

Exemple 2 : Traitements ayant pour finalité la surveillance constante de l'activité des employés d'une entreprise. Les données sont sensibles et il s'agit d'une surveillance systématique donc de traitement automatique, réunion de 2 critères posés par le G 29. L'AIPD sera nécessaire pour mettre en place :

– un dispositif de cyber surveillance tels que ceux procédant à une analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information (dispositifs dits de Data Loss Prevention) ;

- une vidéosurveillance portant sur les employés manipulant de l'argent ;

- une vidéosurveillance d'un entrepôt stockant des biens de valeur au sein duquel travaillent des manutentionnaires

-Soit le traitement remplit au moins **deux des neuf critères** issus des lignes directrices du G29 :

- évaluation/*scoring* (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ou données à caractère hautement personnel ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, *etc*.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Exemple : une entreprise met en place un traitement publicitaire visant à collecter les données de géolocalisation de plusieurs millions d'individus pour créer des profils publicitaires et leur afficher de la publicité ciblée en fonction de leurs déplacements ; ce traitement remplit le critère de la collecte à grande échelle et celui de la collecte de données sensibles (données de localisation), donc la réalisation d'une AIPD sera nécessaire.

Concrètement une analyse d'impact doit comporter au minimum :

- une **description** systématique des **opérations de traitement** envisagées et les **finalités** du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une **évaluation de la nécessité** et de la **proportionnalité** des opérations de traitement au regard des finalités ;
- une **évaluation des risques** sur les droits et libertés des personnes concernées ; et
- les **mesures envisagées** pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

La procédure de l'AIPD est une procédure assez complexe et qui peut prendre du temps mais il est possible de s'exonérer de ces contraintes en anonymisant les données.

L'AIPD sera ensuite transmise à la CNIL dans les cas suivants :

- l'analyse présente des risques résiduels élevés (article 36 du RGPD) ;
- dans le cas des traitements relevant de la directive « Police-Justice » si l'analyse présente des **risques résiduels élevés** ou si le traitement, en particulier en raison de

l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des **risques initiaux élevés** (article 90 de la loi Informatique et Libertés).

Ou :

dans le cas de l'instruction d'un dossier de formalité CNIL (demande d'avis, autorisation-recherche, autorisation santé, engagements de conformité à certains actes réglementaires uniques (RU-065)).

Dans la pratique, dès lors que les données collectées sont sensibles l'AIPD est privilégiée indépendamment du cumul avec un autre critère parmi les 9 visés par le G29. Elle permet d'appréhender l'intensité du risque d'atteinte aux droits des personnes concernées et de définir une politique de traitement adaptée pour le minimiser au maximum. Toutefois, ce risque ne peut être complètement éradiqué en raison, notamment, de la possibilité de croisement des données qui peut échapper au responsable de traitement.