LE DROIT DES DONNÉES PERSONNELLES

EN CARTES MENTALES

Rose-Marie Borges

ellipses

Introduction

Le développement d'Internet, des réseaux sociaux, des objets connectés et, plus généralement des technologies numériques, a provoqué une explosion de la quantité de données personnelles collectées par les acteurs privés et publics du marché. Les données ne sont pas seulement quantitativement plus importantes, elles sont également plus diversifiées et couvrent des champs très variés allant des habitudes d'achat d'un consommateur à son profil génétique. De plus en plus, les individus rendent eux-mêmes publiques des informations les concernant, sans toujours en être conscients d'ailleurs. Cette quantité colossale de données constitue ce qu'il convient d'appeler le Big Data. Le terme Big Data désigne de vastes ensembles de données collectées par différentes structures, pouvant être analysées afin d'en dégager des informations exploitables ou utilisées pour des usages divers. Traditionnellement, le Big Data se caractérisait par trois facteurs, dits «les 3 V»: le volume, la vitesse et la variété. Ces dernières années, deux caractéristiques supplémentaires sont apparues, la valeur et la véracité : les données possèdent une valeur intrinsèque qui doit être optimisée et elles doivent être les plus fiables possible.

En 2024, la quantité totale de données créées dans le monde a atteint 149 zettaoctets, c'est-à-dire 149 mille milliards de gigaoctets. Le volume colossal de données numériques produites, combiné aux capacités accrues de stockage et à des outils d'analyse en temps réel de plus en plus performants, offre des possibilités inégalées d'exploitation des informations et représente un marché en pleine croissance. En 2024, le marché mondial de la Data était estimé à 25 milliards de dollars et devrait atteindre 62 milliards en 2029. En France, ce marché a dépassé les 3 milliards € en 2024 et devrait continuer à croître. L'exploitation des données ne peut que s'intensifier, celles-ci constituant le carburant de l'intelligence artificielle, elle-même en pleine expansion.

Les données personnelles tendent à devenir des marchandises comme les autres, alors même qu'elles touchent à la personne même et à son intimité.

L'utilisation croissante des outils numériques par les individus s'accompagne, dans le même temps, d'une préoccupation grandissante quant à la protection de leurs données personnelles. Celles-ci constituent en effet l'un des aspects de la vie

privée des personnes et méritent, à ce titre, d'être protégées. Le droit au respect de la vie privée est consacré à l'article 9 du code civil et a été intégré au bloc de constitutionnalité par le Conseil constitutionnel, qui le rattache à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, parmi les « *droits naturels et imprescriptibles de l'Homme* ». Le droit à la vie privée est également reconnu par le droit international et communautaire : à l'article 12 de la Déclaration universelle des droits de l'homme de 1948, à l'article 8 de la Convention européenne des droits de l'homme de 1950 et, plus récemment, à l'article 7 de la Charte des droits fondamentaux de l'Union européenne en 2000.

L'encadrement juridique du traitement des données personnelles s'est opéré progressivement. En France, dans les années 1970, les utilisations de l'informatique à grande échelle ont fait prendre conscience des effets potentiellement néfastes du traitement des données personnelles. En 1974, le projet SAFARI (*Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*) envisage de créer un identifiant unique visant à interconnecter les fichiers des différentes administrations et suscite la crainte que le système de fichage ne serve principalement à la surveillance des citoyens. Face au tollé soulevé par ce projet, la France se dote de la loi Informatique et Libertés (LIL), entrée en vigueur le 6 janvier 1978. L'article 1er de la LIL réaffirme le principe selon lequel « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle 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* ».

La LIL va créer la Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante chargée de veiller au respect de la loi informatique et libertés.

Au niveau européen, la directive 95/46/CE du 24 octobre 1995 (*Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281, 23 novembre 1995, p. 31)* établit un cadre juridique commun pour les États membres en matière de protection des données personnelles. Malgré la directive, les pratiques des États membres demeuraient très variables, assurant un degré de protection inégal à leurs ressortissants. Le défaut d'harmonisation des législations nationales et l'essor d'Internet ont conduit les autorités européennes à adopter le « paquet européen de protection des données personnelles », constitué du Règlement général sur la protection des données (RGPD) en 2016 (*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, JOUE n° L 119, 4 mai 2016, p. 1*) et de la Directive « Police-Justice » concernant les données pénales *(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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JOUE n° L 119, 4 mai 2016, p. 89).

Parallèlement au « paquet protection des données personnelles », l'UE a adopté des règlements sur les marchés et les services numériques, qui contiennent également des dispositions relatives aux données personnelles des citoyens européens et viennent compléter le RGPD dans ces domaines.

Le règlement sur les marchés numériques dit DMA (*Digital Markets Act*) a été adopté le 14 septembre 2022 et est entré en vigueur le 6 mars 2024 (*Règlement UE 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives UE 2019/1937 et UE 2020/1828, JOUE n° L 265, 12 octobre 2022, p. 1*). Il vise à lutter contre les pratiques anticoncurrentielles des géants d'internet que sont les GAFAM, BATX et autres NATU, et à corriger les déséquilibres de leur domination sur le marché numérique européen. Selon la Commission européenne, plus de 10 000 plateformes en ligne opèrent en Europe, mais seules les plus grandes captent l'essentiel de la valeur du marché numérique européen, alors qu'elles ne représentent que 10 % des plateformes. Le DMA s'applique uniquement aux entreprises qui sont des « contrôleurs d'accès » ou « *gatekeepers* » à l'entrée d'internet. Il s'agit d'acteurs qui ont une forte incidence sur le marché intérieur, sont un point d'accès important des entreprises utilisatrices pour toucher leur clientèle et occupent ou occuperont dans un avenir proche une position solide et durable. Peu importe qu'ils soient établis en Europe ou ailleurs dans le monde. La Commission européenne a publié une liste de « contrôleurs d'accès » soumis au DMA, certains pour plusieurs de leurs services :

- Alphabet : Google Chrome, Google Play, Google Maps, Google Shopping, Google Search, YouTube, Android et Advertising service.
- Amazon : Marketplace et Advertising.
- Apple : AppStore, iOS, Safari et iPadOS.
- Booking.
- ByteDance : TikTok.
- Meta : Facebook, Marketplace, Instagram, WhatsApp, Messenger et Meta Ads.
- Microsoft : Windows OS et LinkedIn.

Le règlement sur les services numériques dit DSA (*Digital Services Act*), a été adopté le 19 octobre 2022 et est entré en vigueur le 17 février 2024 (*Règlement UE 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, JOUE n° L 277, 27 octobre 2022, p. 1*). Il vise à lutter contre les contenus et produits

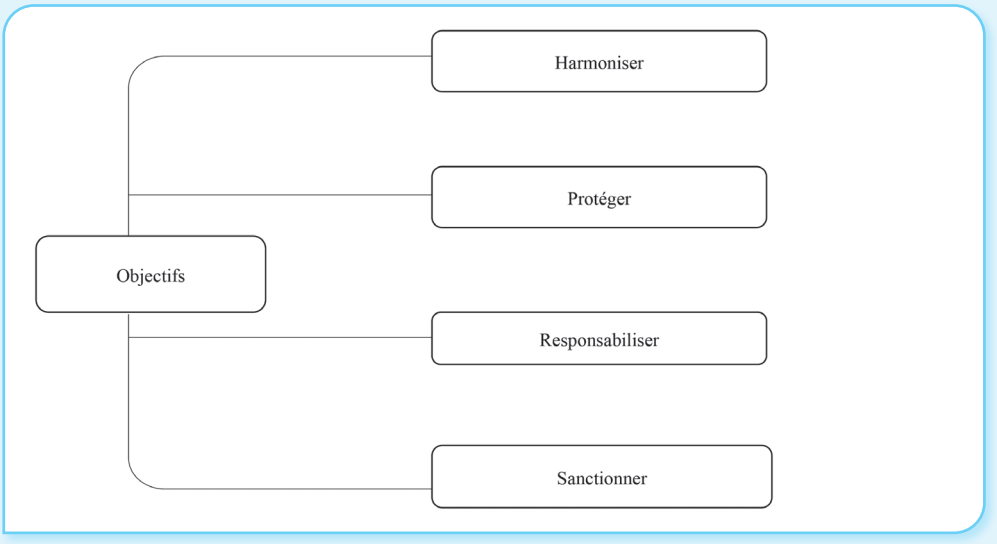
illégaux en ligne (haine, désinformation, contrefaçons…). L'objectif est de faire d'internet un espace plus sûr pour les utilisateurs, en appliquant le principe selon lequel « *ce qui est illégal dans le monde physique l'est aussi en ligne* ». Le DSA concerne tous les intermédiaires en ligne qui offrent leurs services sur le marché européen, peu importe que ces intermédiaires soient établis en Europe ou ailleurs dans le monde.

Sont notamment visés : les fournisseurs d'accès à internet (FAI), les services d'informatique en nuage (*cloud*), les plateformes en ligne et les très grandes plateformes et très grands moteurs de recherche en ligne, utilisés par plus de 45 millions d'européens par mois. La Commission européenne a d'ores et déjà désigné 25 acteurs considérés comme de très grandes plateformes et de très grands moteurs en ligne (AliExpress, Amazon Store, Apple AppStore, Bing, Booking, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X (ex Twitter), YouTube, Zalando, Pornhub, Stripchat, XVideos, Shein, Temu et XNXX).

Ces textes tentent, à travers leurs dispositions, de trouver un équilibre entre la protection des données personnelles des individus et les besoins des organisations qui collectent et traitent ces données. Celles-ci sont en effet indispensables au fonctionnement de ces structures et constituent même le fondement du business model de nombreuses entreprises.

Cet ouvrage à vocation pédagogique exposera plus particulièrement les grands principes portés par le RGPD et son application sur le territoire français, à travers trois parties : l'objet de la protection, les acteurs du traitement et le contrôle du traitement des données personnelles.

Carte mentale 1. Objectifs du RGPD



Partie 1

L’objet de la protection

Chapitre 1

Champ d'application des règles relatives à la protection des données

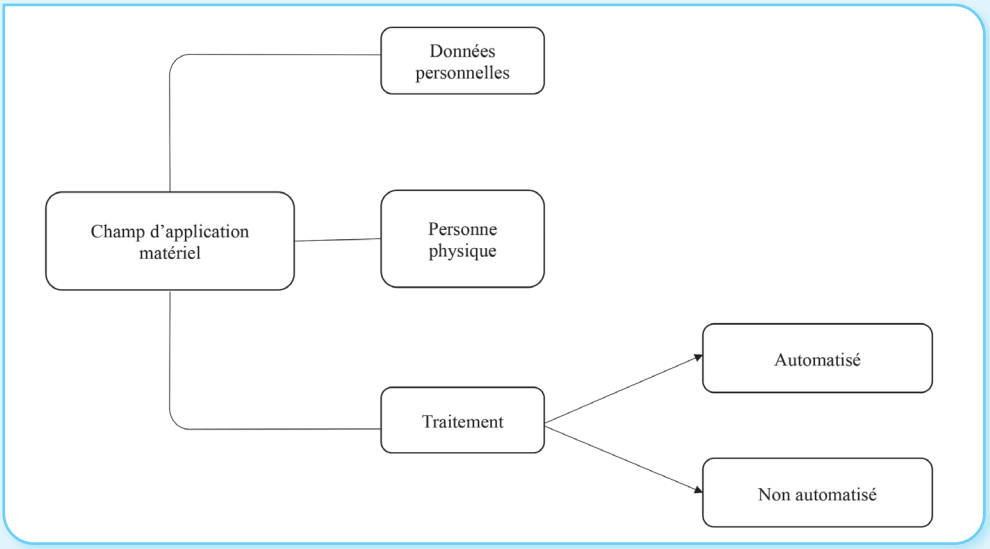
L'application du RGPD suppose d'en déterminer le champ d'application, tant matériel que territorial.

Section 1
Champ d'application matériel

Le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier (*RGPD, article 2*).

L'application du RGPD suppose donc la présence de données à caractère personnel et le traitement de celles-ci.

Carte mentale 2. Champ d'application matériel



I. Des données à caractère personnel

A. Définition

L'article 4-1 du RGPD définit les données à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable (…)* ». Ne sont concernées que les données personnelles se rattachant à une personne physique (*RGPD, article 1*).

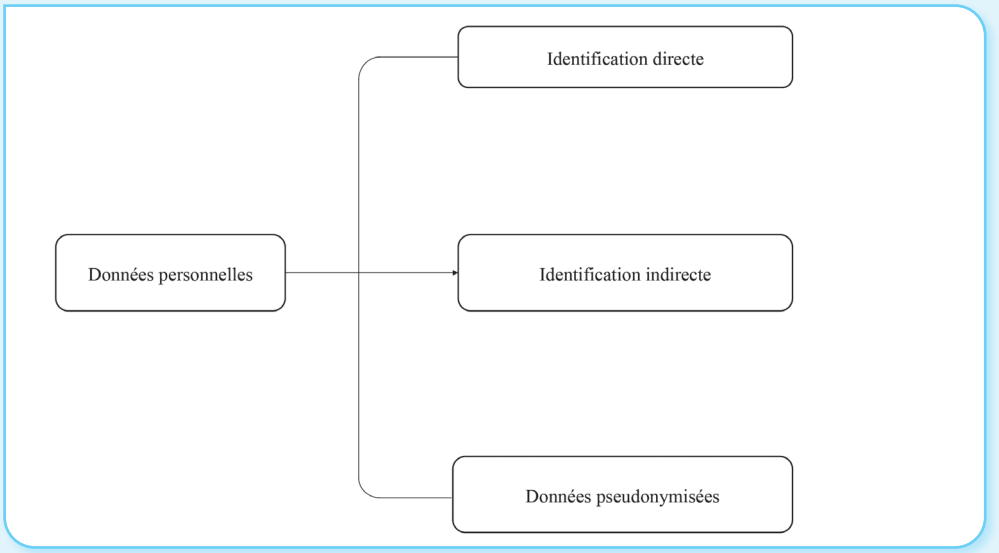
La personne doit pouvoir être identifiée directement ou indirectement. Les données directement identifiantes peuvent consister en un nom et prénom, une photo, etc.

Les données indirectement identifiantes sont celles qui permettent de déterminer l'identité de la personne par référence à un numéro d'identification, des données de localisation, un identifiant en ligne, ou d'autres éléments qui, grâce à des recoupements, permettront de l'identifier. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation demeurent soumises aux règles du RGPD. Les données pseudonymisées restent attachées à une personne, via un identifiant par exemple. Elles pourront être réattribuées à une personne physique par le recours à des informations supplémentaires. Ces informations supplémentaires doivent être conservées séparément

et soumises à des mesures techniques et organisationnelles afin de garantir que les données ne sont pas attribuées à une personne physique identifiée ou identifiable (*RGPD, article 4-5*).

Ex. : *l'étudiant avec des béquilles qui a soutenu sa thèse de médecine générale le 5 octobre à l'Université de Lyon.*

Carte mentale 3. Données personnelles



B. Catégories particulières de données

Certaines catégories de données dites sensibles, font l'objet d'un régime particulier dans la mesure où leur traitement peut avoir un effet potentiellement discriminant.

1. Les données personnelles « sensibles »

Il s'agit de données à caractère personnel qui révèlent « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* » *(RGPD, article 9-1)*.

Le législateur a plus particulièrement défini trois catégories de données : les données génétiques, les donnée biométriques et les données de santé.

Les données génétiques sont « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* » *(RGPD, article 4-13)*.

Ex. : *mutation d'un gène ; existence d'un gène spécifique à une pathologie.*

Les données biométriques sont « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* » *(RGPD, article 4-14)*.

Ex. : *logiciel de reconnaissance faciale ; empreinte rétinienne…*

Les données de santé sont « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » *(RGPD, article 4-15)*. Sont concernées les données provenant tant d'un professionnel de santé que d'un dispositif médical ou du patient lui-même.

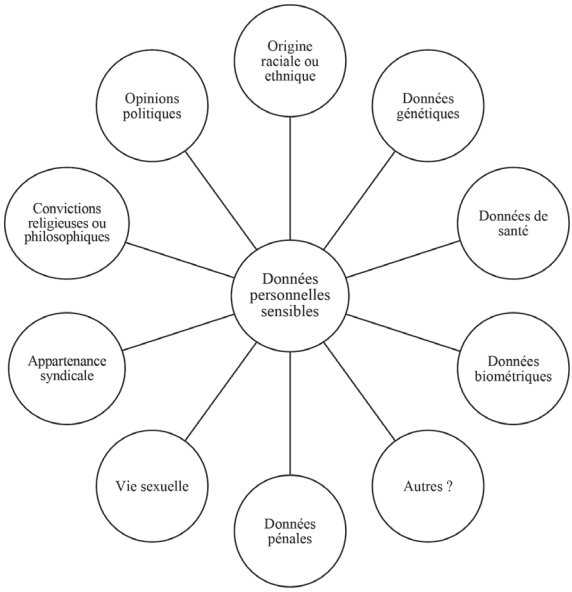
Ex. : *mesure de la fréquence cardiaque, de la glycémie, etc.*

2. Les données relatives aux condamnations pénales et aux infractions

Selon la CNIL, cette catégorie de données comprend les données qualifiées comme telles par une autorité compétente (la condamnation de M. X à une peine d'emprisonnement de 2 ans pour fraude fiscale par exemple) ainsi que les données collectées dans le but d'établir l'existence ou de prévenir la commission d'infractions.

En plus du casier judiciaire, qui reprend les condamnations judiciaires dont une personne a pu faire l'objet, il existe d'autres fichiers de police, gendarmerie ou renseignement (Fichier des personnes recherchées, Fichier national des empreintes génétiques…) dont le traitement des données est soumis au RGPD.

Carte mentale 4. Données personnelles sensibles



C. Exclusion de certaines données

1. Données anonymisées

Les données anonymisées sont exclues du champ d'application du RGPD (*RGPD, considérant 26*) puisqu'elles ne permettent plus l'identification de la personne. Les données anonymisées sont des données personnelles qui ont été rendues anonymes de manière irréversible, garantissant que la personne ne pourra pas être identifiée ultérieurement. L'évolution des outils de traitement de l'information et le développement de l'intelligence artificielle font que l'anonymat est aujourd'hui très rarement atteint.

2. Les données à usage personnel ou domestique

Le règlement ne s'applique pas aux traitements de données personnelles effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale (*RGPD, considérant 18*).

Ce sera par exemple le cas d'un fichier d'adresses à usage privé, l'échange de correspondance, l'utilisation de réseaux sociaux à titre privé, etc.

Toutefois, l'organisme qui fournit les moyens de traiter les données personnelles pour ces activités privées ou domestiques demeure soumis au RGPD.

Ex. : *un étudiant a un compte personnel sur un réseau social. L'ouverture de ce compte ne relève pas du RGPD mais le responsable de l'application qui lui permet d'être présent sur ce réseau devra se soumettre aux obligations du RGPD car il collecte et traite des informations à caractère personnel relatives à l'étudiant ou à ses contacts.*

3. Les données des personnes décédées

Le RGPD n'aborde pas la question du traitement des données personnelles des défunts. Le RGPD ne s'appliquant pas, chaque État membre a la possibilité d'adopter des dispositions sur ce sujet. En France, c'est en 2016 que la loi pour une République numérique a encadré le devenir des données suite au décès de la personne, en modifiant la loi Informatique et libertés (*Loi n° 2016-1321 pour une République numérique du 7 octobre 2016, JORF n° 0235 du 8 octobre 2016*). La mort numérique peut se définir comme la cessation d'activité sur internet du fait du décès d'une personne. Cependant, même après le décès, l'identité numérique d'un individu lui survit. L'identité numérique est « *l'ensemble des traces laissées par un individu (adresses IP, cookies), ses coordonnées d'identification, les contenus qu'il publie ou partage en ligne (blogs, avis, discussions, contributions à des sites collaboratifs, jeux), ses habitudes de consommation sur internet ou son e-réputation* » (*Commission des affaires économiques de l'Assemblée nationale, Rapport d'information sur le développement de l'économie numérique française, 14 mai 2014*). En effet, sans intervention particulière, les données numériques de la personne décédée restent présentes sur le web.

La gestion post-mortem des données personnelles sera différente selon que le défunt a ou non laissé des directives concernant ses données personnelles.

■ Existence de directives laissées par le défunt

Chacun « *peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès* » (*LIL, article 85-I*).

Les directives peuvent être générales ou particulières.

- **Les directives générales** portent sur l'ensemble des données concernant la personne.

  Ex. : *la personne souhaite que tous ses comptes soient supprimés après son décès.*

Elles peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL. Les références des directives générales et du tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique tenu par la CNIL.

- **Les directives particulières** ne concernent que certains traitement de données.

  Ex. : *la personne souhaite que certains comptes uniquement soient supprimés, alors que d'autres seront maintenus.*

Ces directives sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet d'un consentement spécifique et les responsables de traitement concernés doivent inscrire ces directives dans leur registre de traitement.

Les directives peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. Si le défunt a laissé des directives mais n'a désigné aucune personne de confiance, ou en cas de décès de la personne désignée, ce sont ses héritiers qui ont qualité pour prendre connaissance des directives et les mettre en œuvre (*LIL, article 85-I al. 8*).

Ces directives peuvent être modifiées à tout moment.

Absence de directives laissées par le défunt

La plupart des personnes ne se préoccupent pas des conditions de conservation et de communication de leurs données post-mortem. Au décès de la personne, la plupart des profils et des comptes qui lui étaient rattachés sont simplement laissés à l'abandon.

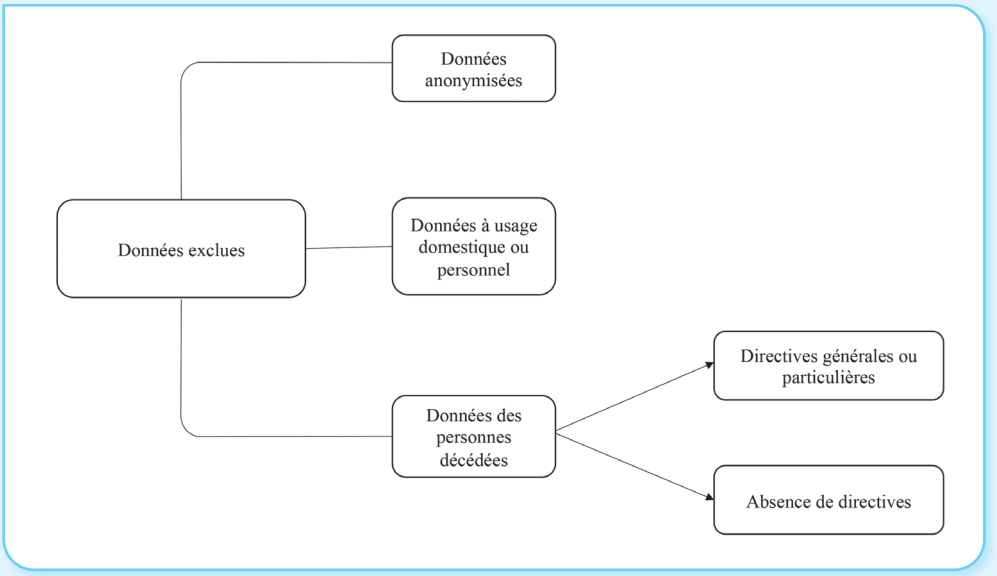
Par principe, un profil sur un réseau social ou un compte de messagerie est strictement personnel et soumis au secret des correspondances. Les données personnelles d'une personne décédée ne sont pas transmissibles à ses héritiers. De ce fait, les héritiers ne peuvent pas se substituer au défunt dans l'exercice de ses droits car ils ne sont pas considérés comme des personnes concernées. En effet, la seule qualité d'ayants droit de la personne à laquelle se rapportent les données ne leur confère pas ce statut (*Conseil d'État, 10e–9e chambres réunies, 7 juin 2017, n° 399446, point 2*). En revanche, lorsque la victime d'un dommage décède, son droit à réparation est transmis à ses héritiers. Par conséquent, lorsque la victime a engagé une action en réparation avant son décès ou lorsque ses héritiers ont ultérieurement eux-mêmes engagé une telle action, ces derniers doivent être regardés comme des « personnes concernées » au sens de la loi Informatique et libertés. Ils peuvent donc exercer leur droit d'accès aux données à caractère personnel concernant le défunt, dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée (*Conseil d'État, 7 juin 2017, n° 399446, point 3*).

La loi prévoit cependant que les héritiers de la personne concernée peuvent exercer certains droits après son décès, lorsque ces droits sont nécessaires à l'organisation et au règlement de la succession du défunt ou à la prise en compte, par les responsables de traitement, de son décès (*LIL, article 85-II*). À ce titre, les héritiers ont un droit d'accès aux traitements de données qui concernent le défunt afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession, recevoir communication des biens

numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers. Ils peuvent également faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.

Les principaux réseaux sociaux proposent des formulaires permettant de gérer les données d'une personne décédée. Les héritiers doivent solliciter chaque responsable de traitement et fournir les justificatifs prouvant leur identité et le décès de la personne.

Carte mentale 5. Données exclues du RGPD



II. Le traitement des données à caractère personnel

A. Définition

Un traitement consiste en une opération ou ensemble d'opérations portant sur des données à caractère personnel, peu importe le procédé utilisé. Le RGPD donne une liste non limitative d'opérations pouvant être qualifiées de traitement : 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 de données.

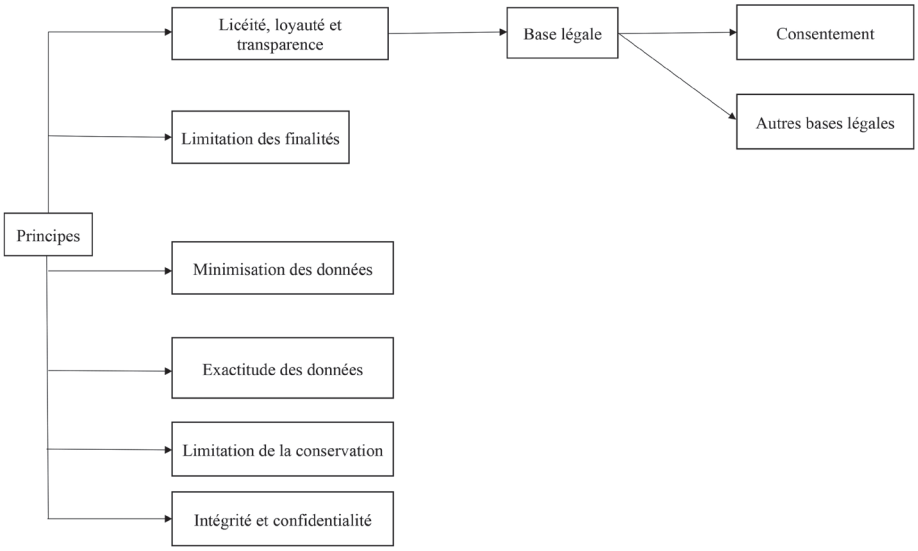
Le traitement ne se limite pas à la constitution d'un fichier. Ainsi, la mise en place d'un système de reconnaissance biométrique ou une application de géolocalisation constitue une opération de traitement de données.

Le traitement peut être informatisé en tout ou partie (base de données par exemple), mais il peut également ne pas être automatisé (traitement manuel de fichiers papier par exemple).

B. Principes applicables au traitement des données personnelles

Tout traitement de données personnelles doit respecter les principes fondamentaux contenus à l'article 5 du RGPD.

Carte mentale 6. Principes applicables au traitement des données personnelles



1. Le principe de licéité, loyauté et transparence

Le responsable du traitement doit informer toute personne dont les données sont collectées, que cette collecte soit directe (données recueillies auprès de la personne) ou indirecte (données récupérées auprès de partenaires commerciaux, de sources accessibles au public, etc.). Les données ne peuvent en aucun cas être collectées à leur insu.

L'information doit être délivrée au moment de la collecte en cas de collecte directe ou dans un délai raisonnable après avoir obtenu les données en cas de collecte indirecte.