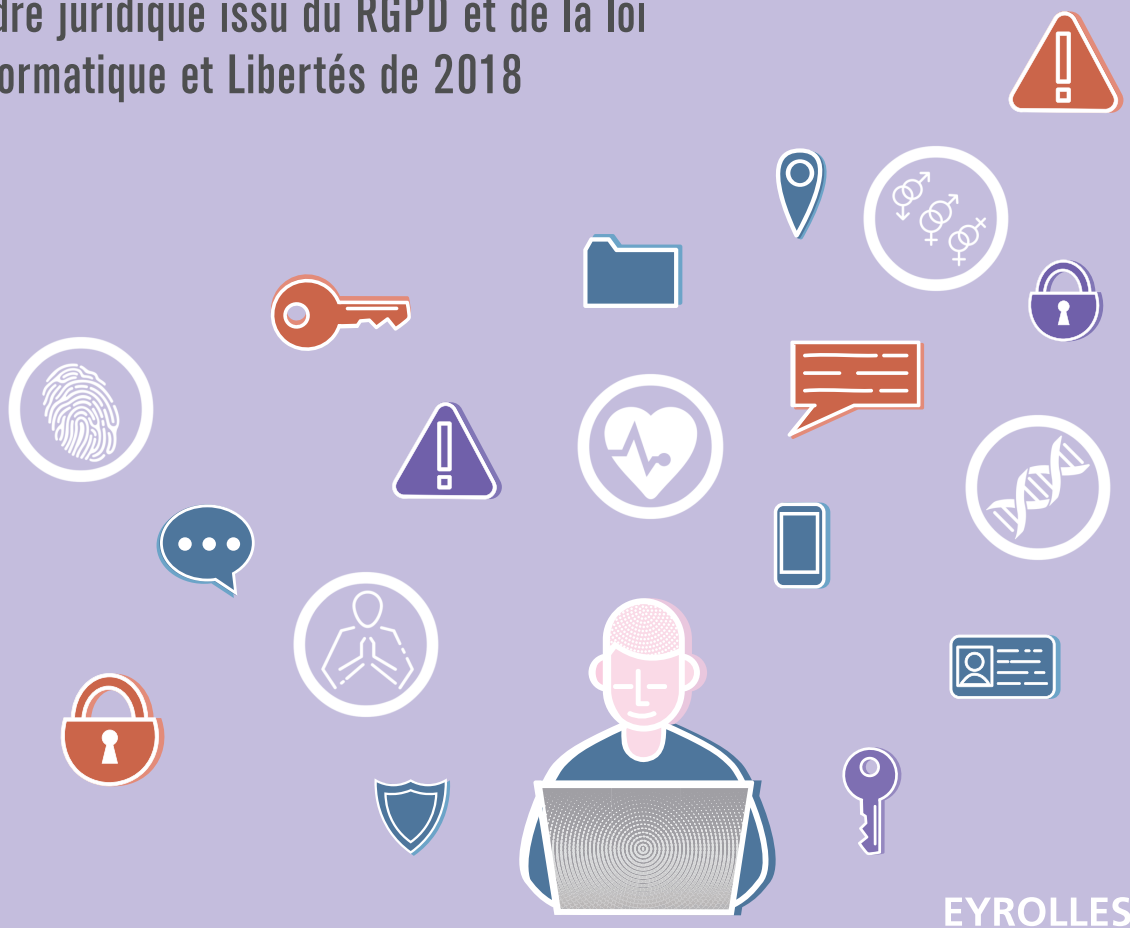
Fabrice Mattatia

RGPD ET DROIT DES DONNÉES PERSONNELLES

Enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et Libertés de 2018



EYROLLES

RGPD et droit des données personnelles

3e édition

1978 : adoption de la loi Informatique et Libertés. 2018 : avec l'entrée en application du règlement européen sur la protection des données et de la nouvelle loi Informatique et Libertés, le cadre juridique du traitement des données personnelles est renouvelé de fond en comble.

Nouvelles notions, nouvelles obligations, sanctions alourdies, les acteurs publics et privés doivent rénover leur gouvernance pour diminuer leur exposition au risque. Une bonne protection des données personnelles représente plus qu'un avantage concurrentiel, notamment en termes d'image de marque ; c'est désormais un must. Voici une présentation complète, totalement remise à jour et remaniée, sur le droit des individus à voir leurs données personnelles protégées, sur les obligations des organisations et des entreprises en la matière, et sur les sanctions encourues en cas de manquement.

La troisième édition de cet ouvrage, totalement remaniée et mise à jour, fait le point sur le droit applicable en France aux traitements des données personnelles suite aux bouleversements du cadre juridique en 2018 (RGPD, nouvelle loi Informatique et Libertés, apports récents de la loi pour une République numérique de 2016, nouveau Code des relations entre le public et l'administration, nouvelles procédures concernant les données en matière de santé, etc.). Elle intéressera aussi bien les juristes en quête d'un ouvrage de synthèse ou les informaticiens préparant un nouveau développement que les directeurs informatiques et les dirigeants d'entreprises ou d'administrations désireux de connaître leurs obligations légales. Ils y trouveront un exposé méthodique des textes applicables, ainsi que l'analyse des jurisprudences les plus récentes, afin de pouvoir répondre aux questions concrètes qu'ils peuvent se poser : quelles sont leurs obligations avant de traiter des données émanant de leurs employés ou de leurs clients ? Quelles formalités administratives accomplir ? Quels sont les droits des personnes concernées ? Y a-t-il des données dont le traitement est interdit ou encadré ? Combien de temps peuvent-ils conserver les données personnelles collectées ? Comment sous-traiter une application informatique ? Peut-on envoyer des données personnelles hors d'Europe, et notamment aux États-Unis ? Quel risque pénal prennent-ils en négligeant leurs obligations ? Comment concilier données personnelles et big data ?

Fabrice Mattatia est à la fois ingénieur spécialisé dans le numérique et docteur en droit. Ancien conseiller de la secrétaire d'État au numérique, il a contribué à plusieurs projets numériques nationaux. Chercheur associé à l'université Paris I, il dirige le mastère spécialisé Data Protection Management de l'Institut Mines - Telecom Business School.

À qui ce livre s'adresse-t-il ?

- À toute organisation publique ou privée qui gère un site sur le Web, une application mobile ou des fichiers, et qui récolte, entre autres, des données client
- Aux développeurs, agences web, prestataires informatiques et SSII
- Aux responsables du traitement des données personnelles, services métier, services marketing, DRH, DSI, DPO, RSSI
- Aux dirigeants d'organisations, pour connaître leurs obligations légales et leur risque pénal ou administratif
- Aux étudiants en informatique et en communication
- Aux juristes à la recherche d'un ouvrage de référence sur ce sujet

www.editions-eyrolles.com

RGPD ET DROIT DES DONNÉES PERSONNELLES

DU MÊME AUTEUR

F. MATTATIA. – **Droit d'auteur et propriété intellectuelle dans le numérique**.
N°67426, 2017, 214 pages.

F. MATTATIA. – **Le droit des données personnelles**.
N°14298, 2e édition, 2016, 234 pages.

F. MATTATIA. – **Internet et les réseaux sociaux : que dit la loi ?**
N°14029, 2e édition, 2015, 246 pages.

F. MATTATIA. – **Expliquer Internet et la loi en milieu scolaire**.
N°14136, 2015, 140 pages.

SUR LE MÊME THÈME

O. ITEANU. – **Quand le digital défie l'état de droit**.
N°11859, 2016, 192 pages.

O. ITEANU. – **L'identité numérique en question**.
N°12255, 2008, 166 pages.

Fabrice Mattatia

RGPD ET DROIT DES DONNÉES PERSONNELLES

Enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et Libertés de 2018

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Crédits iconographiques
Figures pages 99 et 103 : © Groupe de travail Article 29 sur la protection des données

Table des matières

CHAPITRE 4

Principales obligations 75

CHAPITRE 8

Que risquez-vous devant un tribunal ? 177

CHAPITRE 9

Introduction

La pratique de la Kabbale est une bonne préparation à la lecture du règlement européen sur la protection des données.

Paul-Olivier Gibert
Président de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP)[1]

À partir de 2018, l'entrée en application du nouveau règlement européen sur la protection des données personnelles, qui remplace de larges pans de la loi Informatique et Libertés, bouleverse le cadre juridique applicable aux données personnelles. Même si les principes fondamentaux demeurent, la mise en œuvre des obligations légales change fondamentalement. La très symbolique loi Informatique et Libertés elle-même est modifiée pour s'adapter au règlement.

Cet ouvrage fait par conséquent le point sur le nouveau cadre légal en vigueur, résultant principalement du règlement européen et de la nouvelle loi Informatique et Libertés, mais aussi des apports récents de la loi pour une République numérique de 2016, du nouveau code des relations entre le public et l'administration, des nouvelles procédures concernant les données de santé, etc. Un droit des données personnelles totalement renouvelé émerge désormais. Il est enfin stabilisé après plusieurs années d'incertitude, ce qui permet d'en proposer une présentation complète.

Pour le travail comme pour les loisirs, il devient difficile d'échapper à l'utilisation des ordinateurs fixes ou portables reliés à Internet, des smartphones, des cartes à puce… pour ne citer que les applications dont les utilisateurs sont conscients. Notre smartphone permet de nous localiser en permanence grâce au GPS intégré, et d'enregistrer tous nos déplacements. Désormais arrivent les objets communicants, voitures et autres compteurs électriques, réunis au sein d'un « Internet des objets », dans lequel tous les objets de notre environnement communiqueront bientôt entre eux pour notre plus grand bien : le réfrigérateur deviendra capable de gérer le stock

1. Allocution de Paul-Olivier Gibert, université des Correspondants Informatique et Libertés, 25 janvier 2017.

de yaourts et d'en commander lui-même par Internet lorsque cela lui apparaîtra nécessaire. Le *quantified self*, qui consiste à porter des objets connectés (montres, bracelets, lunettes…) pour enregistrer sa vie quotidienne, ses activités, le nombre de calories ingérées… se répand également. Ces évolutions nécessitent la multiplication d'échanges de données personnelles.

Vocabulaire

Pour une plus grande commodité de lecture, nous remplacerons l'expression officielle « données à caractère personnel » par « données personnelles ».

Non seulement l'exploitation des données personnelles est indispensable au fonctionnement même des nouveaux services, qu'il s'agisse des réseaux sociaux, de la relation client personnalisée ou des comptes en ligne proposés par les administrations ou par les banques, mais la connaissance de l'utilisateur ou du client devient un élément essentiel du modèle économique de ces services. La volonté de limiter l'exploitation des données personnelles risque alors d'entrer en conflit avec la créativité des nouveaux services et d'en entraver le développement en empêchant de valoriser ces données.

Le traitement des données personnelles représente désormais un enjeu crucial pour les responsables d'entreprises, d'administrations ou d'associations : qu'il s'agisse des données de leurs employés, de leurs clients, de leurs usagers ou de leurs membres, elles sont omniprésentes et doivent être traitées et protégées dans les formes prescrites par la loi. Or, leur importance économique est croissante : l'exploitation des données personnelles permet non seulement de rendre un meilleur service aux clients, mais parfois aussi de financer à elle seule ce service. Tous les nouveaux géants du Web, les Facebook et les Google, ne sont gratuits que parce qu'ils monétisent les données personnelles de leurs utilisateurs concernant leur profil de consommation, leurs centres d'intérêts ou leur mode de vie.

PERSPECTIVES La valeur des données personnelles

Selon une étude du Boston Consulting Group publiée en 2012, « The value of our digital identity », la valeur totale des données personnelles des citoyens européens représenterait 330 milliards d'euros par an pour les organisations publiques et privées (gains de productivité et conquête de nouveaux marchés). La libéralisation de l'usage de ces données amènerait également un gain potentiel de 670 milliards d'euros par an pour les consommateurs (gains de temps et baisses de prix).

Cependant, les responsables des traitements ne peuvent se permettre d'abuser des données qu'ils ont récoltées. Protéger les données personnelles des individus est indispensable pour préserver leur vie privée et leurs droits fondamentaux, tels que les libertés d'opinion, d'expression et de communication, la non-discrimination, l'égalité de traitement, etc. Par conséquent, la loi fixe un cadre strict et des limites précises à l'exploitation qui peut en être faite ; des sanctions administratives et pénales sont prévues en cas d'infraction. Ensuite, le citoyen-client, de plus en plus conscient des risques, est lui-même demandeur de garanties sur l'usage de ses données. Les pressions exercées à de multiples reprises sur Facebook par ses utilisateurs mécontents, qui ont contraint plus d'une fois le réseau social à reculer, témoignent de l'importance croissante de la demande de protection des données personnelles.

Bien plus, le respect des données personnelles et de la vie privée constitue désormais un argument commercial et un avantage compétitif dans la concurrence entre acteurs marchands. Dans ce contexte, pour se démarquer, les directeurs de projets informatiques, des systèmes d'informations ou les responsables de traitement de données, ce qui inclut les dirigeants d'entreprise, ont désormais intérêt à adopter des pratiques vertueuses, c'est-à-dire à connaître les principes de protection des données personnelles, à les appliquer et, *surtout* à le faire savoir !

Note au lecteur

Cet ouvrage a pour ambition de donner une vision d'ensemble sur un sujet complexe. Aussi, pour une lecture plus fluide et plus aisée, certains points seront simplifiés et vulgarisés. Chaque cas d'espèce présentant des particularités, il est conseillé au lecteur, lors de la mise en œuvre d'un traitement de données personnelles, de prendre le conseil d'un juriste spécialisé.
Les ouvrages juridiques de référence à consulter pour plus de précisions figurent en bibliographie.

Rappels juridiques

RAPPEL La hiérarchie des tribunaux

Un litige judiciaire est jugé par un tribunal en première instance (tribunal d'instance [TI] ou de grande instance [TGI]).
Si la décision ne satisfait pas l'une des parties, celle-ci peut faire appel ; et le litige sera rejugé sur le fond par une cour d'appel (CA).
L'arrêt d'appel ne peut plus être rejugé, sauf s'il comporte un vice de procédure. La partie lésée doit alors introduire un pourvoi en cassation auprès de la Cour de cassation. Celle-ci ne juge pas sur le fond, mais examine seulement si la cour d'appel a bien appliqué le droit. Si elle estime que ce n'est pas le cas, elle casse l'arrêt d'appel et renvoie le dossier devant une nouvelle cour d'appel pour un nouveau jugement sur le fond. À cette occasion, la Cour de cassation explique souvent comment il faut comprendre la loi, d'où l'intérêt de l'analyse de ses motivations.
En outre, depuis 2008, dans le cadre d'un procès, il est possible, pour une personne estimant que la loi applicable est contraire à la Constitution, de déposer une question prioritaire de constitutionnalité (QPC). Si cette question est validée par le Conseil d'État ou par la Cour de cassation, elle est transmise au Conseil constitutionnel. L'examen du litige est alors suspendu dans l'attente de la réponse du Conseil.

RAPPEL La hiérarchie des textes en France

En France, le texte le plus fondamental est la **Constitution**, qui organise notamment le partage des compétences entre les pouvoirs législatif et exécutif.
Comme son nom l'indique, le pouvoir législatif (le Parlement) a pour fonction de discuter et d'adopter les lois. Une **loi** décrit des situations générales.
Le pouvoir exécutif (le Gouvernement), qui a pour fonction de faire exécuter ces lois, publie le cas échéant des **décrets** précisant certains détails nécessaires à l'application de la loi. Il publie également, si besoin, des **arrêtés** pour préciser des mesures particulières : tarifs, nominations, autorisations…
Dans certains cas (urgence, technicité, nécessité d'un rédacteur unique…), le Parlement peut déléguer au pouvoir exécutif le droit de rédiger un texte législatif, en lui remettant un mandat bien précis. À cette occasion, le texte, qui est du niveau d'une loi, porte le nom d'**ordonnance**.
L'administration peut rédiger une **circulaire** pour expliciter son interprétation d'une loi ou d'un décret. Une circulaire n'a pas de valeur juridique, même si en pratique elle est appliquée par les services.
La hiérarchie des textes est donc :

- Constitution
- Loi/ordonnance
- Décret
- Arrêté

Par exemple, le statut général d'un fonctionnaire de l'État dépend de la loi de 1983 sur la fonction publique. Son statut particulier (missions, déroulement de carrière…) dépend du décret organisant le corps auquel il appartient (enseignant, administrateur civil, ingénieur, militaire…). Son affectation et son niveau de rémunération sont fixés par des arrêtés personnels.

Table des abréviations

AAI	Autorité administrative indépendante
ARCEP	Autorité de régulation des communications électroniques et des postes
CA	Cour d'appel
CAA	Cour administrative d'appel
Cass. civ.	Arrêt de la Cour de cassation, chambre civile
Cass. com.	Arrêt de la Cour de cassation, chambre commerciale
Cass. crim.	Arrêt de la Cour de cassation, chambre criminelle
CE	Conseil d'État
CEDH	Cour européenne des droits de l'homme
CGU	Conditions générales d'utilisation
ch.	Chambre
CJCE	Cour de justice de la Communauté européenne
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Cons. cons.	Conseil constitutionnel
CP	Code pénal
CPCE	Code des postes et des communications électroniques
CPI	Code de la propriété intellectuelle
CRPA	Code des relations entre le public et l'administration
FAI	Fournisseurs d'accès Internet
G29	Groupe de l'article 29
HADOPI	Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet
IP	*Internet Protocol*
JORF	Journal officiel de la République française
LCEN	Loi pour la confiance dans l'économie numérique
NIR	Numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, plus connu sous le nom de « numéro de sécurité sociale »
OCDE	Organisation de coopération et de développement économiques
RGPD	Règlement général sur la protection des données
STAD	Système de traitement automatisé de données
T. Com.	Tribunal de commerce
T. corr.	Tribunal correctionnel
TA	Tribunal administratif
TGI	Tribunal de grande instance
TI	Tribunal d'instance
TUE	Tribunal de l'Union européenne

1

Les grands principes

Domus tutissimum cuique refugium atque receptaculum sit[1]

Gaïus, cité par le Digeste *de Justinien, 2, IV, 18*

Les préoccupations relatives à la protection des données personnelles contre l'informatique ont émergé dans les années 1970, lorsque les progrès technologiques ont donné aux États la capacité de « fliquer » leur population en constituant de gigantesques bases de données.

Le concept de tels fichiers n'était toutefois pas nouveau : dès 1749, le policier Guillaute, dans son *Mémoire sur la réformation de la police de France*, suggérait à Louis XV de créer un fichier des habitants de Paris ; et au XIX^e^ siècle, le fichier (manuel) de la préfecture de police de Paris regroupait des millions de fiches concernant des criminels. Mais c'est dans les années 1970 que l'informatique permit d'industrialiser ces fichiers, de les automatiser, et de donner corps au spectre si redouté de *Big Brother*. Or, à la même période, le respect de la vie privée devenait également une priorité, puisque c'est en 1970 que ce principe fut inscrit dans le Code civil.

Ainsi, les notions de données personnelles et de vie privée sont étroitement mêlées.

1. « Le domicile doit constituer pour chacun un refuge inviolable. »

Vie privée : une notion récente et imprécise

Une notion récente

La vie privée est un concept relativement récent, d'un point de vue aussi bien sociologique que juridique. Des philosophes comme Aristote ont distingué vie publique (du citoyen) et vie familiale ; Montaigne estimait qu'on n'est libre que si l'on peut s'isoler pour réfléchir dans la sphère privée. Mais la notion juridique d'un véritable droit à l'intimité et à la vie privée n'a pris corps qu'au XIX^{e} siècle dans les pays industrialisés. Elle est formalisée pour la première fois dans un article de 1890 de Brandeis et Warren dans la *Harvard Law Review*, intitulé « *The Right to Privacy* ». Il s'agissait déjà de protéger cette vie privée contre les intrusions de la technologie et des médias de l'époque : la presse et la photographie.

En France, si la Déclaration des droits de l'homme de 1789 reconnaît un droit à la sûreté, il faut l'entendre essentiellement comme une protection de l'individu contre les abus du pouvoir. Ce n'est qu'en 1970 que fut inséré dans l'article 9 du Code civil, le principe que « chacun a droit au respect de sa vie privée ». Enfin, c'est en 1999, lors de la discussion de la loi sur la couverture maladie universelle, que le Conseil constitutionnel a rattaché le droit à la vie privée à l'article 2 de la Déclaration de 1789 (« la liberté proclamée par cet article 2 implique le respect de la vie privée »)[2], lui donnant ainsi une portée constitutionnelle. Le droit à la protection de la vie privée est donc particulièrement récent.

Il reste à donner une définition de la « vie privée ». Le droit à la vie privée consiste à pouvoir conserver une part d'intimité, ce qui doit certes s'entendre comme le droit à ne pas voir certaines actions surveillées ou divulguées, mais qui recouvre également le droit à ne pas subir des sollicitations ou des discriminations en fonction d'une vie privée que l'on ne souhaite pas divulguer. Mais cette notion n'est pas précisée par le droit. C'est donc par une construction progressive de la jurisprudence que l'on constate, au gré des jugements, que ce concept peut englober aussi bien le droit à l'intimité et le droit au secret des correspondances écrites, téléphoniques et électroniques, que la protection contre l'informatique, voire le droit à l'image (qui est pourtant plutôt d'ordre patrimonial). Non seulement les jurisprudences ne permettent pas de dégager une définition globale de la vie privée, mais il apparaît que le respect qui lui est dû n'est pas absolu : la liberté d'expression ou l'intérêt public peuvent éventuellement justifier des atteintes à ce droit.

S'il n'existe pas de définition positive de la vie privée, peut-on recourir à une définition négative, en l'opposant à la vie publique ? Relèverait alors du domaine privé tout ce qui n'advient pas dans le domaine public ou qui n'est pas porté à la connaissance du public par la personne concernée. Mais il ne s'agit pas là non plus d'un critère absolu. La notoriété de la personne concernée, le lieu où se déroulent les faits concernés, la volonté plus ou moins affichée de communiquer sur sa vie privée ou au contraire de la protéger jouent également leur rôle. On peut ainsi donner l'exemple des informations concernant la santé, qui forment une part éminemment sensible de la vie privée de chacun ; s'agissant de la santé du président de la République, un débat oppose depuis des décennies les partisans du secret à ceux de la transparence.

2. Cons. cons., décision n° 99-416 DC du 23 juillet 1999.

Une notion relative

Comme l'écrit le tribunal de grande instance de Paris, « en vertu de l'article 9 du Code civil, toute personne a droit au respect de sa vie privée et est fondée à en obtenir la protection, toute personne dispose également en vertu du même texte, d'un droit exclusif sur son image, attribut de la personnalité, et sur l'utilisation qui en est faite ; ce droit lui permet, en principe, de s'opposer à la diffusion de celle-ci sans son autorisation et d'obtenir réparation du préjudice qui lui aurait été causé de ce fait »[a].
Mais, poursuit le tribunal, « ces droits peuvent cependant céder devant les nécessités de la liberté d'expression lorsque la diffusion des informations ou des images sont légitimes au regard de ces nécessités, l'appréciation de cette légitimité étant fonction d'un ensemble de circonstances tenant à la personne qui se plaint de l'atteinte aux droits protégés par l'article 9 du Code civil, notamment sa qualité et son comportement antérieur, l'objet de la publication en cause, son contenu, sa forme, l'absence de malveillance et d'atteinte à la dignité de la personne, ainsi que sa participation à un débat d'intérêt général ».

a. TGI Paris, 17e ch., 13 novembre 2013.

DROIT INTERNATIONAL **Notion de vie privée**

Les textes fondamentaux

L'article 12 de la Déclaration universelle des droits de l'homme (1948) dispose :
« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »
Ce thème est repris par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (1950) :
« Article 8 – Droit au respect de la vie privée et familiale
Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »
La jurisprudence de la Cour européenne des droits de l'homme (CEDH) confirme que la protection des données personnelles représente une composante du droit à la vie privée et relève à ce titre de l'article 8 de la Convention.

Les textes européens

La Charte des droits fondamentaux de l'Union européenne, qui figure à l'article 6 du Traité sur l'Union européenne depuis 2009, énonce un droit au respect de la vie privée et familiale et un droit à la protection des données personnelles :
« Article 7 - Respect de la vie privée et familiale
Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.
Article 8 - Protection des données à caractère personnel
1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

De la vie privée aux données personnelles

Il convient de souligner la différence entre « vie privée » et « données personnelles ». Toutes les données personnelles ne relèvent pas de la vie privée. Par exemple, les informations concernant l'activité publique d'un individu constituent des données personnelles, mais ne relèvent pas de sa vie privée. Si le concept de vie privée existe depuis le XIX^e^ siècle, c'est seulement avec la généralisation de l'informatique qu'est apparue la nécessité de prévoir également une protection pour les données personnelles.

Jusqu'au début des années 1980, le système informatique se résumait à un ordinateur central avec ses logiciels, régis par le droit de l'informatique (consacré au traitement de l'information). L'invention d'Internet fut l'occasion d'un changement fondamental en créant un réseau mondial et décentralisé. Dans ce cadre, la protection des données personnelles a pour objectif d'établir un équilibre entre les droits des personnes (vie privée, mais aussi liberté de penser et de communiquer, droit de ne pas être soumis à une décision automatique, etc.) et le légitime besoin de certains tiers (entreprises, administrations) de traiter des informations concernant ces mêmes personnes.

Historiquement, le droit à la protection des données personnelles s'est constitué en accompagnant le développement de l'informatique. Dans les années 1970, plusieurs pays ont pris des mesures, avant qu'une harmonisation internationale ne débute dans les années 1980. Cette protection offerte aux citoyens s'est imposée en réaction aux risques croissants que la puissance de l'informatique – on ne parlait pas encore de nouvelles technologies, mais celles-ci ont confirmé la tendance – faisait courir aux droits fondamentaux, en donnant aux États la possibilité technique de collecter tous les faits et gestes. Elle résulte d'une prise de conscience des limites à imposer aux moyens de surveillance pour préserver ces droits. Les États ont donc accepté d'encadrer leurs pratiques, en se dotant d'une législation protectrice.

Depuis les années 1970, la situation a encore évolué, et les États ne sont plus les seuls à menacer les droits des individus : d'abord, les entreprises ont acquis elles aussi la capacité de collecter et de traiter les données personnelles de leurs salariés, de leurs clients ou de leurs prospects. Puis, plus récemment, chacun, muni de son PC, de sa tablette ou de son smartphone, se retrouve dépositaire, sciemment ou inconsciemment, de ses données personnelles et de celles de ses relations.

Historique de la loi Informatique et Libertés

Un texte évolutif

Le droit français de la protection des données personnelles s'est construit en réaction aux dangers réels ou supposés des nouvelles technologies. Dans les années 1970, la divulgation du projet du ministère de l'Intérieur de créer un mégafichier appelé SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) et contenant les données de toute la population, crée le scandale, conduit à l'adoption de la loi de 1978 et à la création de la CNIL.

« Safari » ou la chasse aux Français

Extrait de l'article fondateur de Philippe Boucher dans *Le Monde*, 21 mars 1974.
« Rue Jules Breton, à Paris 13e, dans les locaux du ministre de l'Intérieur, un ordinateur Iris-80 avec biprocesseur est en cours de mise en marche. À travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouvent posées – et, à terme, théoriquement résolues – les données d'un problème comprenant, d'une part, l'énormité des renseignements collectés ; de l'autre, la méthode à définir pour faire de cet ensemble une source unique, à tous égards, de renseignements.
L'histoire du très puissant appareil qu'est l'Iris-80 est exemplaire du secret qui entoure l'épanouissement de l'informatique dans les administrations, quelles que puissent être les informations qui filtrent ici et là. Puissant, cet Iris-80, une comparaison le démontre sans contestation. L'appareil employé pour engranger les données de l'opération Safari, qui concerne l'identification individuelle de l'ensemble des 52 millions de Français, a une contenance de 2 milliards d'octets. Celle de l'ordinateur du ministère de l'Intérieur est de 3,2 milliards d'octets. […] Le ministère de l'Intérieur a d'encore plus vastes ambitions. Détenteurs, déjà, du fichier national du remembrement, les services de M. Jacques Chirac font de grands efforts pour, affirme-t-on, s'en adjoindre d'autres : le cadastre, le fichier de la direction nationale des impôts et, plus grave peut-être, celui du ministère du Travail.
De telles visées comportent un danger qui saute aux yeux, et que M. Adolphe Touffait, procureur général de la Cour de cassation, avait parfaitement défini le 9 avril 1973 devant l'Académie des sciences morales et politiques, en disant : "La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques". »
Pour mesurer les progrès effectués depuis cette époque, on notera que l'auteur soulignait l'effrayante capacité de stockage de l'ordinateur du ministère de l'Intérieur en 1974 : une mémoire de 2 Go…

À l'époque, le risque ressenti comme majeur résidait dans les fichiers que seuls le gouvernement et quelques entreprises pouvaient s'offrir : la loi initiale était donc très axée sur le contrôle des fichiers. Avec la généralisation, à partir des années 1980, de l'informatique à toutes les entreprises, puis à tous les individus, le risque principal réside désormais dans les données personnelles et les traces concernant chaque individu, disséminées potentiellement dans le monde entier grâce à Internet et au *cloud computing*. La loi moderne doit désormais s'attacher à protéger efficacement chaque donnée, qu'elle soit ou non dans un fichier, car les données personnelles sont devenues le « carburant » de l'économie numérique, et la contrepartie de la gratuité des services.

Des principes persistants

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est la loi fondatrice de la protection des données personnelles en France. Modifiée à de nombreuses reprises, et particulièrement en 2004 pour transposer la directive européenne de 1995, cette loi demeure en vigueur, mais de nombreux pans ont été remplacés par le nouveau Règlement européen de 2016.

Cette loi avait été rédigée à l'origine dans une optique de contrôle des fichiers centraux, principalement de l'État, tandis que la directive de 1995 avait une visée plus large concernant aussi bien l'administration que le secteur privé. Toutefois, la directive de 1995 n'a pas révolu-

tionné les principes préexistants de la protection des données en France, comme le principe de loyauté de la collecte des données, la protection des données dites sensibles, le principe de finalité des traitements ou le droit d'information, de rectification ou d'opposition des personnes, ainsi que l'exigence d'une autorité de contrôle indépendante. Cela n'est pas surprenant, car la directive était elle-même largement inspirée de la loi française de 1978. Le législateur, en transposant cette directive par la loi du 6 août 2004, a surtout pris acte de la montée en puissance des traitements privés, rééquilibrant ainsi une loi initialement tournée vers les fichiers publics. Il a principalement axé le nouveau dispositif de protection sur le critère de la sensibilité des données, que le fichier soit public ou privé, comme l'exigeait la directive.

La transposition en 2004 de la directive de 1995 a en définitive nécessité la modification de la loi Informatique et Libertés initiale sur les points suivants :

- la prise en compte, dans le champ d'application de la loi, des fichiers manuels, des sons et des images, y compris la vidéosurveillance privée mais à l'exception de la vidéosurveillance pour la sécurité publique qui fait l'objet d'une loi distincte (loi n° 95-73 du 21 janvier 1995, désormais codifiée par les articles L251-1 et suivants du Code de la sécurité intérieure) ;
- le renforcement des pouvoirs de contrôle *a posteriori* de la CNIL qui se voit en outre dotée d'un pouvoir de sanction envers le secteur privé ;
- l'égalité de procédure entre traitements relevant du secteur public et ceux relevant du secteur privé, sauf pour les domaines de souveraineté, qui ne relèvent pas de la compétence de l'Union européenne ;
- la distinction entre les transferts de données internes à l'Union européenne (autorisés sans formalité) et ceux à destination d'États tiers, qui ne deviennent possibles que si l'État destinataire assure un niveau de protection adéquat.

On constate ainsi l'importance de définir dans la loi des principes suffisamment universels pour résister à l'évolution technologique, comme l'obtention du consentement, la finalité explicite du traitement, la proportionnalité de la collecte, l'exactitude des données, ou encore la limitation de la durée de conservation.

Un objectif moral

La loi dispose en son article 1 :

« 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.

Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

Le législateur rappelle ainsi la subordination de l'informatique à l'humain : la technique doit être un moyen, non une fin. Il affirme également la suprématie de certaines valeurs : identité humaine, droits de l'homme, vie privée, libertés.