

## De la protection des données personnelles à la lumière de la loi n° 18-07 : une nouvelle responsabilisation pour les entreprises

**YACOUB Zina** <sup>(1)</sup>

<sup>(1)</sup> Maître de conférences classe « A », Faculté de Droit et des Sciences Politiques, membre du Laboratoire de recherche sur l'effectivité de la norme juridique, Université de Bejaia, 06000 Bejaia, Algérie  
Email : [t\\_ninadz@yahoo.fr](mailto:t_ninadz@yahoo.fr)

### Résumé :

La loi n° 18-07 relative à la protection des personnes physiques dans le traitement de leurs données personnelles, est intervenue dans un environnement économique propice au marchandage des données personnelles au détriment du respect de la vie privée. Cette loi institue de nouvelles obligations pour les entreprises, lieu dans lequel s'enchevêtrent les opérations de traitement des données entre clients, salariés, consommateurs et utilisateurs. Ces obligations, destinées à assurer l'équilibre entre le traitement nécessaire des données personnelles et la protection vitale de la vie privée varient selon le positionnement de l'entreprise dans l'opération de traitement des données, et la qualité de la personne physique sujette à ce traitement.

### Mots clés :

Données personnelles, vie privée, entreprises, traitement des données, économie numérique, responsable du traitement, sous-traitance des données, protection, obligations.

---

*Date de soumission : 14/04/2021, Date d'acceptation : 15/05/2021, Date de publication : 08/06/2021*

**Pour citer l'article :**

YAKOUB Zina, « De la protection des données personnelles à la lumière de la loi n° 18-07 : une nouvelle responsabilisation pour les entreprises ». RARJ, Vol. 12, n° 01 (spécial), 2021, pp. 664-689

**Disponible sur :** <https://www.asjp.cerist.dz/en/PresentationRevue/72>

**L'auteur correspondant :** Yakoub Zina, [t\\_ninadz@yahoo.fr](mailto:t_ninadz@yahoo.fr)

## حول حماية البيانات الشخصية على ضوء قانون رقم 07-18 : مسؤولية جديدة المؤسسات في ظل الاقتصاد الرقمي

### المخلص:

لقد صدر قانون 07-18 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي في بيئة اقتصادية تحفز الاستغلال اللاعقلاني للبيانات الشخصية على حساب احترام الحياة الشخصية. يضع هذا القانون التزامات جديدة على عاتق المؤسسة، أين تتشابك مختلف عمليات معالجة المعطيات الشخصية للزبائن، العمال، المستهلكين ومستخدمي الأنترنت. هذه الالتزامات التي من شأنها أن تحقق التوازن بين المعالجة الضرورية للمعطيات الشخصية والحماية اللازمة للحياة الشخصية، تتباين وفقا لموقع المؤسسة في عملية معالجة المعطيات وصفة الشخص الطبيعي موضوع هذه المعالجة.

### الكلمات المفتاحية:

المؤسسة، المعطيات الشخصية، الاقتصاد الرقمي، الحماية، معالجة المعطيات، الحياة الشخصية، مسؤول المعالجة، الالتزامات.

## On the protection of personal data in the light of Law n ° 18-07: A new responsibility for companies

### Abstract :

Law n ° 18-07 relating to the protection of natural persons in the processing of their personal data intervened in an economic environment conducive to the haggling of personal data to the detriment of respect for private life. This law institutes new obligations for companies, a place in which data processing operations between customers, employees and users are entangled. These obligations, intended to ensure the balance between the necessary processing of personal data and the vital protection of privacy, vary according to the positioning of the company in the data processing operation, and the quality of the natural person subject to this treatment.

### Keyword :

Personal data, privacy, companies, data processing, digital economy, data controller, protection, obligations.

## Introduction

La révolution numérique dans les entreprises, marquée par le développement de l'intelligence artificielle et l'évolution sans précédent des Techniques d'Information et de Communication (TIC), a comme conséquence directe le traitement massif de données personnelles de toutes les personnes physiques qui interviennent tant dans le processus de la production que dans celui de la consommation.

Clients, salariés, consommateurs et/ou utilisateurs, dressent la problématique du respect de leur vie privée, en ce sens que, si la collecte informatique de données est un outil incontournable de gestion, tant pour les transactions économiques que pour les relations de travail, laisser libre court à l'autonomie des entreprises dans le traitement des données personnelles des différents acteurs de la sphère économique, pourrait constituer une atteinte à leur vie privée et à leurs libertés individuelles.

Il n'est d'ailleurs pas facile de trouver le juste équilibre entre le traitement et l'usage des données nécessaires au fonctionnement de l'entreprise et sa course concurrentielle à l'ère de l'économie numérique, d'une part, et la protection de la vie privée des personnes physiques qui interviennent dans la vie économique de celle-ci, d'autre part. C'est pourquoi, les obligations, et donc la responsabilisation des entreprises en matière de protection des données personnelles, sont conditionnées par plusieurs variantes, dont le positionnement de celles-ci dans l'opération de traitement des données, la qualité de la personne physique objet de ce traitement, l'objectif du traitement et la nature des données récoltées.

Et alors que les rhétoriques de la protection des données personnelles étaient méconnues en Algérie, voilà qu'intervient la loi n° 18-07 relative à la protection des personnes physiques dans le traitement de leurs données personnelles<sup>1</sup>, pour poser les lignes directrices d'une politique de protection des données, en établissant les règles à respecter lors du traitement des données personnelles des personnes physiques, de sorte à garantir le respect de leur vie privée. Cette loi étant à vocation générale, son applicabilité à l'entreprise suscite une étude minutieuse de ses dispositions en les adaptant aux différents statuts que celle-ci peut revêtir dans ses rapports avec plusieurs catégories de personnes physiques.

Par ailleurs, le sujet étant inédit en Algérie, il convient de s'inspirer des dispositifs internationaux entrepris en la matière et qui traitent, dans de bien plus amples détails, les différentes situations de traitements des données personnelles dans l'entreprise et le régime applicable à chacune d'entre elles.

En ces termes, la question qui se pose est de savoir comment la loi n° 18-07, dans sa généralité et l'absence des textes d'application, pourrait s'appliquer dans

---

<sup>1</sup> Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 34 du 10/06/2018.

l'entreprise, lieu propice d'exploitation des données personnelles, dans toutes les variations qui engagent différemment la responsabilité de l'entreprise en cette matière ?

Il s'agit donc dans cette étude, de mettre la lumière sur les nouvelles obligations qui s'imposent à l'entreprise dans le cadre du traitement des données personnelles, et les droits qui en résultent pour les personnes physiques sujettes aux traitements, (chapitre2), après avoir passé en revue les différentes variations qui permettent de positionner l'entreprise dans le processus de traitement des données, de sorte à définir les contours de sa responsabilité en la matière (Chapitre1).

## **Chapitre 1 : La place de l'entreprise dans la protection des données personnelles des personnes physiques**

La promulgation de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement de leurs données personnelles est intervenue dans un contexte international de renforcement légal de la protection des données personnelles<sup>2</sup>, avec l'entrée en vigueur, moins d'un mois auparavant, du Règlement Général sur la Protection des Données (RGPD)<sup>3</sup> qui s'adresse particulièrement aux entreprises publiques et privées et associations de l'Union Européenne. La loi 18-07 avait corroboré par ailleurs l'article 46 de la Constitution algérienne, devenu article 47 dans sa dernière révision, lequel garantit la protection juridique de la vie privée du citoyen et consacre la protection des personnes physiques dans le traitement des données à caractère personnel, en tant que droit fondamental dont la violation serait punie par la loi<sup>4</sup>.

La loi sur la protection des données personnelles interpelle d'ailleurs toutes les institutions amenées à collecter des données sur les personnes physiques et fixe les règles de protection de ces personnes dans le traitement de leurs données personnelles. Mais le danger que représente le traitement des données personnelles des personnes physiques dans un environnement aussi impliqué que celui de l'entreprise (Section 1) donne à réfléchir à la place de celle-ci dans les opérations de traitement effectuées dans différents contextes, pour tenter de cerner toutes les

<sup>2</sup> HAFIZ Chems-eddine, HAFIZ Sohel, SILINI Madiha, « Le cadre juridique de la protection des données personnelle en Algérie », Smart News Algérie, Juillet 2018.

<http://www.lpalaw.com/admin/wp-content/uploads/2018/07/Smart-News-Alg%C3%A9rie-Juillet-2018.pdf>

<sup>3</sup> Règlement n° 2016/679, dit Règlement Général sur la Protection des Données, adopté par le parlement européen le 14/04/2016 et entré en vigueur le 25/05/2018, Publié par CNIL, le 23/05/2018, sur <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

<sup>4</sup> Article 47 de la Constitution de la République Algérienne Démocratique et Populaire, Modifiée, promulguée par Décret présidentiel n° 20-442 du 30-12-2020 relatif à la promulgation au Journal Officiel de la République algérienne démocratique et populaire, de la révision constitutionnelle adoptée par référendum du 1<sup>er</sup> novembre 2020, JORA n° 82 du 30-12-2020.

situations possibles qui nécessitent protection des personnes concernées et responsabilise l'entreprise (Section 2).

## **Section 1 : La protection des données personnelles des personnes physiques dans l'entreprise : Une nécessité argumentée**

Les données personnelles sont devenues un outil sans précédent de gestion de l'entreprise contemporaine (Sous-section 1). Aussi, le traitement des données personnelles par les entreprises affecte-t-il différemment mais certainement, toutes les personnes physiques qui interviennent dans le processus de production et de consommation, en leurs qualités de salariés, clients, ou utilisateurs (Sous-section 2)

### **Sous-section 1 : Les données personnelles, un outil au cœur de l'activité numérique**

Les données personnelles sont omniprésentes dans l'activité économique, de telle sorte que leur traitement devient un outil indispensable dans la gestion de l'entreprise. Mais l'évolution des moyens de traitement des données génère également une recrudescence des dangers qui en résultent sur la vie privée.

#### **1/ Portée des données personnelles et de leur traitement**

L'article 03 de la loi n° 18-07 définit les données personnelles comme étant toute information, quel qu'en soit le support, concernant une personne identifiée ou identifiable, dénommée «personne concernée», de façon directe ou indirecte, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale.

Les données personnelles sont donc au cœur de l'activité numérique. Produites en masse, elles atteignent des volumes extravagants en raison de la puissance des processeurs informatiques, de la capacité de stockage et de la démultiplication des sources de données à travers les capteurs (Cloud, Big Data) et les objets connectés. Cette technologie numérique prône tant l'audace que la prudence : audace pour que le numérique soit vecteur d'innovation et de progrès social et prudence pour qu'il n'assiège pas nos libertés, et vies privées<sup>5</sup>.

Le traitement des données personnelles désigne, au sens de la loi 18-07, toutes opérations effectuées à l'aide de moyens ou de procédés automatisés ou non et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la

<sup>5</sup> PERES Erice, « Protection des données personnelles, RGPD et relations de travail : une affaire trop sérieuse pour la laisser aux seules mains des employeurs », Miroir Social (Votre Réseau d'information sociale), thèmes : Dialogues social, sécurité, 04/07/2018.

<http://www.miroirsocial.com/membre/FOCadres/post/protection-des-donnees-personnelles-rgpd-et-relations-de-travail-une-affaire-trop-serieuse-pour-la-laisser-aux-seules-mains-des-employeurs-1>

diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction<sup>6</sup>.

Le développement du numérique à l'échelle mondiale pousse à se demander jusqu'à quel point l'entreprise peut-elle utiliser les données récoltées dans la gestion de son personnel et de ses clients et dans quelle mesure les données personnelles peuvent-elle, ou pas, influencer ses décisions sans que cela ne soit considéré comme une exploitation abusive de ces données. A titre d'exemple, aux Etats-Unis, les assurances ont le droit d'adapter leurs tarifs en fonction du mode de vie des individus ; une assurance peut ainsi imposer à son client une augmentation des tarifs si sa montre connectée, capable de mesurer le pouls, produit des données susceptibles de prouver une dégradation de son hygiène de vie<sup>7</sup>.

La loi 18-07, dans sa généralité, ne saurait répondre aux problématiques des limites de l'utilisation des données. Seule la pratique pourrait amener, au besoin, des solutions réglementaires et/ou jurisprudentielles à ces questions.

## **2 / L'évolution des moyens de traitement des données personnelles : un danger en recrudescence**

En s'invitant dans chaque partie ou étape de la vie des personnes, la technologie numérique a bouleversé la vie de ces dernières. Des logiciels informatiques de traitements de formulaires par voie électronique et des réseaux sociaux sur lesquels on communique volontairement, ou pas, les moindres détails de la vie quotidienne, à la voiture connectée qui sait faire des créneaux à l'application pour ouvrir ou clore les volets de chez soi à distance, en passant par les montres connectées, ces collecteurs d'informations deviennent des objets du quotidien, à tel point que les individus ne se rendent pas nécessairement compte de toutes les informations qu'ils communiquent sur leurs vies privées<sup>8</sup>.

La préoccupation autour de l'impact de la technologie sur la vie privée des personnes ne date pas d'aujourd'hui dans les pays développés. En France, le premier texte ayant encadré l'utilisation de l'informatique et son impact sur les libertés date de 1978<sup>9</sup>. Mais les évolutions technologiques à grande échelle des dernières décennies ont rendu nécessaire l'adaptation des législations déjà existantes à

<sup>6</sup> Article 03 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement de leurs données à caractère personnel, Op.cit.

<sup>7</sup> WOZNY Mallorie, Exploitation des données personnelles : raison commerciales, raison d'état et opportunités, Mémoire pour l'obtention du diplôme national de Master, Domaine : sciences humaines et sociales, Université de Lyon, aout 2017, p. 43.

<sup>8</sup> Ibid.

<sup>9</sup> LOI n° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Journal officiel du 7 janvier 1978 et rectificatif au JORF du 25 janvier 1978, Modifiée et complétée.

l'aggravation des risques sur la vie privée, sinon l'instauration d'un dispositif de protection dans les États qui n'en ont pas encore, à l'image de l'Algérie.

En effet, si, durant les années 1990, internet n'était encore qu'à ses débuts, aujourd'hui, la protection des données à l'échelle mondiale doit s'envisager en incluant l'avènement de l'intelligence artificielle, la puissance du Big Data, l'industrie dite « 4.0 », la robotique, la domotique...etc.

Si nous prenons par exemple le Big Data, qui désigne un important volume de données rassemblées sur les comportements de consommation, les données médicales, la communication des internautes... cette capture des données faite souvent à leur insu, bien qu'elle soit profitable à plusieurs aspects de la vie contemporaine, tels que l'industrie, la médecine, le marketing...etc et bien que sa pertinence ait été prouvée dans la recherche médicale contre le cancer et dans la lutte contre la criminalité, il n'en demeure pas moins que la collecte massive, la conservation et l'usage de ces données sont mal perçus et sont considérés comme une atteinte dissimulée à la vie privée des internautes<sup>10</sup>.

Il faut donc que le citoyen, quel que soit son rapport avec l'entreprise, ou la qualité de celle-ci, soit correctement informé de ce que l'utilisation des réseaux sociaux, des Cloud, de la géolocalisation... implique en matière de collecte et d'exploitation de ses données personnelles, et qu'il soit instruit de façon à réagir de manière intelligente face au Big Data, et autres moyens de collecte de données.

## **Sous- Section 2 : Des différents profils de personnes sujettes au traitement des données personnelles par l'entreprise (salariés, clients utilisateurs)**

Pour tenter de cerner l'implication de l'entreprise dans le traitement des données personnelles, et la responsabilité qui en résulte, il faut d'abord s'arrêter sur les différents profils des personnes physiques qui interagissent avec l'entreprise, en leur qualité de salariés, de clients ou d'utilisateurs, car l'impact et l'étendue du traitement de leurs données personnelles dépendent souvent de leur rapport avec l'entreprise.

### **1/ Le traitement des données personnelles des clients**

Le client, par définition, est une personne qui achète ou requiert des biens ou des services, de façon occasionnelle ou habituelle, à un fournisseur, moyennant une rétribution. Le client confie donc ses intérêts à l'entreprise en contrepartie d'un paiement.

L'entreprise gère une multitude de fichiers clients et prospects. Il peut sembler que l'entreprise n'ait aucun droit sur les données personnelles de ses clients, mais

---

<sup>10</sup>Le Big Data, c'est quoi?, Digital Guide IONOS, Mis en ligne le 20/03/2019, consulté le 10/04/2020

<https://www.ionos.fr/digitalguide/web-marketing/analyse-web/le-big-data-cest-quoi/>

dans la gestion contemporaine des relations commerciales, ancrée par l'utilisation massive de la technologie numérique, l'entreprise est de plus en plus à la quête de données lui permettant de cerner les besoins de la clientèle, et il est nécessaire de protéger la vie privée du client dans le traitement de ses données personnelles.

Le RGPD ordonne aux entreprises d'informer ses clients et prospects des conditions dans lesquelles leurs données seraient traitées, ainsi que de leurs droits. Il leur préconise également de ne collecter et ne traiter que les informations nécessaires à la relation commerciale, tout en prévoyant des mesures de sécurité adaptées aux risques encourus. Les fichiers de ces opérations doivent par ailleurs être inscrits dans un registre des activités de traitements des données tenu par l'entreprise<sup>11</sup>.

En droit algérien, le traitement des données personnelles des clients doit être conforme à la loi n° 18-07 dans sa généralité, sans qu'il soit prévu des dispositions particulières pour les clients. La difficulté, à l'état actuel des choses où la pratique est encore novice, est de savoir distinguer les données nécessaires à la relation commerciale de celles qui ne le sont pas.

## 2/ Les utilisateurs / consommateurs

Il peut être difficile de distinguer entre les utilisateurs, les consommateurs et les clients, notamment lorsque l'entreprise responsable du traitement est une plateforme intelligente ou un réseau social, ou tout simplement une entreprise du Web, comme les GAFAM<sup>12</sup>. En réalité, les utilisateurs sont considérés comme des consommateurs du web. Mais ils sont aussi le produit de vente des GAFAM à leurs clients potentiels, à travers le ciblage publicitaire, sans que lesdits utilisateurs n'en soient vraiment conscients, ce qui rend d'autant plus accrue la nécessité de protéger leurs données personnelles.

On sait d'ailleurs que la récolte des données par les réseaux sociaux, comme Facebook, se fait à l'aide de procédés très sophistiqués et extrêmement intrusifs et que les données finissent toujours dans les serveurs implantés dans les quatre coins du monde, au service des géants du web et leurs clients, sans que les utilisateurs n'en soient au courant<sup>13</sup>.

Les GAFAM nous fournissent des services que l'on croit gratuits, alors qu'en vérité, la contrepartie réside dans la multitude de données auxquelles nous permettons le libre accès au profit de ces entreprises du Web qui les récoltent et les utilisent à des fins commerciales. Le ciblage publicitaire pratiqué sur nos données permet aux

<sup>11</sup> Voir Rapport CNIL, Gestion des clients et prospects, que faire ?

<https://www.cnil.fr/fr/cnil-direct/question/gestion-des-clients-et-prospects-que-faire>

<sup>12</sup> Est désigné par GAFAM, les cinq géants du Web : Google, Apple, Facebook, Amazon et Microsoft.

<sup>13</sup> GOUASMI Yahia, « Un réseau très social, Facebook vend nos données personnelles », Chronique PAS, mis en ligne le 07/03/2018, consulté le 10/04/2020. <https://www.partiantisioniste.com/articles/un-reseau-tres-social-facebook-vend-nos-informations-personnelles.html>



rédacteurs du web de faire valoir leurs marchandises et aux entreprises de trouver des clients potentiels.

Les internautes et utilisateurs de réseaux sociaux doivent prendre conscience de l'importance de se protéger et réfléchir aux renseignements qu'ils postent sur internet, en évitant de lier son nom à des renseignements personnels, et en agissant de manière consciente et responsable. Mais ceci n'est pas toujours évident, d'où le rôle important que peut jouer la loi pour encadrer l'activité intrusive de récolte de données par ces entreprises et en protéger les utilisateurs.

### **3/ Les salariés**

Dans les entreprises, la question de traitement des données des salariés est d'autant plus sensible que ces derniers sont sous la subordination de l'employeur, ce qui confère à l'employeur le droit d'exercer un pouvoir de contrôle continu sur ses salariés, et dont les limites ne sont pas clairement délimitées, encore moins à l'ère de la récolte numérique des données personnelles et de leur traitement automatisé.

La relation employeur-salarié est d'ailleurs plus propice à la collecte et à l'exploitation des données personnelles qu'une relation entreprise-client. Constante et régulière, la collecte des données des salariés débute dès la période de l'embauche et se poursuit tout au long de sa carrière<sup>14</sup>.

L'entreprise est amenée à récolter et à manipuler quotidiennement les données personnelles des salariés, ce qui constitue un risque permanent sur leur vie privée, d'où la primordialité de définir les contours de ce qui est permis à l'entreprise, au nom de la subordination, et de ce qui ne l'est pas, au nom du respect de la vie privée. La loi sur la protection des données personnelles est susceptible de garantir une protection suffisante aux salariés contre toute utilisation abusive de leurs données personnelles par l'entreprise qui les emploie. Encore faut-il qu'elle soit adaptée à chaque situation et appliquée à bon escient.

## **Section 2 : Comprendre l'emplacement de l'entreprise dans les opérations de traitement des données personnelles**

Si les profils de personnes physiques qui peuvent faire l'objet de traitement des données personnelles dans le cadre de l'entreprise sont multiples, celle-ci se situe différemment dans les opérations de traitement dont elle peut être la première responsable, mais aussi, la sous-traitante ou la destinataire. Afin de cerner l'emplacement de l'entreprise dans les opérations de traitement des données personnelles des personnes physiques (Sous-section2), il convient en premier lieu de définir les principaux acteurs qui interviennent dans ces opérations (Sous-section 1).

---

<sup>14</sup>FISCHER Servane, KERVADEC Ronan; « L'impact du RGPD sur la gestion des données personnelles des salariés », Les Cahiers Lamy du CE, n° 178, 1<sup>er</sup> mars 2018, p. 1/11.

## **Sous-section 1 : les acteurs principaux des opérations de traitement des données personnelles**

La loi n° 18-07 distingue les différents acteurs qui interviennent dans les opérations de traitement des données personnelles. Il s'agit du responsable du traitement, du sous-traitant et du destinataire. Ce sont donc les rôles que peuvent endosser les entreprises dans les opérations de traitement des données.

### **1/ Le responsable du traitement**

Le responsable du traitement est la personne physique ou morale, publique ou privée, ou toute autre entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens de traitement des données<sup>15</sup>. Aussi, lorsque l'entreprise est responsable du traitement, elle se voit incombent toutes les obligations du respect de la vie privée, au titre du RGPD dans la communauté européenne, et de la loi n° 18-07 en Algérie.

Il faut aussi préciser que les employés traitant des données à caractère personnel au sein des entreprises responsables de traitement, agissent pour exécuter les ordres de celles-ci en tant que responsables de traitement. Il est de ce fait possible qu'une personne physique soit salariée dans une entreprise, et exécute en même temps les tâches qui incombent au responsable du traitement.

Par ailleurs, la loi n° 18-07, tout comme le RGPD, dans sa définition du responsable du traitement, consacre l'hypothèse que ce responsable puisse aussi être une personne physique. Or, dans la pratique, du moins celle des entreprises soumises au RGPD, les entreprises ayant pour vocation de soustraire des résultats à partir de la collecte et de la manipulation des données, désignent un ou plusieurs responsables de traitement qui endossent de ce fait toutes les obligations légiférées dans le cadre de la protection des personnes physiques dans le traitement de leur données personnelles.

La question majeure qui se pose dans ces différents cas de figure est de savoir qui endosse la responsabilité en cas de dépassement.

Il faut bien faire attention à ne pas confondre ici le salarié d'une entreprise (personne morale) responsable du traitement des données, et la personne physique responsable du traitement de donnée au sein d'une entreprise. Ainsi, les salariés dont la mission est de traiter des données au nom et pour le compte d'une personne morale, identifiée « responsable du traitement », n'endossent de responsabilité que dans le cadre de l'exécution de leur contrat de travail. Il appartient ici au chef d'entreprise de tracer avec clarté les tâches qu'il délègue à ses salariés tout en veillant au respect des obligations qui lui incombent dans le cadre de la loi relative à la protection des données, si bien qu'en cas de dépassement, il incombe à l'entreprise d'en assumer la totale responsabilité.

<sup>15</sup> Article 03 de la loi 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Op.cit.

À l'image de ces personnes morales spécialisées dans le traitement des données, nous pouvons citer en exemple la société IPSOS en France qui est une entreprise de sondage français et une société internationale de marketing d'opinion, créée en 1975. Ipsos a été le prestataire attitré de la présidence de la République Française entre 1981 et 2007, mais son expansion tant au niveau matériel que géographique en fait l'un des meilleurs fournisseurs de données pour différents organismes publics ou privées telles que la banque postale en France, Research partner en Norvège ou punto vista au Chili...etc<sup>16</sup>. Ipsos est donc responsable du traitement des données personnelles pour ces organismes et doit être en conformité avec le RGPD dans tous les sondages qu'elle effectue, quelles qu'en soient la finalité.

Mais lorsqu'il s'agit d'une personne physique désigné en tant que responsable du traitement par une entreprise ou un établissement, cette personne, qu'elle soit salariée ou missionnée, endosse la responsabilité qui incombe au responsable du traitement dans la limite de son contrat ou sa mission. Dès lors que ce traitement est exercé par une personne, physique ou morale, pour le compte d'une entreprise qui a déjà la qualité de responsable du traitement, on bascule dans la sous-traitance, et l'étendue de la responsabilité du sous-traitant est définie par le contrat de sous-traitance, étant précisé qu'elle peut se confondre avec celle du responsable du traitement original.

Par exemple, il peut arriver qu'une entreprise comme IPSOS confie la mission de traitement des données particulières à un sous-traitant, tandis qu'elle confie d'autres tâches de traitement à des salariés, en gardant dans tous les cas la qualité de responsable du traitement. En revanche, une entreprise qui ne travaille pas dans le traitement des données personnelles, peut confier le traitement des données personnelles de ses salariés à un tiers qui en endossera la responsabilité totale en sa qualité de responsable du traitement.

## 2/Le sous-traitant

L'article 03 de la loi 18-07 définit le sous-traitant en matière de traitement des données comme étant toute personne physique ou morale, publique ou privée ou toute autre entité qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le sous-traitant traite les données à caractère personnel uniquement pour le compte du responsable du traitement. C'est généralement un tiers extérieur à l'entreprise. Toutefois, dans le cas des groupes d'entreprises, une des entreprises peut être le sous-traitant d'une autre entreprise.

La loi n°18-07 ne le précise pas de manière explicite, mais conformément aux règles générales de la sous-traitance, les obligations du sous-traitant envers le responsable du traitement, considéré comme donneur d'ordre, doivent être précisés

---

<sup>16</sup> Ipsos, Wikipédia, L'encyclopédie libre. <https://fr.wikipedia.org/wiki/Ipsos>

dans un contrat type de sous-traitance, tel qu'il est stipulé par la loi d'orientation sur le développement de la PME, promulguée en 2017<sup>17</sup>.

Il est donc attendu que l'Agence de développement de la PME et de la promotion de l'innovation (ADPIPME), instituée par la loi n° 17-02 et organisée par le décret exécutif n°18-170<sup>18</sup>, qu'elle élabore un ou des contrats type de sous-traitance dans la filière de traitement des données personnelles pour définir les droits et les obligations des responsables de traitement en tant que donneurs d'ordres, et des sous-traitants en tant que receveurs d'ordres<sup>19</sup>.

En tout état de cause, Le contrat entre le responsable du traitement et le sous-traitant doit déterminer l'objet et la durée du traitement, sa nature et sa finalité, le type des données à traiter et les catégories des personnes concernées. Il doit aussi préciser le sort des données personnelles traitées, quand le contrat prend fin. Le sous-traitant doit s'en tenir au contrat ; il ne doit traiter les données auxquelles il a accès que sur instruction documentée du responsable du traitement et il est préférable qu'il ne s'en écarte pas, au risque d'engager sa responsabilité<sup>20</sup>.

Par ailleurs, aux termes du RGPD, le sous-traitant des données ne peut recruter un autre sous-traitant ou nommer un sous-traitant conjoint pour effectuer une partie de sa mission que lorsqu'il a reçu au préalable du responsable du traitement une autorisation écrite, qui peut être spécifique ou générale<sup>21</sup>.

Naturellement, il semble que le sous-traitant n'a pas toutes les obligations du responsable du traitement. Le contrat doit encadrer la réalisation du traitement mais c'est le responsable du traitement initial qui reste le premier à mettre sa crédibilité en jeu. Les choses ne sont pourtant pas si simples. En effet, l'étendue des attributions du sous-traitant n'étant pas délimitée, la confusion entre le responsable du traitement et le sous-traitant n'est pas à écarter. La solution donnée par la doctrine Française

<sup>17</sup> Voir les articles 30 et 31 de la Loi n° 17-02 du 10 janvier 2017 portant loi d'orientation sur le développement de la petite et moyenne entreprise (PME), JORA n° 02 du 11-10-2017.

<sup>18</sup> L'ADPIPME, dénommée « agence » dans la loi n° 17-02 qui l'avait instituée, est régie par le décret exécutif n° 18-170 du 26-06-2018 fixant les missions, l'organisation et le fonctionnement de l'agence de développement de la PME et de la promotion de l'innovation, JORA n° 39 du 04-07-2018.

<sup>19</sup> Voir l'article 31 de la Loi n° 17-02 portant loi d'orientation sur le développement de la PME, Op.cit., et l'article 05 du Décret exécutif n° 18-170 fixant les missions, l'organisation et le fonctionnement de l'ADPIPME, Op.cit.

<sup>20</sup>-DUPRE Jérôme, « RGPD et sous-traitance : des questions et leurs réponses », Village de La Justice : la communauté des métiers et du droit, Actualité juridique, paru le 29-08-2017.

<https://www.village-justice.com/articles/rgpd-sous-traitance-des-questions-leurs-reponses,25724.html>

-Voir aussi : GUILLEMAIN Maïté, « La sous-traitance en droit des données personnelles », Revue Lamy Droit de l'Immatériel, n° 152, 1<sup>er</sup> octobre 2018, p. 1/6.

<sup>21</sup> RGPD- Guide du sous-traitant, CNIL, p. 10.

[https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide\\_sous-traitant-cnil.pdf](https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf)

consiste à considérer le sous-traitant, de fait, comme un responsable du traitement si, aux termes de son contrat, il détermine lui-même les finalités et les moyens du traitement dont il assure la sous-traitance<sup>22</sup>.

### **3/ Le destinataire**

Selon l'article 03 de la loi 18-07, est destinataire du traitement de données, toutes personnes physique ou morale, autorité publique, service ou toute entité qui reçoit communication des données personnelles.

Lorsqu'il s'agit de collecter et de manipuler les données personnelles des employés, l'entreprise le fait généralement pour son propre compte, dans le but de gérer son fonctionnement. Elle est donc celle qui soustrait l'information dont elle a besoin à partir des données récoltées. L'entreprise peut être de ce fait responsable du traitement et destinataire des données des salariés qu'elle emploie. Par contre, dans l'exemple de IPSOS, les destinataires des données sont les clients demandeurs des sondages, comme la Banque Postale, le Ministère du travail ...etc.

### **Sous-section 2 : Positionnement des entreprises dans les opérations de traitement des données personnelles**

Nous l'avons compris, dans chaque opération de traitement de données personnelles, il y a toujours une entreprise responsable du traitement, mais qui n'exerce pas forcément ce rôle de façon directe et intégrale. Aussi, sa responsabilité dépend-elle de son degré d'implication, et de l'étendue des tâches qu'elle confie à autrui.

En tout état de cause, Selon qu'elle soit entreprise du web ou entreprise classique, et selon qu'elle traite avec les utilisateurs, les clients ou les salariés, l'entreprise endosse des responsabilités relativement différentes, mais qui ont le point commun de découler de son statut de responsable du traitement.

### **1/Les entreprises du web et le traitement des données personnelles des utilisateurs**

Les entreprises de la GAFA, (Google, Amazon, Facebook et Apple), devenues GAFAM avec l'introduction de Microsoft, et qui forment les géants du Web sont en même temps les plus gros traiteurs de données personnelles, qu'ils manipulent depuis leur création. La technologie numérique, et plus précisément, la pratique de la collecte et de l'exploitation des données des utilisateurs, étant au cœur des investissements des GAFAM, ils sont naturellement responsables du traitement des données à caractère personnelle des milliers d'utilisateurs. Il en est de même pour toutes les entreprises dont l'activité principale est centrée sur la collecte et l'exploitation des données pour son propre compte, ou pour le compte d'autrui.

<sup>22</sup> DUPRE Jérôme, « RGPD et sous-traitance : des questions et leurs réponses », Op.cit.

Et alors que l'utilisation du Web est déontologiquement et réglementairement soumise aux règles de la confidentialité, Facebook, à titre d'exemple, exhibe et partage les opinions des utilisateurs, leurs lieux de vie, leurs contenus multimédia, afin qu'ils soient accessibles à un maximum de personnes. Ne se souciant aucunement de la confidentialité, il cherche au contraire à ce que ses contenus soient relayés à la plus grande échelle possible, afin d'impacter durablement et positivement sa réputation<sup>23</sup>. Il va de soi que les utilisateurs acceptent cette diffusion à grande échelle de leurs données personnelles, et la vie privée perd bien des repères devant les nouveaux besoins sociétaux du monde connecté. Ce qu'ils ignorent ou acquiescent inconsciemment c'est l'exploitation excessive qui en est faite derrière les écrans.

Les sociétés GAFAM, ou celle des réseaux sociaux tels que Instagram, Twitter ou LinkedIn peuvent être en même temps responsables des opérations de traitement et destinataires des données personnelles des utilisateurs. Ce qui n'est pas divulgué, c'est que les données personnelles sont récoltées et stockées dans des serveurs insaisissables et utilisées à des fins commerciales, d'où toute la difficulté de les responsabiliser pour les innombrables récoltes frauduleuses et/ou exploitations abusives des données, malgré les efforts continuels de la cybercriminalité qui a quand-même valu plusieurs actions à l'encontre des géants du web dans des affaires de vols de données, comme le scandale Facebook Cambridge Analytica en 2018<sup>24</sup>.

## **2/L'entreprise responsable du traitement des données personnelles des salariés**

L'entreprise, représentée par l'employeur, est amenée à traiter, au quotidien, de nombreuses données à caractère personnel à l'occasion de la gestion de son personnel, telles que les coordonnées bancaires, les numéros de sécurité sociale, les déclarations sociales obligatoires... en tenant des registres du personnel et annuaires pouvant même comporter des photographies des salariés. Ainsi, toute entreprise employant des salariés est considérée comme responsable du traitement des données personnelles de ses salariés<sup>25</sup> dès lors qu'elle en détermine tant la finalité que les moyens employés, au sens de l'article 03 de la loi n° 18-07, lequel, non seulement

<sup>23</sup> WOZNY Mallorie, Exploitation des données personnelles : raison commerciales, raison d'état et opportunités, Op.cit., p. 08.

<sup>24</sup> En mars 2018, le réseau social Facebook a fait face à un scandale concernant la gestion des données de ses utilisateurs. [La société britannique Cambridge Analytica a collecté les données de plus de 50 millions d'utilisateurs](#), sans autorisation, afin de bâtir un programme informatique permettant de prédire et d'influencer le choix des électeurs américains. Voir : Fuites des données : Cinq grands scandales des dernières années, Radio Canada, publié le 21/06/2019.

<https://ici.radio-canada.ca/nouvelle/1193991/scandale-fuite-vol-renseignements-personnel>

<sup>25</sup> DESTAILLATS Emmanuelle, « Employeurs : Quelles sont vos nouvelles obligations de traitements de données depuis l'entrée en vigueur du règlement européen RGPD ? », Village de la Justice, Actualités Juridiques Droit Social, TIC et Droit du travail, article paru le 06/06/2018.

<https://www.village-justice.com/articles/employeurs-compter-mai-2018-entree-vigueur-reglement-europeen-rgpd-vos,28653.html>

définit le responsable du traitement, mais aussi les opérations de traitement des données.

Les entreprises employant des salariés se trouvent ainsi dans l'obligation de se mettre en conformité avec la loi n° 18-07 dans le traitement des données personnelles de ces derniers. Mais ces obligations peuvent néanmoins être mitigées par le lien de subordination qui lie les salariés à leurs employeurs.

### **3/ L'entreprise responsable du traitement des données des clients**

Lorsque l'entreprise traite les données de ses clients, elle se voit incomber toutes les obligations du responsable du traitement, sans restrictions ou conditions particulières, autres que celles qui se rapportent à la nature des données récoltées, selon qu'elles soient sensibles ou ordinaires. Différemment des utilisateurs du Web, les clients sont clairement informés du traitement de leurs données personnelles et différemment des salariés, leur consentement doit être obligatoirement recueilli.

Bien évidemment, comme détaillé plus haut, l'entreprise peut aussi être seulement sous-traitante des données personnelles, ou destinataire de ces données. Mais sa responsabilité n'est entièrement engagée que lorsqu'elle agit en qualité de responsable du traitement sans en déléguer l'exercice à une tierce personne, physique ou morale, d'où l'importance de mettre la lumière sur les conditions applicables sur le traitement des données personnelles dans l'entreprise, en tant que responsable du traitement.

## **Chapitre 2 : Les conditions applicables sur le traitement des données personnelles des personnes physiques dans l'entreprise**

La loi 18-07, à l'image du RGPD, consacre une nouvelle responsabilisation des entreprises sur le traitement des données personnelles de leurs clients, consommateurs /utilisateurs et salariés. De nouvelles obligations s'imposent ainsi aux entreprises, afin de garantir que le traitement des données ne porte pas atteinte à la vie privée, aux droits et libertés fondamentales des personnes concernées (Section 1). Et pour les mêmes raisons, des droits sont conférés à ces personnes de sorte qu'ils prennent conscience de l'enjeu de ces traitements et qu'ils puissent se protéger contre toute utilisation abusive de leurs données personnelles (section 2). Il va de soi que le degré de responsabilisation des entreprises et l'étendue des droits des personnes concernées par le traitement des données personnelles varient en fonction tant de la qualité de la personne concernée que de l'emplacement de l'entreprise dans les opérations de traitement de données effectuées.

## **Section 1 : Des obligations de l'entreprise dans le traitement des données personnelles des personnes physiques**

La loi n° 18-07, à l'image du RGPD, détermine les obligations de toute personne, physique ou morale, qui procède, en tant que responsable du traitement, à la collecte et à l'exploitation des données personnelles des personnes physiques. L'entreprise se voit alors incomber ces obligations dès lors qu'elle prend la qualité de responsable du traitement. Mais l'étendue et l'applicabilité de ces obligations peuvent diverger selon la qualité de la personne physique, sujette au traitement de ses données personnelles, vis-à-vis de l'entreprise.

### **Sous section 1 : De l'obligation du recueil du consentement**

Il est naturel d'exiger le recueil du consentement explicite de toute personne physique pour le traitement de ses données personnelles, mais pour certaines catégories de personnes, cette condition est confrontée à d'autres considérations plus vitales que le respect de la vie privée. Aussi, le recueil du consentement est-il problématique pour les salariés de l'entreprise.

#### **1/ Portée de la condition du consentement**

La loi n° 18-07, dans son article 07 précise que le traitement des données à caractère personnel ne peut être effectué qu'avec le consentement explicite de la personne concernée, laquelle, peut à tout moment se rétracter.

La manière avec laquelle le consentement est récolté n'est cependant pas toujours des plus authentique, notamment lorsqu'il s'agit des entreprises du web. En effet, lorsqu'une page web vous empêche d'accéder à un document en vous suggérant d'abord d'accepter les cookies, qui sont des traceurs de données, et que vous cliquez sur « accepter », votre consentement sur le traçage de vos données est considéré comme recueilli, alors qu'en réalité, vous n'avez fait que vous débarrasser d'une page-annonce qui vous empêche de lire votre article.

Il faut savoir que si ces questions sont encore assez vagues pour les utilisateurs non avertis, les législations de la protection des données personnelles dans les pays d'implantation des géants du Web, considèrent bel et bien les cookies comme une récolte de données qui suscite le recueil du consentement. Selon une directive Européenne, dite « paquet télécom », les internautes doivent être informés et donner leur consentement préalablement à l'insertion de traceurs. Ils doivent disposer d'une possibilité de choisir de ne pas être tracés lorsqu'ils visitent un site ou utilisent une application. Les éditeurs ont donc l'obligation de solliciter au préalable le consentement des utilisateurs, et ce consentement est valable pour une durée ne



dépassant pas 13 mois. Certains traceurs sont cependant dispensés du recueil de ce consentement<sup>26</sup>.

La question est de savoir quel est le degré de conscience des utilisateurs, surtout dans un pays comme le nôtre, où la loi est encore récente et imparfaite, et où une grande partie des internautes sont encore novices sur les enjeux de l'utilisation des données et ce qu'implique le traçage de leur navigation sur internet. Il convient d'ailleurs de noter qu'en communiquant nos données personnelles sur les réseaux sociaux, comme Facebook, nous consentons à les afficher, mais pas forcément à leur utilisation. Pourtant, sans recueil de consentement clair et plausible, nos données sont souvent utilisées à des fins commerciales, parfois en violation de la loi, parfois dans le respect de celle-ci, mais en recourant à des moyens frauduleux de recueils de consentements d'utilisateurs non suffisamment avertis.

La règle qui consiste à recueillir le consentement de la personne sujette à un traitement de données personnelles, compte cependant plusieurs exceptions ayant trait à des considérations plus vitales que la protection de la vie privée<sup>27</sup>. Par exemple, ledit consentement n'est pas exigé lorsque le traitement des données est nécessaire à la sauvegarde de la vie de la personne concernée ou à la sauvegarde de ses intérêts vitaux si elle est physiquement ou juridiquement dans l'incapacité de donner son consentement. Le consentement n'est pas non plus demandé lorsque le traitement des données est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou encore à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de l'intérêt et/ou des droits et libertés fondamentales de la personne concernée<sup>28</sup>.

D'autres exceptions interpellent les obligations professionnelles ou contractuelles de la personne concernée, ou les obligations légales du responsable du

---

<sup>26</sup> -Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs. Journal Officiel de l'Union Européenne du 18-12-2009, L.137, pp. 11-36.

- Voir aussi : Cookies et traceurs, que dit la loi ?, CNIL, 01/10/2020.

Consulté sur : <https://www.cnil.fr/fr/cookies-et-traceurs-que-dit-la-loi>

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:fr:PDF>

<sup>27</sup> YACOUB Zina, La protection des données personnelles, Actualité Juridique Internationale – Algérie-, Revue de Droit Comparé du Travail et de la Sécurité Sociale, 2018, n° 03, Comptrasec, CNRS, Université de Bordeaux, p.128.

<sup>28</sup> Art. 07 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Op.cit.

traitement, et de là découle l'applicabilité problématique de cette condition sur les salariés.

## **2/ L'applicabilité problématique de la condition du consentement sur les salariés**

L'employeur étant considéré comme un responsable du traitement des données personnelles de ses salariés, il serait légitime de croire que le consentement des salariés doit être recueilli avant toute opération de traitement de leurs données personnelles. Pourtant, dans la foulée des exceptions posées par l'article 07 à la condition du consentement, on retient que le recueil du consentement de la personne concernée n'est pas nécessaire :

- Lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ;
- Lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle est soumise ladite personne ou le responsable du traitement ;
- Lorsque le traitement est nécessaire aux fins de réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

Dans le cadre de l'exécution d'un contrat de travail, le consentement du salarié n'est donc pas nécessaire pour les traitements courants de ses données personnelles tels que la gestion de la paie, les déclarations sociales ainsi que les dispositifs de contrôle de l'activité des salariés.

La loi ne le stipule pas clairement, mais certains traitements de données nécessitent en revanche le consentement du salarié, lorsqu'il n'est pas susceptible de correspondre à l'une des hypothèses d'exception prévues par la loi. Par exemple, l'utilisation d'une photographie d'un salarié à des fins publicitaires ou promotionnelles n'est, sauf stipulation contraire relative au contenu même du contrat, ni nécessaire à la préservation des intérêts légitimes de l'entreprise, ni à l'exécution du contrat de travail<sup>29</sup>.

La même question se pose au sujet des données sensibles, définies par la loi n° 18-07 comme étant des données qui révèlent l'origine ethnique ou raciale de la personne, ses convictions religieuses, ses opinions politiques, son appartenance syndicale, sa santé ou ses données génétiques. Certaines de ces données ne devant pas faire partie des données nécessaires à l'exécution du contrat de travail, elles ne devraient pas dispenser l'employeur du recueil du consentement. D'autres, au

---

<sup>29</sup> DESTAILLATS Emmanuelle, « Les nouvelles obligations de l'employeur en matière de protection des données personnelles des salariés », Village de la Justice- La communauté des métiers du droit, Edition électronique Legi Team, 13 juin 2018.

<https://www.village-justice.com/articles/les-nouvelles-obligations-employeur-matiere-protection-des-donnees-personnelles,28756.html>

contraire, tout en étant des données sensibles exigeant un traitement particulier pour les autres, elles sont des données utiles dans le cadre de la relation de travail, comme celle concernant l'état de santé ou l'appartenance syndicale.

En tout état de cause, devant l'imprécision de la loi et l'absence de textes réglementaires, ou de solutions jurisprudentielles, il est bien difficile de savoir comment trouver la juste mesure entre ce qui est considéré comme des données nécessaires à l'exécution du contrat de travail et les autres données dont le traitement devrait être soumis au consentement du salarié<sup>30</sup>, ou encore, les données suscitant un traitement particulier, pour les salariés de l'entreprise comme pour les autres.

## **Sous-section 2 : De l'obligation d'information des personnes du traitement des données personnelles**

Conformément à l'article 32 de la loi n° 18-07, toute personne sollicitée en vue d'une collecte de ses données personnelles doit en être préalablement informée, de manière expresse et non équivoque, par le responsable du traitement ou son représentant, de l'identité du responsable du traitement et, le cas échéant, de son représentant, des finalités du traitement et de toutes informations supplémentaires utiles notamment le destinataire, l'obligation de répondre et ses conséquences ainsi que ses droits et le transfert des données à l'étranger.

Aussi, lorsque les données personnelles n'ont pas été collectées auprès de la personne concernée, l'entreprise responsable du traitement ou son représentant doit, avant l'enregistrement des données ou leur communication à un tiers, fournir à la personne concernée les informations déjà citées. En cas de collecte de données, en réseaux ouverts, la personne concernée doit être informée, sauf si elle sait déjà que les données à caractère personnel la concernant peuvent circuler sur les réseaux sans garanties de sécurité et qu'elles risquent d'être lues et utilisées par des tiers non autorisés<sup>31</sup>.

S'agissant des salariés de l'entreprise, les exceptions à l'obligation d'obtenir leur consentement n'exempte pas le responsable du traitement de l'obligation de l'informer. Ainsi, l'entreprise a l'obligation d'informer ses salariés, au même titre que ses clients, de l'existence d'un traitement de données et des données qu'il contient, la finalité de ce traitement et toute autre information supplémentaire utile à une prise de connaissance complète et sans équivoque de toute l'opération du traitement des données<sup>32</sup>.

La loi 18-07 ne cite cependant pas le fondement légal du traitement des données dans la nomenclature des éléments dont il est nécessaire d'informer la personne

<sup>30</sup> YACOUB Zina, traitement des données personnelles, Op.cit., p. 130.

<sup>31</sup> Art. 32 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Op.cit.

<sup>32</sup> YACOUB Zina, Traitement des données personnelles, Op.cit., P. 129.

concernée. Cette information est pourtant nécessaire en l'absence du consentement. Par exemple, l'entreprise devrait être tenue d'indiquer à ses salariés sur quel fondement légal elle traite leurs données lorsque ce traitement n'a pas été soumis à leur consentement.

L'information de la personne concernée devra en outre porter sur les droits dont elle dispose. L'entreprise responsable du traitement doit informer la personne concernée qu'elle dispose du droit d'accès à ses données, du droit de les rectifier lorsque cela est nécessaire et du droit de s'opposer au traitement pour des motifs légitimes.

### **Sous-section 3 : L'obligation de la déclaration auprès de l'autorité nationale et l'éventuelle autorisation de celle ci**

Afin d'asseoir une stratégie de contrôle du respect de la loi dans le traitement des données personnelles, la loi n° 18-07 a annoncé la création, auprès du président de la République, d'une autorité administrative indépendante de protection des données à caractère personnel, dotée de la personnalité morale et de l'autonomie financière et administrative, et dont le siège est fixé à Alger<sup>33</sup>. En attendant son installation et sa nomination, ladite autorité est désignée sous le nom d' « autorité nationale ».

Cette autorité administrative indépendante est chargée de veiller à ce que le traitement des données à caractère personnel soit mis en œuvre dans le respect de la loi. A ce titre, elle est habilitée à recevoir les déclarations relatives au traitement des données personnelles et à délivrer les autorisations quand elle les juge nécessaires<sup>34</sup>.

#### **1/ La déclaration**

L'entreprise qui procède à un traitement des données personnelles doit déposer une déclaration préalable auprès de l'autorité nationale. Cette déclaration comprend l'engagement que le traitement sera effectué dans le respect des dispositions de la loi. Un récépissé de dépôt est remis à l'entreprise ou lui est transmis par voie électronique au plus tard dans les 48 heures qui suivent<sup>35</sup>.

La déclaration de traitement des données personnelles doit comporter un certain nombre d'éléments dont la teneur dépend de la nature des données à traiter et de l'impact dudit traitement sur la vie privée. Nous pouvons ainsi distinguer la déclaration intégrale de la déclaration simplifiée, même si les cas qui en font la différence ne sont pas encore fixés.

<sup>33</sup> Art. 22 de la loi n° 18-07 relative à la protection des personnes physiques..., Op.cit.

<sup>34</sup> Art. 25, Ibid.

<sup>35</sup> Art. 13 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Op.cit.

En effet, au sens de l'article 14 de la loi n° 18-07, la déclaration intégrale doit comprendre :

- Des informations sur le responsable du traitement ou son représentant, tels que : son nom, son adresse;
- Une description relative à l'opération de traitement, telle que : la nature, les caractéristiques et la ou les finalités du traitement envisagé, les moyens d'assurer la confidentialité et la sécurité du traitement, les interconnexions entre les données, les modalités de leur cessions...
- Une description de la ou des catégories de personnes concernées et des données ou des catégories de données à caractère personnel s'y rapportant, la durée de la conservation des données, la nature des données dont le transfert à l'étranger est envisagé
  - Les destinataires, ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;
  - Le service auprès duquel la personne concernée pourra exercer, le cas échéant, les droits qui lui sont reconnus par les dispositions de la présente loi, ainsi que les mesures prises pour faciliter l'exercice de ceux-ci.

La déclaration simplifiée quant à elle ne comprend pas l'intégralité de ces éléments, et se contente de fournir les informations relatives au responsable du traitement et au destinataire, une description précise des personnes sujettes au traitement, des données à traiter, et de l'opération de traitement.

La déclaration simplifiée intervient généralement lorsqu'il s'agit de données à caractère personnel qui ne sont pas susceptibles de porter atteintes aux droits et libertés des personnes concernées et à leur vie privée. C'est pourquoi, il n'est pas besoin de préciser ici le service auprès duquel la personne concernée pourra exercer ses droits et les mesures prises pour faciliter cet exercice. Il n'est pas besoin non plus de fournir une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la confidentialité et la sécurité du traitement, ni de rapporter les interconnexions des données ou leur cession à des tiers, car tous cela est inapproprié lorsque les droits des personnes ne sont pas menacés.

Ainsi, lorsqu'il s'agit de salariés d'entreprises, il semble qu'une déclaration simplifiée suffise pour procéder au traitement de leur données personnelles nécessaires à la gestion de l'entreprise et à l'exécution de la relation de travail, et ce pour les mêmes raisons qui dispensent l'employeur du recueil de leur consentement.

## 2/ L'autorisation

A l'examen de la déclaration fournie par le responsable du traitement, il peut apparaître à l'autorité nationale que le traitement envisagé présente des dangers manifestes pour le respect et la protection de la vie privée et des libertés et droits fondamentaux des personnes. Dans ce cas, l'autorité soumet ledit traitement au régime d'autorisation préalable. La décision de l'autorité nationale dans ce cas, doit

être motivée et notifiée au responsable du traitement dans les 10 jours suivant le dépôt de la déclaration<sup>36</sup>.

A ce titre, et alors que la loi interdit en principe le traitement des données sensibles, il peut être autorisées par l'autorité nationale dans des cas énumérés par l'article 18 de la loi n° 18-07, comme pour des motifs d'intérêt public indispensables à l'exercice des fonctions légales ou statutaires du responsables de traitement, ou lorsque la personne concernées a donné son accord exprès, en cas d'une disposition légale qui le consacre, ou encore lorsque le traitement est nécessaire à la défense d'intérêts vitaux de la personne concernée ou d'un autre personne incapable de manifester son consentement...etc.

L'autorisation de l'autorité nationale est aussi indispensable pour l'interconnexion des données qui consiste en la mise en relation de données traitées pour une finalité déterminées avec d'autres données traitées pour des finalités identiques ou non, par le même responsable du traitement ou par d'autres responsables de traitement, le tout devant permettre d'atteindre des objectifs légaux et légitimes pour les dits responsables de traitement<sup>37</sup>.

Dans tous ces cas, l'entreprise responsable du traitement doit introduire auprès de l'autorité nationale, une demande d'autorisation comprenant tous les éléments d'une déclaration entière au sens de l'article 14 de la loi n°18-07. L'autorité nationale doit rendre sa décision dans un délai de 2 mois de sa saisine, mais ce délai peut être prorogé par l'autorité nationale pour une même durée. Lorsque l'autorité nationale ne s'est pas prononcée dans le délai, la demande d'autorisation est réputée rejetée<sup>38</sup>.

#### **Sous-section 4 : L'influence de la pandémie Covid-19 sur les obligations de l'entreprise dans les opérations de traitement des données**

À l'échelle mondiale, l'épidémie Covid-19 a entraîné une remise en cause des restrictions posées sur les opérations de traitement des données personnelles, mettant ainsi en priorité l'urgence sanitaire, par rapport à la considération du respect de la vie privée, moins vitale dans ce contexte particulier. On assiste alors à la profusion d'applications anti-covid qui recueillent les données personnelles des personnes physiques par des questionnements minutieux sur leur état de santé, leur position, leurs contacts... etc, sachant qu'en France, ces applications sont juridiquement encadrées<sup>39</sup>. Il s'agit là de données qui n'auraient jamais été exploitées de la sorte dans des circonstances ordinaires, et d'un procédé qui remet en cause tout ce qui a été

<sup>36</sup> Article 17 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement de leurs données à caractère personnel, Op.cit.

<sup>37</sup> Voir les articles 03 et 19 de la loi n° 18-07, Op.cit.

<sup>38</sup> Art. 20, Ibid.

<sup>39</sup> Par exemple, le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé «STOPCOVID» JORF n° 0131 du 30-05-2020.

dit sur les obligations de l'entreprise, qu'elle soit responsable du traitement, sous-traitante ou destinataire du traitement.

Et alors que la CNIL en France, à titre d'exemple, et dans un souci de limiter au maximum l'abus qui peut être perpétré par ces applications de lutte contre la covid, s'astreint à délimiter la frontière entre le traitement des données nécessaires à la lutte contre la pandémie, et le respect de la vie privé devant demeurer dans les préoccupations de l'institution<sup>40</sup>, en Algérie, alors que la loi cadre n°18-07 n'a même pas encore été suivie des textes d'application qui permettraient sa mise en œuvre, il est clairement difficile de contrôler la proportionnalité de l'exploitation des données par des applications anti-Covid opérationnelles, à la lutte nécessaire contre la pandémie.

## **Section 2 : les droits des personnes physiques sujets au traitement de leurs données personnelles par l'entreprise**

En même temps que la responsabilisation des entreprises sur les données personnelles de leurs clients, utilisateurs/consommateur ou salariés, des droits sont accordés à ceux-ci pour faire face à la menace que pourrait constituer le traitement des données, par l'entreprise, sur leur vie privée. Outre le droit à l'information, la loi n° 18-07 accorde à la personne concernée le droit d'accès aux données qui lui permet d'obtenir du responsable du traitement la communication intelligible de ses données objet de traitement. Elle confère également le droit de rectification, en vertu duquel la personne concernée obtient l'actualisation, l'effacement ou le verrouillage des données personnelles dont le traitement n'est pas conforme à la loi. La personne concernée dispose enfin du droit de s'opposer, pour des motifs légitimes, à ce que des données personnelles la concernant fassent l'objet d'un traitement<sup>41</sup>.

### **Sous-section 1 : Le droit à l'information**

Tel que nous l'avons détaillé in supra<sup>42</sup>, l'entreprise ne peut procéder au traitement des données personnelles sans en informer préalablement les personnes concernées. En principe, le responsable du traitement va au-delà de la simple information en procédant au recueil du consentement. Mais, dans certaines situations, ce consentement n'est pas exigé. Il s'agit notamment des traitements de données personnelles des salariés.

Toutefois, les exceptions à la condition du consentement préalable ne privent pas les personnes concernées de leur droit à l'information claire et précise des

<sup>40</sup> Voir à titre d'exemple la Délibération n° 2021-004 du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19. Délibérée par la CNIL suite à la demande d'avis n° 210000315. <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-n2021-004.pdf>

<sup>41</sup> Articles 34, 35 et 36 de la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Op.cit.

<sup>42</sup> Voir Supra, PP. 18-19.

opérations de traitement les concernant, et n'exemptent pas le responsable du traitement de l'obligation de la fournir, cette information devant comprendre de façon non exhaustive les modalités de traitements et ses finalités, un rappel des droits de la personne concernée sur ses données et si les données en question feraient l'objet d'un transfert à une autre entité juridique<sup>43</sup>.

## **Sous-section 2 : Le droit d'accès**

Aux termes de l'article 34 de la loi 18-07, la personne dont les données personnelles font objet de traitement, a le droit d'obtenir du responsable du traitement, la confirmation que les données personnelles la concernant sont ou ne sont pas traitées, les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires et la communication, sous une forme intelligible, des données qui font l'objet de traitement, ainsi que de toute information disponible sur l'origine des données.

En application de ces dispositions en matière de traitement des données des salariés par l'entreprise, le salarié pourra exiger de son employeur qu'il lui adresse une copie intégrale de ses données objet de traitement, qui devra préciser la nature des données traitées, leur catégorie, la finalité du traitement, etc.

Il est d'ailleurs envisageable que ces dispositions deviennent un moyen de pression juridique en cas de conflit avec l'entreprise. Il peut arriver que des salariés invoquent la non-conformité des éléments de preuve issus de fichiers non conformes à la loi sur la protection des données pour faire rejeter les arguments de l'employeur dans un conflit donné.

## **Sous-section 3 : Le droit à la rectification**

En application de l'article 35 de la loi n° 18-07, la personne physique, dont les données ont été traitées, a le droit d'obtenir gratuitement, du responsable du traitement l'actualisation, la rectification, l'effacement ou le verrouillage des données personnelles dont le traitement n'est pas conforme à la loi, notamment en raison du caractère incomplet ou inexact de ces données, ou dont le traitement est interdit par la loi. Le responsable du traitement est alors tenu de procéder aux rectifications nécessaires, sans frais pour le demandeur, dans un délai de 10 jours de saisine.

En cas de refus ou de non réponse dans le délai précité, la personne concernée peut introduire une demande de rectification auprès de l'autorité nationale, laquelle charge l'un de ses membres à l'effet de mener toutes investigations utiles et faire procéder aux rectifications nécessaires, dans les plus brefs délais. La personne concernée est tenue informée des suites réservées à sa demande.

---

<sup>43</sup> FISCHER Servane, KERVADEK Ronan, « L'impact du RGPD sur la gestion des données personnelles des salariés », Op.cit., p. 2/11.



En outre, toute actualisation, toute rectification, tout effacement ou tout verrouillage des données à caractère personnel effectués doivent être notifiés, par le responsable du traitement, aux tiers ayant reçu communication des données, si cela ne s'avère pas impossible.

#### **Sous section 4 : Le droit d'opposition**

Le traitement des données personnelles ne saurait constituer une routine ordinaire à laquelle il faudrait se soumettre sans s'y opposer. Il appartient à la personne concernée, au contraire, de s'opposer pour des motifs légitimes à ce que des données personnelles la concernant fassent l'objet d'un traitement. Elle a notamment le droit de s'opposer à ce que des données qui la concernent soient utilisées à des fins de prospection commerciale, soit par le responsable du traitement à un moment donné, ou lors d'un traitement ultérieur.

À ce titre, l'article 37 de la loi n° 18-07 interdit la prospection directe au moyen d'un automate d'appel, d'un courrier électronique, d'un télécopieur ou de tout autre moyen employant une technologie de même nature, qui utilise, sous quelque forme que ce soit les coordonnées d'une personne physique qui n'ait pas exprimé son consentement au préalable.

Il est toutefois difficile d'appliquer ces dispositions dans un contexte de subordination. Aussi, les salariés ne peuvent exercer un droit d'opposition sur le traitement de leurs données personnelles lorsque ce traitement est effectué par le chef d'entreprise dans le cadre de la gestion de celle-ci. En ce sens, l'article 36 de la loi n° 18-07 déclare que les dispositions concernant le droit d'opposition ne s'appliquent pas lorsque le traitement répond à une obligation légale, ce qui est le cas des salariés tenus de se plier aux obligations émanant de leurs contrats de travail, dont la mise à disposition de l'employeur de toute information les concernant, et qui est utile à la gestion de l'entreprise et des relations de travail.

Par ailleurs, le droit d'opposition peut aussi être écarté par une disposition expresse de l'acte autorisant le traitement des données personnelles, conformément à l'article 36 de la même loi.

#### **Conclusion**

Pour conclure, la loi n° 18-07 constitue une avancée importante en matière de protection des libertés individuelles, mais aussi, dans la responsabilisation des entreprises sur les données qu'elles collectent et la préservation de la vie privée des personnes physiques qui interagissent tant dans le processus de production que dans celui de la consommation.

Cette loi est cependant encore récente en Algérie, et pour parer à la difficulté de sa mise en application, il y a encore un grand effort à faire tant au niveau de la réglementation, à travers des textes d'application, qu'au niveau de la jurisprudence, au moyen d'arrêts de la Cour suprême explicatifs et/ou complémentaires. Il est

d'ailleurs envisageable qu'elle génère de nouveaux conflits ou qu'elle devienne un moyen de pression juridique de part et d'autre dans des situations conflictuelles, d'où la nécessité d'actions complémentaires en réglementation, en informations et en sensibilisation.

Il serait ainsi de bon augure de prévoir un guide pratique de conformité des entreprises à la loi sur la protection des données personnelles. Au-delà, de l'objectif de conformité, ce guide pourrait permettre à l'entreprise d'optimiser la valorisation des données récoltées au service de son développement, ainsi que l'ont fait la CNIL et Bpfrance afin d'aider les PME et TPE à mettre en œuvre tous les moyens nécessaires pour être en conformité avec le RGPD<sup>44</sup>.

Il convient par ailleurs de réglementer les questions qui prêtent à confusion, comme la sous-traitance des données personnelles, et les conditions particulières d'application dans des circonstances exceptionnelles telles que les épidémies ou les catastrophes naturelles.

Mais en attendant de telles initiatives complémentaires, la loi n° 18-07 s'avère pour l'heure difficilement applicable, si l'on sait que même l'Autorité publique qui y est citée n'est toujours pas instituée, ou définie. Il faudra donc attendre longtemps avant de sortir du cadre de l'étude purement théorique de la question de la protection des données personnelles des personnes physiques au sein des entreprises.

---

<sup>44</sup> Voir pour plus de détails : Rapport CNIL et BpFrance, « La CNIL et Bpfrance s'associent pour accompagner les TPE et PME dans leur appropriation du règlement européen sur la protection des données (RGPD), 17/04/2018.

<https://www.cnil.fr/fr/la-cnil-et-bpfrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement>