Publié le 29 juin 2018

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Lire cet article en ligne

La nouvelle loi sur la protection des données personnelles

La loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles a été promulguée le 20 juin 2018 et publiée au Journal officiel du 21 juin 2018.

Cette loi a pour objet d'adapter la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après la « Loi Informatique et Libertés ») au droit de l'Union européenne résultant du Règlement général sur la protection des données (RGPD) applicable depuis le 25 mai 2018[1] (ci-après « RGPD ») (un règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre) et de la Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (une directive lie les Etats quant

au résultat à atteindre tout en leur laissant la compétence quant à la forme et aux moyens) qui devait être transposée avant le 6 mai 2018 (Ci-après la « Directive 2016/680).

Pour se mettre en conformité avec le droit européen, l'état français a donc choisi de ne pas abroger la loi dite Informatique et Libertés de 1978 mais de l'adapter.

La loi comprend un premier titre comprenant les dispositions d'adaptation communes au RGPD et à la Directive 2016/680, un deuxième des dispositions relatives aux nombreuses marges de manœuvres permises aux Etats membres par le RGPD, un troisième des dispositions de transposition de la Directive 2016/680, un quatrième des dispositions spécifiques visant à faciliter l'application des règles relatives à la protection des données à caractère personnel par les collectivités territoriales (en habilitant le Gouvernement à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires pour améliorer l'intelligibilité de la législation applicable à la protection des données) et enfin un cinquième des dispositions diverses et finales.

A noter que sont maintenant attendus une dizaine de décrets d'application pris en Conseil d'Etat après avis de la Commission nationale de l'informatique et des libertés (CNIL), afin de finaliser l'adaptation au droit européen.

La fin des formalités préalables

Alors que la loi Informatique et Libertés reposait sur une logique de formalités préalables, le règlement opère un changement radical et repose sur une logique de conformité continue : chaque acteur concerné doit être en conformité en permanence avec les règles relatives à la protection des données et en mesure de le démontrer.

La loi remplace donc le système de contrôle a priori, basé sur les régimes de déclaration et d'autorisation préalables, par un système de contrôle a posteriori, fondé sur l'appréciation par le responsable de traitement des risques en matière de protection des données.

En contrepartie, les pouvoirs de la CNIL sont renforcés, et les sanctions encourues pourront atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial consolidé.

Il convient de préciser que les formalités préalables sont cependant maintenues pour les données les plus sensibles, telles que les données biométriques nécessaires à l'identification ou au contrôle de l'identité des personnes, les données génétiques, les données utilisant le numéro d'inscription au répertoire national d'identification des personnes physiques ou les données de santé.

La CNIL

La loi définit le champ des missions de la CNIL conformément au RGPD.

La CNIL devient l'autorité nationale de contrôle pour l'application du RGPD.

Celle-ci prend en charge la publication de référentiels, de codes de bonne conduite et de règlements types sur les nouvelles obligations des opérateurs. Elle peut certifier des organismes et des services. Elle peut être consultée pour tout proposition de loi portant sur la protection des données personnelles par les présidents ou les commissions compétentes de l'Assemblée nationale ou du Sénat et par les présidents des groupes parlementaires.

La loi précise et étend les pouvoirs de contrôle de la CNIL. Ses agents ont accès, de 6 heures à 21 heures aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel, à l'exclusion des parties de ceux-ci affectées au domicile privé. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous certaines réserves, par le secret médical. Pour les contrôles en ligne, les agents peuvent dorénavant recourir à une identité d'emprunt.

Les données sensibles

Conformément au RGPD, le champ des données sensibles (sur l'origine raciale, les opinions politiques, etc.) est étendu **aux données génétiques et biométriques ainsi qu'aux données relatives à l'orientation sexuelle d'une personne.**

En principe, ces données ne peuvent pas faire l'objet d'un traitement en raison de leur nature même.

Des dérogations à cette interdiction sont toutefois prévues par le droit européen (si la personne a expressément consenti au traitement de ses données ou si elle les a rendues publiques, en matière de sécurité sociale, etc.).

La loi du 20 juin 2018 ajoute d'autres dérogations. Sont notamment permis les traitements de données biométriques (empreintes digitales, etc.) strictement nécessaires aux contrôles d'accès sur les lieux de travail, aux ordinateurs et aux applications utilisés au travail. Sont de même autorisés les traitements portant sur la réutilisation d'informations figurant dans les décisions de justice diffusées dans le cadre de l'open data.

Le consentement des mineurs

Pour les mineurs de moins de quinze ans, le consentement des titulaires de l'autorité parentale sera nécessaire pour le traitement des données personnelles sur les réseaux sociaux. C'est à partir de l'âge de quinze ans qu'un mineur pourra s'inscrire sur des réseaux sociaux sans autorisation parentale.

Le recours aux algorithmes

La loi étend les cas dans lesquels, par exception, une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel (c'est-à-dire le recours à des algorithmes pour prendre des décisions individuelles automatisées).

Ces dispositions ont fait l'objet de débats intenses entre le Sénat et l'Assemblée nationale dans un contexte de controverse concernant l'utilisation d'algorithmes par les universités dans le cadre de Parcoursup (site web destiné à recueillir et gérer les vœux d'affectation des futurs étudiants de l'enseignement supérieur public français).

Dans sa décision du 12 juin 2018, le Conseil a validé ces dispositions en indiquant toutefois que l'administration doit avoir la « *maîtrise du traitement algorithmique et de ses évolutions* » et donc que « *ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement* » (les algorithmes « auto-apprenants »).

L'action de groupe

L'action de groupe en matière de données personnelles a été introduite en France par la loi de modernisation de la justice du XXIe siècle n°2016-1547 du 18 novembre 2016, qui a créé un nouvel article 43 *ter* dans la loi Informatique et Libertés.

Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de cette loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente pour faire cesser en justice un manquement par un responsable de traitement ou un sous-traitant (sachant que seules des associations ou organisations peuvent exercées une telle action).

La loi étend cette action de groupe à la réparation des préjudices matériels et moraux subis en cas de violation des données personnelles, dans un contexte où l'association de défense des internautes la Quadrature du Net a annoncé avoir déposé cinq plaintes collectives contre Google, Apple, Facebook, Amazon et LinkedIn (Microsoft), estimant que ces derniers ne respectent pas le RGPD sur le consentement « libre et éclairé » des internautes.

[1] Cf. nos articles intitulés « Nouveau règlement européen sur la protection des données (Partie I) » et « Nouveau règlement européen sur la protection des données (Partie II) »

conseil juridique. Le destinataire est seul responsable de l'utilisation qui pourrait être faite des informations qu'il contient.