Introduction

« L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. »

Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit Règlement Général sur la Protection des Données « RGPD », considérant 6.

QUI EST CONCERNÉ PAR LA PROTECTION DES DONNÉES PERSONNELLES ?

Toutes les organisations sont concernées par les données personnelles : personnes physiques et personnes morales à but lucratif (entrepreneurs individuels, artisans, commerçants, professions libérales, start-up, TPE/PME, sociétés cotées) ou à but non lucratif (associations, syndicats, Etat, collectivités territoriales, établissements publics). Tous les volumes et tous les traitements de données sont en cause. Il ne s'agit pas seulement du big data ou de l'intelligence artificielle, mais des différents fichiers, en version papier ou électronique, quotidiennement utilisés par les organisations (fichiers clients, fichiers RH de salariés, fichiers fournisseurs, données des utilisateurs des réseaux sociaux, vidéosurveillance, fichiers de police, télémédecine, marketing ciblé, lutte contre la fraude, etc.).

Toutes les fonctions de l'entreprise sont également impactées : direction juridique, direction des systèmes d'information (DSI), direction des risques, direction des ressources humaines, services marketing, ventes et achats (Depadt Bels et Haas, 2018).

Les pratiques des organisations doivent respecter le droit à la vie privée. Le RGPD est entré en vigueur au sein de l'Union européenne le 25 mai 2018. Il « *protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel* » (RGPD, art. 1.2) en renforçant les droits des personnes physiques concernées par les données personnelles (e-mails, numéros de téléphone, nom, etc.), en accentuant les obligations des responsables de traitement et des sous-traitants et en aggravant les sanctions encourues. Transparence et maîtrise des données sont les deux piliers du RGPD.

Comme le soulignent des auteurs, « *à travers le monde entier, les pays ne veulent plus d'entreprises en roue libre faisant ce qui leur plaît des données personnelles. C'est un moment clé*

que les entreprises ne doivent pas rater » (Morey, Forbath et Schoop, 2018, p. 66). En effet, « *identifier et adopter volontairement les politiques de confidentialité des données les plus strictes immunisera une entreprise contre les ennuis juridiques et enverra aux consommateurs un message important qui pourra donner un avantage compétitif* » (*ibid.*).

À SAVOIR

« Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques » (RGPD, consid. 18).

QUE SONT LES DONNÉES PERSONNELLES ?

On entend par données à caractère personnel, « *toute information se rapportant à une personne physique identifiée ou identifiable (...) ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (RGPD, art. 4.1). La définition des données personnelles est donc large. Peu importe la forme de l'information : caractères alphanumériques, images, sons, identifiants, données de localisation, nom, numéro d'identification comme le

numéro d'inscription au Répertoire national d'identification des personnes physiques géré par l'INSEE, adresse IP, etc. Peu importe également la technologie utilisée et la volonté d'identifier la personne ou non.

À SAVOIR

Les réponses écrites fournies par un candidat lors d'un examen professionnel ainsi que les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère personnel (CJUE, 20 déc. 2017, n° C-434/16).

Le règlement ne s'applique pas aux données anonymes qu'elles le soient initialement ou qu'elles aient fait l'objet d'une anonymisation (RGPD, considérant 26). La donnée anonyme ne peut pas être rattachée à une personne identifiée ou identifiable. D'après le règlement, « *pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci* ».

Le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier (RGPD, art. 2.1). Le traitement est « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enre-*

gistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » (RGPD, art. 4.2).

COMMENT S'APPLIQUE LE RGPD ?

D'un point de vue territorial, le RGPD s'applique « *au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* » (art. 3.1). L'existence d'un établissement doit se faire à l'aune « *du degré de stabilité de l'installation* [ainsi] *que* [de] *la réalité de l'exercice des activités [de la personne dans l'État membre considéré] en tenant compte de la nature spécifique des activités économiques et des prestations de services en question* » (Cour de Justice de l'Union Européenne, 1er oct. 2015, aff. C-230/14, Weltimmo, point 29, JurisData n° 2015-025844). La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard (considérant 22 du RGPD).

Par exemple, une entité établie en France héberge des données personnelles aux Etats-Unis.

Il s'applique également « *au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* » (art. 3.2). Par exemple, un responsable de traitement est établi aux Etats-

Unis, mais il profile des Français ou un responsable de traitement est établi en Inde, mais il a un sous-traitant en France pour des opérations de crédit en ligne et a accès à la base de données du sous-traitant.

DROIT FRANÇAIS : ORDONNANCE DU 12 DÉCEMBRE 2018

Le RGPD, issu du droit de l'Union européenne, s'applique directement en droit français depuis le 25 mai 2018. Il coexiste cependant avec des textes de source française. En effet, avant l'adoption du règlement, la France connaissait déjà une loi sur les données personnelles : la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (couramment appelée loi Informatique et Libertés). Cette loi a été modifiée, après l'adoption du règlement européen, par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Cette dernière loi s'est accompagnée du décret n° 2018-687 du 1er août 2018 qui modifie le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le RGPD comporte de nombreux renvois au droit des Etats membres. La loi de 2018 a peu utilisé les marges de manœuvre disponibles. En effet, la nouvelle loi française s'est limitée à compléter la réglementation sur les missions de la CNIL et a apporté des précisions sur les données sensibles, les infractions, les données de santé ou le numéro de sécurité sociale. Le texte français ne rétablit quasiment aucune formalité préalable à accomplir auprès de la CNIL.

La loi du 20 juin 2018 prévoyait un projet d'ordonnance dans les six mois de la loi. Le 12 décembre 2018 a été édicté l'ordonnance n°2018-1125 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la

protection des données à caractère personnel. Cette ordonnance met le droit français en conformité avec le règlement européen. Elle a, avant sa ratification par le Parlement, une valeur infra-législative.

L'ordonnance permet notamment de procéder à l'adaptation et à l'extension à l'outre-mer des dispositions prévues par la loi Informatique et Libertés du 6 janvier 1978 ainsi qu'à l'application à Saint-Barthélemy, à Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans les Terres australes et antarctiques françaises de l'ensemble des dispositions de la loi du 6 janvier 1978 précitée (titre V).

Les dispositions de l'ordonnance entrent en vigueur en même temps que le décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la présente ordonnance, et au plus tard le 1er juin 2019.

Dans les développements, une place sera également faite aux délibérations et aux recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL), qui est l'autorité de contrôle française, ainsi qu'aux avis du G29 (groupe des autorités de contrôles européennes).

DIRECTIVE VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES (ePrivacy)

À noter également que la directive 2002/58/CE 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (PE et cons. UE, dir. 2002/58/CE, 12 juill. 2002), dite directive vie privée et communications électroniques ou directive « cookie » contient des règles spécifiques sur les données personnelles, applicables au secteur des télécommunications. En effet, « *les*

services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à *caractère personnel et leur vie privée* » (dir., consid. 6).

Cette directive fait actuellement l'objet d'une révision dans le cadre d'une proposition de règlement « vie privée et communications électroniques » (e-Privacy) publiée le 10 janvier 2017. La proposition de règlement tend à harmoniser les règles applicables aux communications électroniques avec les nouvelles règles du RGPD. La Commission prévoit que le règlement s'appliquera aux opérateurs de télécommunications dont Google, WhatsApp, etc. Les dispositions protectrices de la vie privée porteront sur le contenu des communications électroniques, mais aussi sur d'autres données telles que celles permettant d'identifier la source et la destination d'une communication, la date, l'heure, la durée d'une communication et sa localisation. Ces données devront être anonymisées ou effacées si l'utilisateur ne consent pas à leur traitement, sauf s'il s'agit de données nécessaires à la facturation. La proposition a vocation à réviser l'ensemble des règles qui s'appliquent aux professionnels en matière de prospection commerciale par voie électronique et de marketing ciblé sur Internet. Comme pour le RGPD, les manquements aux obligations prévues par le règlement ePrivacy pourraient faire l'objet de sanctions pécuniaires. La version définitive du texte devrait être adoptée prochainement. Comme le remarquent des auteurs, *« initialement, l'ePrivacy devait s'appliquer en même temps que le RGPD, et l'on peut regretter que ce ne soit pas le cas car cette approche en deux temps fragmente le paquet européen de protection des données. La proposition de règlement soulève de nombreuses questions d'articulation avec le RGPD, notamment en ce qu'elle privilégie une approche fondée sur le consentement de l'utilisateur et n'emploie pas les termes "responsable du traitement" et "sous-traitant"* » (Fauvarque-Causson et Maxwell, 2018, p. 1033s). Les effets sur les traitements de prospection commerciale

devront alors être étudiés (sur cette question, voir Desgens-Pasanau, 2018, p. 13 et 14).

MÉTHODE

La méthodologie retenue est d'étudier les innovations majeures du règlement et des adaptations en droit français (chapitre I), avant de présenter les différentes étapes de mise en conformité au droit nouveau des pratiques des organisations pour assurer la protection de leurs données (chapitre II).