Réglementation générale sur la protection des données : bref aperçu

Le 12 août 1981, naquit le premier ordinateur personnel IBM. Le 29 juin 2007, était lancée aux Etats-Unis, la première génération d'iPhone. Au cours de la décennie qui suivit, le simple téléphone portable devint un véritable périphérique multimédia, permettant de surfer sur le web, consulter ses emails, prendre et partager des photos. En 2004, fut lancé Facebook et en 2006, Twitter. Depuis le milieu des années 1980, le volume des communications personnelles via les moyens électroniques a augmenté de façon exponentielle.

Les plateformes en ligne et les navigateurs web sont utilisables « gratuitement ». En échange, les utilisateurs doivent céder leurs données à caractère personnel. Une tension indéniable se manifeste entre le droit des individus au respect de leur vie privée et familiale, leur domicile et leurs correspondances, et l'ambition des sociétés d'atteindre de nouveaux clients, d'une façon plus ciblée et efficace.

Au fur et à mesure de l'évolution technologique, le législateur s'est démené pour ne pas se laisser dépasser. La Convention du Conseil de l'Europe pour « la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » fut adoptée à Strasbourg, le 28 janvier 1981. Une première directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données fut mise en œuvre à partir d'octobre 1998.

Cette directive 95/46/CE a été abrogée et remplacée par le Règlement Général sur la Protection des Données (« **RGPD** ») qui s'appliquera à partir du 25 mai 2018. L'ambition du RGPD est de mettre à jour la législation européenne en matière de protection des données et l'adapter au 21ème siècle. Il s'agit d'une réglementation complexe. Le préambule du RGPD comprend 173 considérants. Le RGPD comporte 99 articles répartis en 10 chapitres. Un bref aperçu de la nouvelle législation est ci-après proposé (les références renvoient aux articles du règlement, sauf indication contraire).

Définitions (article 4 du RGPD)

- **Les « données à caractère personnel »** sont définies à l'article 4.1. Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable (la « personne concernée ») et qui comprend des références à un élément identifiant tel qu'un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne.
- **Le « responsable du traitement »** est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement des données personnelles (article 4.7).
- **Le « sous-traitant »** est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (article 4.8).

Champ d'application (articles 2 et 3 du RGPD)

- **Champ d'application matériel :** Le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier (les exceptions se trouvent à l'article 2.2).

- **Champ d'application territorial :** Le champ d'application territorial du RGPD est très large. Il comprend tous les traitements de données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Il s'applique également aux entreprises du monde entier qui traitent des données personnelles de citoyens de l'UE pour leur offrir des biens ou des services ou pour suivre leurs comportements, dans la mesure où ceux-ci ont lieu au sein de l'Union.

Principes relatifs au traitement des données à caractère personnel

- **L'article 5** reprend les grands principes relatifs au traitement des données à caractère personnel. Il établit les principes de licéité, de loyauté et de transparence du traitement et il prévoit que les données doivent être collectées pour des finalités déterminées, limitées à ce qui est nécessaire au regard de la finalité pour laquelle elles sont traitées et exactes (« limitation des finalités », « minimisation des données » et « exactitude »).
- **Le nouveau principe de « responsabilité »** est introduit par l'article 5.2. Le responsable du traitement doit être en mesure de démontrer qu'il respecte les principes relatifs au traitement des données à caractère personnel dont il a la responsabilité.

Licéité du traitement

- **Licéité du traitement :** L'article 6 énonce six conditions sur base desquelles le traitement sera considéré comme licite dans tous les cas. Il en sera ainsi lorsque le traitement est nécessaire à l'exécution d'un contrat ou nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis ou lorsqu'il est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement.
- **Consentement :** Le consentement est l'une des six hypothèses de traitement licite. Il s'agit de toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement (article 7). Il doit être aisé de supprimer ou de donner son consentement.

Droits de la personne concernée (articles 12-23)

- Comme mentionné plus haut, la transparence est un principe clé du traitement des données à caractère personnel.
- Les personnes concernées doivent pouvoir recevoir des informations en ce qui concerne le traitement de leurs données d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (articles 12, 13 et 14).
- L'exigence de transparence est sous-tendue par un certain nombre de droits spécifiques par lesquels la personne concernée peut se voir garantir un traitement loyal de ses données personnelles : un droit d'accès de la personne concernée aux données à caractère personnel la concernant (article 15), un droit de rectification (article 16) et un droit à l'effacement (« droit à l'oubli ») (article 17). Les organisations doivent s'assurer qu'elles disposent de procédés et de technologies qui leur permettent d'effacer les données à caractère personnel en réponse aux demandes des personnes concernées (article 17). La personne concernée dispose également d'un droit à la limitation du traitement et d'un droit à la portabilité des données, (articles 18 et 20).
- Une limitation claire en matière de profilage est instituée par l'article 22. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un

traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Le responsable du traitement et le sous-traitant (articles 24-32)

- **Responsabilité du responsable du traitement (article 24).** Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.
- **N.B**. *Selon l'article 30, chaque responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité.* Cette exigence peut (assorties de certaines conditions) être supprimée pour les petites ou moyennes entreprises qui emploient moins de 250 employés ; l'autorité belge de contrôle de la protection des données a déclaré qu'elle voyait d'un bon œil les sociétés qui tenaient un tel registre.
- **Responsabilité du sous-traitant** : le RGPD étend la responsabilité aux sous-traitants qui ne se conforment pas aux exigences de la réglementation. Assurer la sécurité du traitement par des mesures techniques et organisationnelles appropriées, ce qui inclut la pseudonymisation et le chiffrement des données à caractère personnel, est une exigence obligatoire de conformité pour les responsables de traitement et les sous-traitants, compte tenu de l'état des connaissances, des coûts de mise en œuvre et des risques que le traitement pose pour les personnes concernées.

Outils de conformité

- Le RGPD comporte certains outils de conformité. **Article 25 : La protection des données dès la conception et la protection des données par défaut.** Au lieu de considérer les questions de protection des données après avoir conceptualisé ou réalisé les outils ou procédés de traitement, on vise ici à exiger la conformité aux principes de protection des données et à remplir les exigences du RGPD, au moment de la conception de tels outils ou procédés.
- **Articles 33 et 34 : Notification à l'autorité de contrôle d'une violation de données à caractère personnel**. Les exigences en matière de notification en cas de violation de données sont censées harmoniser les pratiques au sein de l'UE.
- **Analyse d'impact relative à la protection des données (article 35).** Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les personnes concernées, les organisations devront mener une analyse de l'impact des opérations de traitement et pourront avoir besoin de travailler avec l'autorité de réglementation compétente pour assurer la conformité avec le RGPD.

Le délégué à la protection des données (« DPD ») (article 37)

- La désignation d'un DPD est obligatoire dans certains cas, en particulier lorsque le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle. Un groupe d'entreprise peut désigner un seul délégué à la protection des données à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.
- Selon une enquête réalisée par l'Association internationale des professionnels de la protection de la vie privée (« IAPP »), cette exigence signifie que 28 000 DPD devront être nommés en Europe.
- Le DPD peut être une personne physique ou morale. S'il s'agit d'une personne morale, il est essentiel que chaque membre de cette organisation qui agit en tant que DPD le fasse conformément aux règles des articles 37-39.

Codes de conduite et certification (articles 40-43)

- Instruments qui permettent de prouver le respect du RGPD.
- Les codes de conduite (articles 40-41) et certification (articles 42-43) sont expressément reconnus par la réglementation comme étant des mécanismes d'adhérence acceptables qui constituent un moyen de preuve du respect du RGPD. Au moment où nous rédigeons cet article, ceux-ci sont encore en cours d'élaboration.

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales (articles 44-50)

- L'article 44 expose le principe général selon lequel les transferts vers l'extérieur de l'UE peuvent seulement avoir lieu si les conditions définies dans ce chapitre du RGPD sont respectées.
- L'article 45.3 prévoit que la Commission européenne peut décider qu'un pays tiers assure un niveau de protection adéquat de telle sorte que des transferts vers ce pays peuvent avoir lieu sans autre autorisation.
- En l'absence d'une telle décision, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers que s'il a prévu des garanties appropriées. Celles-ci peuvent être fournies par un certain nombre de mécanismes, comme des règles d'entreprise contraignantes (article 47) ou par l'utilisation de clauses contractuelles standard.

Autorités de contrôle indépendantes (articles 51-59)

- Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du RGPD. Leurs compétences, missions et pouvoirs sont énoncés aux articles 55-58.
- **Le mécanisme du « guichet unique » :** pour les transferts transfrontaliers de données à l'intérieur de l'UE, il existe une autorité de contrôle chef de file (« APD »). La présence de l'établissement principal (càd le lieu de l'administration centrale) d'une entité indiquera, en principe, où se situe l'autorité chef de file. Mais cette règle fait l'objet d'exceptions et chaque autorité de contrôle doit être compétente pour traiter une réclamation dont l'objet concerne uniquement l'Etat membre dont elle est responsable.

Coopération et cohérence (articles 60-67) et le Comité européen de la protection des données (articles 68-76)

- Pour s'assurer de l'application effective du RGPD, les APD doivent coopérer entre elles ainsi qu'avec la Commission européenne via un mécanisme de contrôle de la cohérence.
- Le Comité européen de la protection des données est un organisme indépendant doté d'une personnalité juridique. Il se compose d'un chef d'une APD de chaque état membre et du Contrôleur européen de la protection des données. Le Comité a pour mission la résolution de litiges et l'adoption de décisions contraignantes dans certains cas.

Voies de recours, responsabilité et sanctions (articles 77-84)

- **Les risques postérieurs de non-conformité avec le RGPD sont importants.** Certaines violations du RGPD peuvent faire l'objet d'amendes administratives pouvant s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (article 83.6). Il s'agit de l'amende maximale qui sera imposée pour les infractions les plus sérieuses (les violations des

droits des personnes concernées, par exemple). L'amende maximale en cas d'infraction procédurale – considérée comme moins sérieuse – est limitée à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total.

- **Les voies de recours offertes aux personnes concernées incluent :** le droit d'introduire une réclamation auprès d'une autorité de contrôle, le droit à un recours juridictionnel effectif contre une APD et le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant.
- **Droit à réparation et responsabilité.** Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir du responsable du traitement ou du sous-traitant, réparation du préjudice subi.

Les articles 85-91 contiennent des dispositions relatives à certaines situations particulières de traitement

- **L'article 88 concerne le traitement de données dans le cadre des relations de travail.** Il laisse la possibilité aux états-membres de prévoir des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans ce cadre.

Les articles 92-99 concernent la mise en œuvre du RGPD

L'article 99.2 prévoit que le RGPD s'appliquera à partir du 25 mai 2018.