2 | Les données personnelles : un actif et une responsabilité pour les plateformes

Quel utilisateur ne s'est jamais demandé ce qu'il advenait des informations transmises en ayant recours à des applications ou des sites internet ?

Cette question est parfaitement naturelle puisque de (trop ?) nombreuses données personnelles sont communiqués par les utilisateurs lors de l'inscription (identité, coordonnées...) et de l'utilisation (achats, localisation...) des plateformes numériques.

Cette transmission de données pose également de nombreux enjeux juridiques primordiaux pour les entreprises de l'économie numérique dont l'activité est, en partie, fondée sur la collecte massive et systématique de données personnelles.

Pour mémoire, le régime juridique français applicable aux données personnelles trouve son origine dans la combinaison de règles nationales (au premier rang desquelles la Loi informatique et libertés du 6 janvier 1978) et européennes (la directive européenne 95/46/EC du 24 octobre 1995 était la première norme clé en la matière). Cette architecture est actuellement en cours de mutation en raison de l'entrée en application du Règlement (UE) 2016/679 sur la protection des données personnelles (RGPD) qui s'accompagne d'une refonte de la Loi informatique et libertés par un projet de loi qui vient d'être adopté par le Parlement.

Rappelons quelques principes clés du droit des données personnelles :

- les contraintes s'appliquent à ceux qui traitent des « données personnelles » : cette notion fait référence à toute information relative à une personne physique identifiée ou pouvant l'être par référence à un ou plusieurs éléments qui lui sont propres.

- la collecte de données doit reposer sur un fondement juridique (par exemple, le consentement ou le respect d'une obligation légale), avoir une finalité déterminée (les personnes doivent savoir à quoi leurs données vont servir) et une pertinence (seules les données nécessaires à la réalisation de l'objectif doivent être collectées).

- les entreprises collectant les données (appréhendées par la notion de responsable de traitement) sont tenues de s'organiser en interne afin de ménager par leurs propres soins la preuve de leur conformité au droit des données personnelles. Ce principe dit d' « *accountability* » et de « *privacy by design* » a un impact fondamental sur l'organisation interne des entreprises numériques qui traitent de manière massive des données personnelles.

- les données doivent être collectées, traitées et stockées dans des conditions permettant de s'assurer de leur sécurité.

- les personnes dont les données sont collectées sont titulaires de droits (par exemple être informées au moment de la collecte mais également pouvoir accéder, rectifier, s'opposer ou effacer les données qui ont été collectées à leur sujet) dont les responsables de traitement doivent garantir la mise en œuvre effective.

- les sanctions attachées aux manquements à ces principes sont désormais sans commune mesure avec le régime antérieur à l'entrée en vigueur du RGPD, avec des amendes pouvant aller jusqu'à 4% du chiffre d'affaires mondial de l'entreprise concernée.

Les prochains mois seront déterminants dans la construction d'un nouvel équilibre du droit des données personnelles avec le début des premières opérations de contrôle de la CNIL et l'émergence d'une première « jurisprudence CNIL » post entrée en vigueur du RGPD.

Ces éléments sont essentiels pour permettre aux acteurs numériques de déterminer leurs chantiers prioritaires pour une mise en conformité et de prendre en considération ces nouvelles règles.