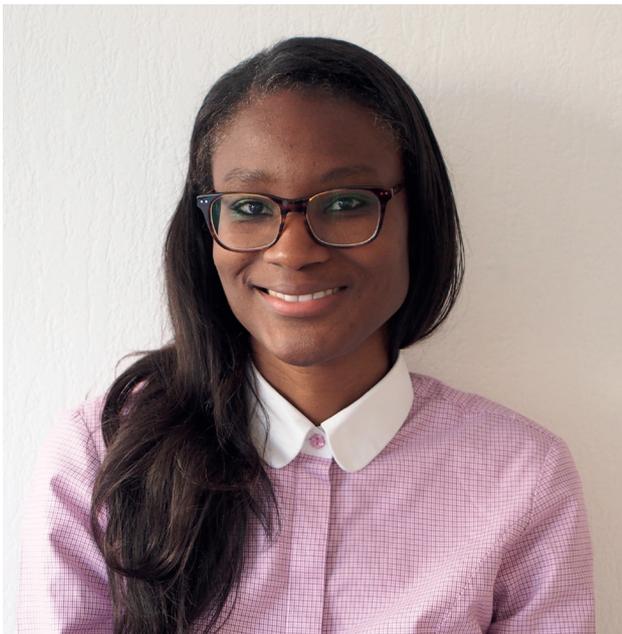


RGPD : droits



À l'heure du Web social et du « tout connecté », le nouveau règlement européen vient utilement protéger les données à caractère personnel.

La société a bien changé depuis la loi relative à l'informatique et aux libertés, visant à protéger les personnes physiques de tout traitement automatisé de données¹. Avec l'essor d'Internet – et notamment depuis 2005 et l'arrivée du Web « 2.0 » –, l'internaute est désormais devenu actif et acteur, il peut sans grande connaissance technique utiliser les nouvelles technologies pour interagir, échanger et communiquer, créant ainsi le « Web social ». Le Web social est un espace d'interaction illimité entre internautes, créant une nouvelle économie – il s'agit notamment des réseaux sociaux tels que Facebook. À cela s'ajoute l'ensemble des objets connectés permettant de simplifier notre quotidien en partageant une multitude d'informations contrôlées par nos smartphones. Nous sommes désormais passés au Web « 3.0 ». Mais quels sont les risques concernant la vie privée, quels sont les points de vigilance à adopter face à toutes ces

avancées technologiques, notamment chez les plus jeunes qui sont les plus vulnérables ? Le règlement général² sur la protection des données, dit « RGPD », vient renforcer la protection des données personnelles des individus, mais vise également à bousculer les habitudes des personnes physiques sur leur vie privée. Protection certes, mais les personnes étant actrices des réseaux sociaux, elles doivent également désormais maîtriser les informations relevant de la vie privée qu'elles communiquent. Il convient d'aborder l'apport de cette nouvelle réglementation européenne, son application en dehors de nos frontières et la vigilance que les plus jeunes notamment doivent adopter.

Les apports du nouveau règlement européen

Le droit français protège déjà largement les données à caractère personnel des individus et a d'ailleurs servi de modèle à de nombreux pays en Europe. Ainsi, toute

* Responsable adjoint du bureau de la propriété intellectuelle à Sorbonne Université et directrice du cabinet Koné & Associés

PRIVÉS RENFORCÉS

personne physique a le droit de s'opposer à tout traitement de données personnelles la concernant, a un droit d'accès, de modification et de suppression des données transmises et son consentement préalable à tout traitement doit avoir été obtenu. Désormais, la matérialisation de ce consentement devra être claire. Pour les mineurs de moins de 16 ans, le consentement des parents est nécessaire.

En plus de ces droits existants, le règlement européen renforce les droits des personnes physiques, chaque individu bénéficiant désormais des nouveaux droits suivants :

- **Droit d'information et de transparence sur le traitement effectué lorsque les données n'ont pas été collectées auprès de la personne physique directement.** Nous sommes ici dans le cas de figure où les données ont été collectées par une entreprise et transmises à une autre. Par exemple des habitudes d'achat transmises à une société de remise en forme pour que cette dernière puisse proposer des services d'entraînement sportif.
- **Droit à l'effacement dit « droit à l'oubli » ou « droit au déréférencement ».** Ce droit vise clairement les moteurs de recherche et offre la possibilité de demander à ce que soit effacé tout résultat de recherche via le nom ou le prénom d'une personne permettant d'accéder à un lien vers une page Internet contenant notamment son nom ou son prénom. Les informations ne seront pas effacées du moteur de recherche, mais les résultats de recherche seront relayés aux dernières pages afin de ne plus être directement visibles.
- **Droit à la limitation du traitement.** Toute personne peut demander au responsable du traitement de limiter l'utilisation de ses données à caractère personnel.
- **Droit à la portabilité des données.** Ce droit vise les plateformes d'écoute de musique « playlist » ou toute application mobile qui conserve, par exemple, l'ensemble des habitudes sportives ou alimentaires d'une personne. En effet, tout comme le droit à la portabilité du numéro de téléphone mobile, qui est également une donnée personnelle appartenant au titulaire de la ligne, les

données musicales, entre autres, constituent désormais des données à caractère personnel. À ce titre, toute personne peut demander au responsable de traitement d'obtenir « *dans un format structuré, couramment utilisé et lisible par une machine* », l'ensemble des données qui la concerne afin de les transmettre, si elle le souhaite, à un autre opérateur. Il est également possible de demander le transfert automatiquement de ses propres données d'une plateforme à une autre.

- **Décision individuelle automatisée, y compris profilage.** Il est interdit de rendre des décisions de justice à l'encontre d'une personne en se basant sur une appréciation faite sur le comportement de celle-ci, si cette appréciation a eu pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Nous remarquons que certains droits couvrent l'évolution des habitudes sociétales. Ainsi, l'ensemble des informations personnelles que chacun place sur les applications mobiles sont-elles également couvertes par le droit. Cela vaut pour l'ensemble des entreprises françaises, mais également pour les entreprises étrangères, dès lors que les données concernent un ressortissant européen. Pour les plus jeunes, il est important de se renseigner sur la finalité du traitement et de penser à cocher la case mentionnant le fait que l'on ne souhaite pas que les données fournies soient utilisées à d'autres fins que celles pour lesquelles elles ont été communiquées (exemple, démarchage commerciale ou communication à d'autres entreprises).

L'application du règlement européen en dehors de l'Europe

Les nouvelles technologies étant sans limitation de frontière, les nouvelles dispositions prévoient un cadre juridique sans frontière, commun à tous les pays européens. Ainsi, tout traitement (toute collecte) de données à caractère personnel

1 - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
2 - Règlement n° 2016/679 du Conseil de l'Europe et du Parlement européen 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.

réalisé dans un pays de l'Union européenne, transmis vers un ou plusieurs pays au sein de l'Union, sera géré par un guichet unique. Un seul établissement national en charge de la protection des données à caractère personnel sera l'autorité compétente pour l'ensemble des formalités. L'individu aura donc un seul interlocuteur. De même, le RGPD s'applique également à tous les responsables de traitement établis à l'étranger, dès lors qu'est ciblé un ressortissant européen. Il s'agit là d'une méthode permettant de réguler les acteurs mondiaux du secteur numérique.

Le pouvoir de sanction de la CNIL³ est également renforcé, des sanctions peuvent donc être prononcées à l'encontre d'une entreprise étrangère qui cible et collecte des données personnelles de personnes françaises. Les sanctions sous formes d'amende administrative pourront s'élever de 2 à 4 % du chiffre d'affaire annuel mondial de l'entreprise. Il y a de quoi, non pas dissuader mais inciter à changer la stratégie des grandes entreprises tels que Google, Apple, Facebook et Amazon notamment. En effet, la stratégie et le *business model* de ces entreprises est de proposer des services de gestion des données personnelles supposés simplifier la vie de leurs clients, sans grande maîtrise, contrôle et vigilance de la part de ces derniers sur les informations qu'ils communiquent, le risque d'atteinte à la vie privée s'accroissant.

À ce titre, l'une des nouvelles obligations apportées par le RGPD concerne l'étude d'impact qui doit désormais être réalisée avant tout traitement de données sensibles⁴, afin de mesurer les risques d'atteinte à la vie privée, les caractéristiques du traitement et les mesures de sécurité à adopter.

La vigilance des plus jeunes et l'atteinte à la vie privée

Le RGPD ne modifie pas les autres dispositions légales en matière de marketing ciblé, ainsi l'ordonnance n° 2006-301 du 14 mars 2016 énonce-t-elle, à l'article 34-5 du code des postes et des télécommunications, toute une série de mesures visant à prévenir la prospection commerciale

par Internet. Toute prospection directe par mail ou SMS sans avoir obtenu au préalable le consentement de la personne ciblée est interdite. Ainsi, avant tout démarchage, une entreprise utilisant des données personnelles telles que numéros de mobile, adresses mail et habitudes (adresses des lieux où elles peuvent se rendre) doit obtenir le consentement des personnes concernées.

Il en est de même pour l'utilisation des « cookies »⁵, dont le but premier est de faciliter la navigation des utilisateurs en évitant, notamment, toute nouvelle saisie d'informations telles que des produits placés dans un panier virtuel, des identifiants de connexion ou des préférences de navigation. Une seconde fonction peut être attribuée aux cookies en matière de sécurisation de la navigation. Par exemple, le filtrage parental se maintient lors des connexions grâce aux préférences mémorisées par l'intermédiaire des cookies. L'ensemble de ces informations sont des données à caractère personnel qui peuvent également relever de la vie privée et, en tant que telles, sont protégées par la loi⁶. Le responsable du traitement doit donc informer de manière claire et complète la personne concernée par le stockage de ces informations de la finalité de ce stockage.

À retenir

En tant qu'acteur et utilisateur de l'ensemble des outils numériques, des objets connectés et plateformes de communication, il revient à chacun d'être vigilant sur l'ensemble des informations qu'il communique, de donner son consentement avant toute utilisation et/ou transfert à des entreprises tierces de ses données, d'identifier la finalité du traitement, de ne pas hésiter à renoncer à communiquer les données et de ne pas utiliser le service proposé s'il le juge préférable. ■

3 - Commission nationale informatique et liberté.

4 - Les données sensibles relèvent de l'origine raciale ou ethnique, des opinions politiques, philosophiques ou religieuses, de l'appartenance syndicale, de la santé ou de l'orientation sexuelle.

5 - Les cookies sont des petits fichiers « .txt » installés sur le disque dur du terminal de connexion, en général dans le dossier Temporary Internet Files, à la demande du site consulté par un navigateur.

6 - L'ordonnance du 24 août 2011 transpose le Paquet Télécom, issu de la directive européenne 2009/136 du 25 novembre 2009 modifiant l'article 32-II de la loi Informatique et libertés n° 78-17 du 6 janvier 1978 modifiée.