Données personnelles : ce que le règlement européen va changer

Le règlement sur la protection des données des résidents de l'UE entre en vigueur. Il expose les entreprises du Net à de lourdes sanctions financières.

Par Laurence Neuer

Modifié le 25/05/2018 à 06:37 - Publié le 08/02/2018 à 06:10 | Le Point.fr

La Commission européenne à Bruxelles. Le règlement unique renforce les droits des consommateurs de l'Union.

À partir de ce vendredi 25 mai 2018, le règlement général sur la protection des données des résidents de l'UE (RGPD) est applicable. Il impacte l'ensemble des acteurs proposant des biens et services sur le marché européen, du micro-entrepreneur au grand groupe, en passant par les associations et les organismes publics. L'enjeu est de taille : ce règlement, qui vient renforcer la maîtrise des utilisateurs sur leurs données, « repose sur une logique de responsabilité et de transparence » résume la Cnil (Commission nationale de l'informatique et des libertés) sur son site.

Elle se montre néanmoins rassurante à l'égard des retardataires : « Pour ce qui est des nouvelles obligations ou des nouveaux droits résultant du RGPD (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes dans une courbe d'apprentissage vers une bonne compréhension et la mise en œuvre opérationnelle des textes. » Comment vont se traduire ces nouveaux droits et obligations ?

Le fichier des salariés d'une entreprise

L'employeur n'a pas à demander l'accord des salariés pour traiter leurs données. Il devra désormais les informer de l'existence d'un « traitement » et des données concernées. « Jusqu'à présent, cette obligation n'était quasiment jamais respectée, elle est désormais généralisée et lourdement sanctionnée puisque l'amende peut aller jusqu'à 4 % du chiffre d'affaires de

l'entreprise », précise l'avocat Marc-Antoine Ledieu, associé du cabinet Bardehle Pagenberg. Ce n'est pas tout : l'employeur devra aussi indiquer à ses salariés sur quel fondement légal il traite leurs données. « Le RGPD prévoit plusieurs bases juridiques possibles, en l'occurrence, pour le fichier des salariés, la base adéquate pourrait être *l'exécution d'un contrat* (de travail) et *le respect d'une obligation légale* (qui consiste dans la transmission de ces informations aux caisses de retraite, d'assurance maladie, etc.). Dans les deux cas, il s'agira d'un traitement de données personnelles sans consentement préalable, mais avec une information préalable obligatoire », ajoute l'avocat.

L'information des salariés porte aussi sur les droits dont ils disposent, à commencer par leur droit d'accès aux données. « Le salarié pourra exiger de son employeur qu'il lui adresse une copie intégrale de ses données », prévient Me Ledieu. Et ce document devra préciser la nature des données traitées, la finalité du traitement, la durée de conservation des données, leur localisation, etc.

- **Moyen de pression**

Le salarié dispose d'un droit de rectification et d'un droit d'opposition à la prospection et au profilage. « Il peut s'opposer à tout traitement de données qui n'est pas destiné à la gestion de son contrat de travail et de sa carrière dans l'entreprise, par exemple un *scoring* de profilage pour l'évaluation de ses performances professionnelles. Cet article 21 du RGPD est un véritable tremblement de terre pour les entreprises qui ont l'obligation d'effacer la partie du traitement des données que le salarié refuse », souligne Me Ledieu. Par ailleurs, les données sensibles qui, par exemple, révèlent l'origine raciale, les convictions religieuses philosophiques ou l'orientation sexuelle des salariés, ne peuvent faire l'objet d'aucun traitement, sauf consentement « explicite » des personnes concernées, précise le règlement.

Et si le RGPD devenait une arme ou un moyen de pression juridique en cas de conflit avec l'entreprise ? « C'est déjà le cas, relève François-Pierre Lani, avocat associé au cabinet Derriennic Associés. Il arrive que des salariés invoquent, souvent avec succès, la non-conformité des éléments de preuve issus de fichiers non conformes à la loi informatique et libertés pour faire rejeter les arguments de l'employeur qui refuse de payer leurs heures supplémentaires. En prévision du RGPD, des entreprises commencent à recevoir de la part de salariés, de syndicats et d'institutions représentatives du personnel, des demandes de notification de la conformité de l'entreprise au RGPD. Elles portent, par exemple, sur les outils qui seront mis en place pour faire valoir leurs droits d'accès et de rectification. »

Le cas de fichiers clients traités par les plateformes de vente en ligne

Les sites marchands qui traitent les données postales et bancaires des acheteurs n'ont pas à leur demander leur accord préalable s'agissant, en principe, d'un « *traitement de données nécessaire à l'exécution d'un contrat* » (de vente, de service, etc.). « L'entreprise doit néanmoins informer ses clients de l'existence d'un tel traitement et leur notifier leur droit d'accès et de rectification de leurs données, ainsi que leur droit d'opposition à prospection et profilage, note Me Ledieu. Mais attention, dès lors que mon fournisseur de shampoing veut me vendre des algues pour le bain, je redeviens son *prospect*, ce qui implique un nouveau traitement de données basé par exemple sur *les intérêts légitimes de l'entreprise* (autre fondement légal sans consentement préalable). Ce concept anglo-saxon, repris dans le RGPD, autorise la prospection commerciale sans le consentement des intéressés, jusqu'à l'exercice du droit d'opposition du prospect. Cela vaut bien sûr pour nous, avocats qui adressons des newsletters à nos clients. »

L'internaute devra néanmoins être en mesure de s'opposer au traitement de ses données (via un lien de désabonnement pas exemple). Si tel est le cas, l'entreprise devra effacer immédiatement les données de prospection de sa base de données. « Les entreprises vont devoir effacer beaucoup de données, mais ce n'est qu'à cette condition que la confiance avec les consommateurs pourra se recréer, assure l'avocat. Dès lors que l'entreprise abordera les consommateurs en disant « *Cher prospect, si vous acceptez de recevoir mes offres et mes conseils, cochez la case « oui* ». *En échange du traitement de vos données, vous aurez un contenu personnalisé. Le jour où vous souhaitez que cela cesse, il vous suffit de vous désabonner* », alors tout ira mieux ! »

Fini l'affichage personnalisé imposé

Comment les sociétés qui pistent l'internaute dès que sa souris s'aventure sur l'écran, et qui utilisent ses données de navigation pour le profiler et lui faire des « recommandations » vont-elles redresser le tir ? Le traitement de ces données de navigation peut être « nécessaire aux intérêts légitimes de l'entreprise », dit le RGPD, soucieux de préserver l'équilibre entre les nécessités du commerce et les droits des personnes. Mais ces dernières doivent avoir la possibilité de refuser ces recommandations et l'entreprise devra respecter ce choix. Autrement dit, « le *prospect* se verra proposer des recommandations ou des publicités, mais celles-ci ne pourront pas prendre en compte les *data*qui permettent de les personnaliser. Ce sera alors de l'affichage *standard et générique*, comme les publicités sur les panneaux d'affichage dans les rues », explique Me Ledieu.

Moteurs de recherche

Nombre d'internautes s'interrogent sur la façon dont les rois de la « data » comme Google ou Facebook vont appliquer le RGDP. Google et Facebook sont actuellement poursuivis (notamment) par L'UFC que choisir pour non-respect de la loi informatique et libertés. L'association de défense des consommateurs leur reproche d'entretenir leurs utilisateurs dans un flou artistique quant aux clauses relatives à l'utilisation de leurs données et aux ciblages qui en découlent. « Par la seule utilisation du service, on adhère à des règles dont on n'a pas conscience. L'internaute autorise le moteur de recherche ou le réseau social, par le jeu des cookies, à le cibler et à revendre ses données de navigation à des sociétés qui font de la publicité sur Internet, souligne Me Lani. Je vous mets au défi d'aller trouver dans le service Google les options de confidentialité que Google assure avoir mis en place pour circonscrire l'exploitation de nos données ! »

En clair, la plateforme a encore de grands efforts à fournir pour devenir RGPD compatible. « Elle devra permettre à l'internaute d'effacer facilement toutes les traces laissées durant la navigation, et mettre en place des outils simples et accessibles pour faire valoir son droit d'opposition au profilage, etc. », précise Me Lani.

Les grandes lignes du règlement

- Principe de minimisation : la collecte des données doit se cantonner au strict nécessaire. Exemple : un vendeur de produits cosmétiques n'a pas à savoir si son client est un amateur de séries télévisées.

- Recueil du consentement de l'utilisateur (dans les cas où il est obligatoire, par exemple pour le recueil de données sensibles) : il doit être effectué par type d'usage et non de manière globale. Le consentement recueilli doit être explicite.

- Mise en place d'outils permettant à l'utilisateur d'exercer son droit d'accès aux données, son droit de les rectifier, son droit de s'opposer à certains types de traitements (profilage par exemple), son droit à la portabilité des données, qui lui permet de récupérer toutes les données communiquées à une plateforme (réseau social, site marchand, site de streaming…) soit pour les conserver, soit pour les transférer vers autre opérateur (une autre application par exemple).

- Privacy by design : l'entreprise doit dans la mesure du possible intégrer la protection de la vie privée dès la conception du logiciel ou du service et mettre en place les outils adéquats pour préserver la liberté de choix de l'utilisateur : possibilité de cocher ou décocher la géolocalisation dans un smartphone, bouton sur une enceinte connectée signalant qu'elle est allumée et enregistre les conversations…

- Accountability ou auto-responsabilisation : il appartient à l'entreprise de prendre toutes les mesures nécessaires pour remplir ses obligations de protection des données, et être capable de le démontrer à tout moment. À cet effet, elle devra tenir un registre recensant les catégories de données traitées, les finalités du traitement, les pays où elles sont transférées, la durée de conservation, etc. Les entreprises qui, notamment, traitent des données à grande échelle devront désigner un délégué à la protection des données (DPO) dédié au contrôle de la conformité au GDPR. « Ce dernier va, par exemple, s'assurer que le DRH n'a pas conservé des fichiers de CV datant de plus de 2 ans ou que le système de pseudonymisation des données est effectif », explique l'avocat Gérard Haas, auteur de « Le RGPD expliqué à mon boss » (Éditions Kawa).

- Security by default : l'entreprise doit prendre les mesures nécessaires pour sécuriser les données, « notamment par le chiffrement ou la pseudonymisation. Elle doit aussi mettre en place des outils de détection de failles de sécurité, car elle a l'obligation de notifier ces failles à la personne

concernée et à la Cnil », précise François-Pierre Lani. Elle doit aussi être en mesure de déceler les failles affectant ses fichiers.

- Droit à l'oubli numérique : le droit à l'effacement des données est le pendant du droit au déréférencement d'une information ou d'un lien par un moteur de recherche. La personne peut s'adresser directement au responsable de traitement dans le cas, par exemple, où l'entreprise a conservé ses données plus longtemps que nécessaire au vu des finalités annoncées. « Ce droit à l'effacement n'est pas absolu, par exemple, un salarié ne peut pas exiger de son ancien employeur qu'il efface ses données immédiatement après son départ, ce n'est qu'au bout de 5 ans qu'il doit les avoir purgées pour les traitements de la paie ou le contrôle des horaires », nuance Me Lani.

- Réparation des dommages et class action : Les associations dédiées à la protection des données pourront introduire des recours collectifs. L'objectif est de faire cesser le dommage causé par la violation du règlement. Un amendement examiné actuellement au parlement prévoit d'y ajouter la réparation du préjudice des personnes concernées.

- Étude d'impact : cette obligation concerne les entreprises qui peuvent être amenées à traiter des volumes de données en masse, par exemple les fabricants des technologies des voitures autonomes. « L'objectif est d'évaluer l'impact d'un système innovant sur les données personnelles des personnes concernées. Par exemple, des caméras placées dans le véhicule autonome vont photographier les piétons, les plaques d'immatriculation, etc. qui sont des données personnelles. L'étude va prendre en compte l'interdiction de collecter ces données et proposer des moyens techniques, voire juridiques pour adapter le système. Par exemple, indiquer à quel moment on floute le visage des piétons », explique Me Lani.

- Des amendes dissuasives en cas de manquement : l'entreprise encourt, selon le manquement constaté, jusqu'à 2 % ou 4 % du chiffre d'affaires mondial de l'entreprise dans la limite de 10 ou 20 millions d'euros.

- Cette réglementation s'appliquera à toutes les entreprises, quel que soit l'endroit où elles se trouvent dans le monde, dès lors qu'elles traitent des données de personnes résidant sur le territoire européen. Les Gafam (Google, Amazon…) ne peuvent donc s'y soustraire.

À savoir : la Cnil fournit un certain nombre d'outils pratiques pour accompagner les entreprises dans leur mise en conformité