LE RGPD : un enjeu pour la responsabilité sociale de l'entreprise

Par Carla Di FAZIO PERRIN, Avocat associée, Cabinet Racine

Avec 4 milliards d'utilisateurs réguliers, Internet est la plus grande base de données au monde ! Numéro de carte bancaire, nom, prénom, adresse, âge, localisation, etc. L'appropriation de ces données se fait parfois à leur insu. En effet, les internautes n'ont, la plupart du temps, pas conscience de l'utilisation et du devenir de ces données. A l'ère du numérique, le Règlement Général sur la Protection des Données Personnelles (RGPD) peut être l'occasion de reprendre la maîtrise des données personnelles et de sensibiliser les individus sur leur valeur. Ces données constituent aujourd'hui un bien ayant une valeur commerciale importante.

Le RGPD, entré en vigueur le 25 mai 2018, offre un cadre juridique unifié au sein de l'Union européenne pour la collecte et l'utilisation des données personnelles. En France, le projet de loi sur la protection des données personnelles, adopté définitivement par le Parlement le 14 mai 2018, adapte la loi Informatiques et Libertés (*loi n°78-17 du 6 janvier 1978*) afin de tenir compte des principes posés par le règlement.

Malgré l'absence de dispositions spécifiques concernant le droit du travail, le RGPD et le projet de loi ont une influence directe sur la vie du salarié et de l'entreprise. L'employeur sera, tout au long de leur carrière dans l'entreprise, responsable du traitement des données des salariés et devra être à même de justifier comment et pourquoi il recueille, conserve et utilise les données liées à la procédure de recrutement ou à la gestion du personnel.

C'est pourquoi la mise en conformité de l'entreprise aux dispositions du RGPD doit devenir une priorité de la politique sociale de l'entreprise. En effet, la sensibilisation des individus à la confidentialité et la sécurité de leurs données personnelles amènera de plus en plus les salariés à exiger de leur employeur d'être transparent sur ce point.

La responsabilisation des entreprises

En vertu de l'article 4 du RGPD, les données personnelles sont constituées par «*toute information se rapportant à une personne physique identifiée ou identifiable*».

Le responsable de traitement de ces données, c'est-à-dire «*la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*», doit définir dès la conception du traitement («*privacy by design*») puis mettre en œuvre à tout moment, les mesures techniques et organisationnelles nécessaires pour assurer la conformité des traitements qu'il opère et pouvoir le démontrer en cas de contrôle par une documentation adéquate («*accountability*»).

Ainsi, la principale innovation du RGPD est de faire disparaître la majorité des formalités préalables (autorisations, déclarations) imposées par l'ancienne directive 95/46/CE du 24 octobre 1995 et d'y substituer une logique de conformité qui responsabilise les entreprises.

Le responsable de traitement doit donc être capable de démontrer à tout moment que les données à caractère personnel sont :
- traitées de manière licite, loyale et transparente au regard de la personne concernée ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- exactes et, si nécessaire, tenues à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (*article 5 du RGPD*).

En France, la Commission Nationale de l'Informatique et des Libertés (CNIL) accompagne les entreprises vers la mise en conformité au RGPD. La première étape conseillée par la CNIL est de constituer un registre des traitements de données afin d'avoir une vision d'ensemble et de recenser tous les fichiers de l'entreprise. Cette étape, bien que rendue obligatoire par le RGPD uniquement pour les entreprises de plus de 250 salariés, est conseillée par la CNIL à toutes les entreprises.

A partir de ce registre, les entreprises peuvent trier les données afin d'en minimiser la collecte et d'éliminer les données inutiles. Enfin, les obligations d'information, de transparence et de sécurisation à l'égard des personnes dont l'entreprise traite les données doivent être renforcées. Egalement, les entreprises dont l'activité amène à réaliser un suivi régulier et systématique des personnes ou à traiter, à grande échelle, des données dites sensibles ou relatives à des condamnations pénales et infractions, doivent désigner un délégué à la protection des données (DPO).

L'employeur comme garant de la protection des données

L'employeur, notamment au travers du service des ressources humaines, collecte, traite et conserve des données personnelles lors du recrutement, pendant la relation de travail et même une fois que la relation de travail a pris fin. Il en est ainsi des documents tels que curriculum vitae, fiches de paie, arrêt maladie, congé maternité, certificat de décès, permis de conduire, photographies, etc. Or, en 2016, 14% des plaintes déposées auprès de la CNIL concernaient le service des ressources humaines.

Par conséquent, la protection des données doit dorénavant constituer un enjeu de la stratégie de responsabilité sociale de l'entreprise. L'employeur doit en assurer la sécurité et la confidentialité ainsi que garantir une transparence accrue envers les salariés, ces derniers devant être à même d'exercer leurs droits.

L'employeur doit ainsi mettre en place des processus permettant de s'assurer que le salarié est informé, qu'il a donné son consentement pour la collecte des données et qu'il pourra en demander l'effacement et le transfert.

L'entreprise peut également aller plus loin que la réglementation, en participant à un enjeu éthique : faire prendre conscience à chaque utilisateur des risques en matière de sécurité et de vie privée. L'employeur pourra ainsi sensibiliser les salariés à la question des données personnelles.

Renforcement des sanctions administratives

Comme auparavant, la CNIL assurera en France le respect du traitement des données personnelles. En cas de non-respect des obligations imposées par le RGPD, le responsable du traitement s'exposera à diverses sanctions administratives : avertissement, mise en demeure, injonction de cesser le traitement, suspension des flux etc. L'amende administrative peut désormais s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel mondial de l'exercice précédent.

De surcroît, les sanctions civiles et pénales peuvent toujours être appliquées. Tout manquement à la législation peut faire l'objet tant d'une action individuelle que d'une action collective en réparation du préjudice subi à l'encontre du responsable du traitement. Les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques constituent également un délit pénal passible d'une peine d'emprisonnement et d'une amende, multipliée par 5 pour les personnes morales (*articles 226-16 à 226-24 Code pénal*).

Risque médiatique

Outre les sanctions évoquées ci-dessus, un autre risque, plus immédiat pèse sur l'entreprise : celui de l'atteinte à l'image. De nos jours, l'opinion publique peut se mobiliser très rapidement, par exemple en relayant par les réseaux sociaux et les médias des propos tenus dans diverses émissions télévisées, poussant ainsi la majorité des marques à cesser de sponsoriser lesdites émissions. En effet, les internautes étant de plus en plus sensibles à la protection de leurs données, l'entreprise qui ne les protégerait pas, s'expose à des retombées médiatiques négatives.

La CNIL publie les mises en demeure et les sanctions sur son site internet afin d'en informer les internautes.

Récemment, WhatsApp a été mis en demeure par la présidente de la CNIL dans le cadre de la transmission à Facebook des données des utilisateurs à des fins de «*business intelligence*» sans les en avoir informés au préalable.

Direct Energie a également été mis en demeure en raison de l'installation de compteurs permettant de récolter des données de consommation régulière sans le consentement des consommateurs.

Enfin, Darty a été sanctionné par une amende de 100.000 euros par la CNIL : une défaillance de sécurité permettait d'accéder librement aux données renseignées par les clients via le formulaire en ligne de demande de service après-vente (*délibération de la formation restreinte n°SAN-2018-001 du 8 janvier 2018*).

Les condamnations qui sont rendues publiques par la CNIL, puis relayées par la presse ainsi que par les réseaux sociaux, peuvent inciter les consommateurs à une plus grande méfiance à l'égard des entreprises sanctionnées.

Ainsi, il existe un paradoxe entre l'utilisation des données faites par les individus et celle que peut en faire l'entreprise. En effet, si chaque individu est personnellement responsable de ses données personnelles et libre de les monétiser, l'entreprise, en tant qu'employeur, ne peut pas conférer de valeur marchande aux données collectées. Elle doit donc faire preuve d'une éthique irréprochable et d'une responsabilité plus importante que celle dont font preuve les individus eux-mêmes, souvent peu conscients de l'importance de leurs données personnelles et des risques associés à leur divulgation.

La responsabilité sociale de l'entreprise doit tenir compte de cette situation, en assurant une protection accrue des données personnelles, qui sera en outre une garantie pour les partenaires et les clients de l'entreprise.

SGG Crossroads with Sir Bob Geldof

Sir Bob Geldof (picture), Gina Miller, Nev Hyman, Patrick Scheurle and other prestigious speakers will be in Luxembourg for a prestigious event on the topic: Can the finance industry contribute to a better society?

SGG, a leading global investor services firm is organizing an exclusive event on 26th June 2018 in Luxembourg.

The objective is to bring together key decision makers and international asset managers and their advisors to exchange on how the industry can create a better society, and to stimulate new ideas on how to promote sustainability within the industry.

"Together with our sponsors Carne, Deloitte, Baker McKenzie and ING, we wanted to show the positive contribution of the finance industry on the society in general and also inspire finance professionals with the outstanding initiatives of our guest speakers." said Serge Krancenblum, Group CEO SGG Group.

Programme

Moderated by Yuri Bender from Financial Times, speakers are:
- **Sir Bob Geldof:** Member of the Africa Progress Panel, which advocates for equitable and sustainable development in Africa, and adviser to the ONE CAMPAIGN.
- **Gina Miller:** Founder of Fund Manager, SCM Direct, transparency activist and campaigner for Parliamentary sovereignty over Brexit, who also champions conscious capitalism and the principle of a triple bottom line.
- **Nev Hyman:** Award-winning entrepreneur and Founder of NevHouse, sustainable social enterprise, which uses recycled plastic to create low cost homes, schools and medical clinics.
- **Patrick Scheurle:** Chief Executive Officer of BlueOrchard, a leading global impact investment manager. Patrick is a published writer in the fields of finance and impact investing and the co-author of the bestseller "Small Money – Big Impact" published by NZZ Libro Verlag.
- **Roger Hartmann:** Member of the supervisory boards of Sqope SA, the leading AML reputation firm, and of Label R, the unique global ESG certification for funds investing in sensitive zones.
- **Myriam Vander Elst:** Vice President and head of Europe at Epic. Myriam Vander Elst is a social-good advocate and an expert in impact-oriented philanthropic strategies. Working closely with Epic's Founder and CEO, the French serial entrepreneur Alexandre Mars, Myriam leverages impact and giving solutions for individuals and corporations to support high-impact social organizations. Known as the Epic Portfolio, that highly-vetted selection of organizations tackles youth and children issues globally. With these solutions, Epic aims to disrupt the philanthropic market and provide a more transparent experience of giving.
- **Itzik Amiel:** is a global leading authority on Networking, Personal Branding & Relationship Capital, an international speaker, bestselling author and Attorney-at-law. He is the founder and CEO of THE SWITCH®. on Leadership™. His signature focus on business success through the ability to sustain strong relationships with other people - be it customers, stakeholders, colleagues and the wider community for whom we also create value.
- **Roelfien Kuijpers:** Member of DWS Executive Committee, Roelfien is also a member of the Board of Directors of the Deutsche Bank Americas Foundation and chairs its Investment Committee. In addition to being a strong supporter of women and diversity in the company, she is also a member of the Women's Leadership Board at Harvard University's Kennedy School of Government.
- **MODERATOR: Yuri Bender - Financial Times**

Yuri Bender is a financial journalist focusing on private banking, international asset management and capital markets. He has edited and launched a variety of titles at the Financial Times group and is currently Editor-in-Chief of the Professional Wealth Management pan-European and Asian magazine, website and events hub.

More information : www.sggcrossroads.com or contact Patrick Sampaio : relations@360crossmedia.com