Une protection des données personnelles uniforme dans toute l'Union européenne

LE RÉSUMÉ

Le Règlement général sur la protection des données (**RGPD**) **est en vigueur**.

Il prévoit une **protection stricte des données personnelles** des particuliers.

Des **plaintes pourront être adressées à l'Autorité de protection des données**. Qui n'est pas encore prête...

PHILIPPE GALLOY

Le Règlement général sur la protection des données (RGPD) entre en vigueur ce vendredi. Cette réglementation européenne s'applique dans une trentaine de pays (les vingt-huit États membres de l'Union européenne, plus l'Islande, le Liechtenstein et la Norvège). Dès aujourd'hui, un demi-milliard de personnes bénéficient ainsi de cette nouvelle législation applicable à tous ceux qui les «suivent».

Ce texte légal vise à protéger les personnes physiques au point de vue du traitement de leurs données personnelles. Tous les pays européens avaient des législations en la matière mais ces anciens textes ne tenaient pas compte de l'évolution récente des technologies et de la mondialisation. L'essor des réseaux sociaux, des moteurs de recherche ou encore des applications mobiles a changé la donne: les entreprises technologiques ont de l'avance par rapport à ces normes désormais dépassées.

La Commission européenne a donc actualisé et uniformisé la protection des données des particuliers. *«Le règlement vise à contribuer à la réalisation d'un marché digital européen homogène, régulé par un règlement unique appliqué par des autorités de protection des données qui communiquent, coopèrent et mènent des actions conjointes»*, explique l'avocat Christophe Boeraeve (Law Right), spécialiste du droit de la propriété intellectuelle et des technologies de l'information. *«Chaque citoyen européen, et même toute personne concernée de n'importe quel pays – client, prospect, partie à une convention ou travailleur – peut donc directement invoquer le règlement et sa protection accrue.»*

Quelles règles, en pratique?

Concrètement, le RGPD s'applique à chaque responsable du traitement de données, c'est-à-dire toute personne physique ou morale, autorité publique, tout service ou autre organisme qui détermine les finalités et les moyens du traitement des données à caractère personnel.

Selon le règlement, le traitement des données doit être transparent vis-à-vis des personnes concernées. Cette transparence implique qu'un langage clair et compréhensible doit être utilisé au moment d'informer le particulier de la manière dont ses données seront traitées. Pas question d'un jargon juridique en petits caractères: il faudra que les particuliers puissent comprendre facilement ce qu'il adviendra de leurs données.

Le traitement doit être licite, c'est-à-dire que ces personnes doivent avoir consenti de manière Spécifique, Éclairée, Univoque et Libre (SEUL) au traitement de leurs données pour une finalité spécifique. Le consentement devra pouvoir être retiré aussi facilement qu'il a été donné (et par la même voie).

Des données à caractère personnel ne peuvent être collectées que pour une finalité déterminée et cette collecte doit être strictement limitée aux données nécessaires au but recherché. Par exemple, si un consommateur s'enregistre sur le site d'une société de livraison à domicile, celle-ci peut réclamer qu'on lui communique une adresse – nécessaire pour la livraison – mais ne peut pas exiger de connaître la profession du client ou sa date de naissance.

Les données ne peuvent être conservées que pour une durée nécessaire au regard de la finalité poursuivie. Dans notre exemple, si l'entreprise arrête son activité de livraison ou si la personne cesse d'être cliente, il n'y a plus de raison de conserver les données. Les données doivent être exactes, sans quoi il faut mettre en œuvre – et ce, activement – toutes les mesures raisonnables pour les rectifier. Il faut aussi garantir la sécurité des données: tout doit être mis en œuvre pour éviter une violation des données.

Tout responsable du traitement doit pouvoir démontrer le respect de ces règles. Il doit pouvoir prouver à tout moment que la personne concernée a donné son consentement au traitement de ses données.

Lourdes sanctions

En outre, un nouveau droit est institué: le droit à la portabilité. Il permet de récupérer les données personnelles et de les transférer à un autre responsable du traitement, par exemple, un autre fournisseur de service.

Le règlement prévoit aussi que le traitement des données d'un mineur de moins de 16 ans n'est possible qu'avec le consentement de la personne qui exerce l'autorité parentale sur celui-ci. Les responsables du traitement doivent fournir des efforts raisonnables pour vérifier l'âge de l'enfant.

Les entreprises, associations et autres avaient jusqu'à ce vendredi pour se mettre en conformité avec le RGPD. En cas de manquement, de lourdes sanctions sont prévues: jusqu'à 20 millions d'euros d'amende, montant qui peut monter à 4% du chiffre d'affaires mondial pour les multinationales coupables d'un grave manquement.

En Belgique, l'Autorité de protection des données (APD) doit veiller au respect du RGPD. Mais cette instance qui doit remplacer la Commission de la protection de la vie privée (CPVP) n'est pas encore prête... Alors que la CPVP n'a qu'une compétence d'avis, la future APD aura un pouvoir de sanction. Ses décisions seront susceptibles de recours devant la cour d'appel.

Où porter plainte?

Le RGPD fait peser une obligation de sécurité sur les responsables du traitement des données (entreprises, associations, et autres) ainsi que leurs sous-traitants. Des mesures de protection renforcées doivent être prévues pour les données sensibles, comme par exemple les informations relatives à la santé ou l'orientation sexuelle ou encore l'appartenance syndicale. Toute entreprise ou organisation confrontée à un v (i) ol de données est tenue de le signaler à l'APD dans un délai de trois jours.

Il faudra en outre tenir un registre des données, sauf dispense pour les entreprises de moins de 250 employés. Puisqu'il est indispensable de cartographier ces données, les autorités de contrôle recommandent à toute organisation de tenir un tel registre.

Les particuliers pourront adresser à l'APD des plaintes sur le traitement de leurs données personnelles. Encore faudra-t-il que le service de première ligne de l'Autorité juge ces plaintes recevables. L'APD aura par ailleurs une compétence d'avis et de recommandation sur tous les sujets ayant des implications en matière de traitement des données personnelles.

Pour gérer toutes les questions liées à la protection des données, les entreprises et autres organisations doivent désigner un délégué à la protection des données (DPD) ou data protection officer (DPO). Cette personne est l'interface entre le responsable de traitement des données (entreprise, association, etc.), les personnes concernées (particuliers dont les données sont traitées) et les autorités de contrôle (l'APD, en l'occurrence).

Pour se conformer au RGPD, le monde des entreprises – mais aussi celui des organismes à profit social – a mis les bouchées doubles. D'où des frais de consultance, d'avocats, de services informatiques, etc. Qui paiera l'addition? Dans la plupart des cas, ce coût sera répercuté sur le consommateur... Par exemple, dès 2017, Securitas a augmenté ses prix, une hausse que la société de services de gardiennage justifie notamment par une *«adaptation des coûts afin de respecter la législation relative au Règlement général sur la protection des données»*. C'est le prix à payer pour que nos données soient mieux protégées.