PAR
NOËLLE LENOIR
ANCIENNE MINISTRE,
AVOCATE ASSOCIÉE
AU BARREAU DE PARIS
(KRAMER LEVIN)

La protection des données personnelles, nouveau champ de conformité pour les entreprises

De plus en plus d'entreprises sont aujourd'hui conscientes de l'urgence de se préparer à l'entrée en vigueur du Règlement européen du 27 avril 2016 sur la protection des données personnelles. Le compte à rebours en effet est enclenché : il reste à peine un an avant que le Règlement ne soit applicable, très exactement à compter du 25 mai 2018. Or les changements qu'il induit dans la gestion des données, et plus largement des entreprises, sont considérables.

Le ministère de la Justice, dont c'est la compétence, s'est attelé à la rédaction d'un projet de loi modifiant la loi Informatique et Libertés devenue inadaptée.

Rappelons cependant que le Règlement est d'applicabilité directe (contrairement aux directives qui nécessitent une transposition en droit national) et qu'à défaut d'adoption dans les délais de la nouvelle loi française, ses dispositions seront opposables dans tous leurs effets. Certaines de ces dispositions sont, il faut le reconnaître sinon obscures, du moins difficiles à interpréter, et il faut donc espérer que le législateur français sera diligent.

Les entreprises et les associations qui les représentent doivent songer à cet égard à faire valoir leurs vues lors des débats parlementaires.

• ***Sur le fond***, il est d'abord important de comprendre en quoi le Règlement constitue une véritable rupture par rapport à la législation actuelle, à savoir la directive du 24 octobre 1995 dont les dispositions sont reflétées dans la loi Informatique et Libertés modifiée en 2004.

• ***Du point de vue des initiatives à prendre*** par les entreprises et les entités qui les composent, c'est à la mise en œuvre d'un plan d'actions coordonnées que nous invite le législateur européen.

A défaut, l'entreprise s'exposera aux risques importants de sanctions, d'actions contentieuses et de dommages financiers et réputationnels qu'impliquera le non-respect du Règlement ; sans parler même des sanctions pénales pour violation de la vie privée.

EN QUOI LE RÈGLEMENT INTRODUIT UNE RUPTURE PAR RAPPORT À LA LÉGISLATION ACTUELLE ?

L'encadrement juridique de la protection des données personnelles

L'esprit même de l'encadrement juridique de la protection des données personnelles est profondément modifié en ce sens que le Règlement supprime (sauf en matière de transfert de données à l'extérieur de l'Union européenne) les formalités préalables jusqu'ici requises (déclarations, déclarations de conformité à une « norme simplifiée », ou encore autorisations).

En contrepartie, il instaure un système d'autocontrôle par les entreprises de la façon dont elles assurent la protection des données personnelles, que ce soit dans le cadre de leurs activités économiques (fournisseurs, clients, prospects, banques etc.) ou pour leurs besoins internes (fichiers de personnel, de visiteurs, etc.)

Pour prendre un exemple concret, actuellement, une autorisation préalable de la CNIL est obligatoire pour les fichiers enregistrant des données sensibles (santé, appartenances syndicales, biométriques…). Cette autorisation ne sera plus exigée, mais l'entreprise responsable du traitement aura à réaliser une « étude d'impact » visant à s'assurer de l'efficacité des mesures de protection de ces données et à défaut, à renforcer ces mesures. On passe ainsi d'un système de contrôle ex-ante à un système de contrôle ex-post renvoyant à des exigences accrues en matière de conformité.

La portée territoriale des règles européennes

La deuxième différence fondamentale entre le Règlement et la directive de 1995 a trait à la portée territoriale des règles européennes. Pour la première fois, une législation européenne est clairement extraterritoriale.

La directive de 1995 s'applique en fonction de la localisation des moyens informatiques (ordinateurs, terminaux, serveurs…) de sorte qu'une entreprise hors de l'UE peut traiter des données sur les citoyens européens sans autre contrainte légale que celle de son pays d'origine.

Le Règlement s'appliquera à toutes les entreprises traitant des données personnelles où que ce soit dans le monde pour peu qu'il s'agisse d'activités de traitement liées à l'offre de biens et services (activités commerciales) ou au suivi du comportement au sein de l'UE de la personne concernée (ex. prospects).

Les incidents devront être notifiés

Autre changement notable : Les incidents, quelle qu'en soit la cause accidentelle ou intentionnelle, ayant conduit à la violation de données personnelles devront être notifiés – si possible dans les 72 heures – à la CNIL, alors qu'actuellement, cette notification n'est obligatoire que pour les entreprises du secteur des communications électroniques.

Les personnes concernées devront en principe être informées de l'incident. Par ailleurs, la loi du 8 août 2016 sur la modernisation de la justice du XXIe siècle a ouvert la voie à d'éventuelles « *class actions* » des personnes lésées, dans des conditions toutefois plus restrictives qu'aux Etats-Unis.

La montée en puissance des autorités de protection des données constituées en réseau

Enfin et en dernier lieu, comme c'est le cas dans le domaine financier, on assiste à la montée en puissance inexorable des autorités de protection des données désormais constituées en réseau.

Elles sont appelées à coopérer, par exemple en cas d'enquête sur un responsable de traitement opérant dans plusieurs pays européens.

Plus encore, le Règlement transforme le fameux « Groupe de l'article 29 » réunissant les autorités de contrôle nationales et qui est purement consultatif, en un « Comité européen de protection des données » dont les avis peuvent être contraignants.

Même si l'entreprise aura à faire à un guichet unique, à savoir l'autorité du pays où elle a son siège ou son établissement principal (en France, la CNIL), cette autorité, en cas de traitement transnational, travaillera conjointement avec ses homologues européens afin de dégager une position commune face à un problème particulier.

L'autorité chef de file proposera une mesure soumise aux autorités homologues. Si celles-ci ne sont pas d'accord avec la proposition, il reviendra au Comité européen de protection des données de rendre un avis contraignant. *Last but not least*, les autorités de contrôle, et donc la CNIL, pourront infliger des amendes administratives allant jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise.

COMMENT SE PRÉPARER POUR NE PAS S'EXPOSER AU RISQUE DE SANCTIONS ?

Comme en toute matière, pour savoir ce qu'il faut faire, il faut pouvoir évaluer ce que l'on a fait.

Procéder à l'inventaire exhaustif et précis de l'ensemble des traitements de données personnelles

Suivant ce principe de bon sens, la première étape à franchir par les entreprises est de procéder à l'inventaire exhaustif et précis de l'ensemble des traitements de données personnelles mis en œuvre au sein du groupe et de ses différentes entités.

Cet inventaire doit conduire à l'élaboration d'une cartographie des données indiquant leur nature (identification des données), la finalité du traitement (pour respecter le principe de « minimisation » obligeant à ne collecter que les données nécessaires à la finalité poursuivie), le lieu d'hébergement des données, leur durée de conservation, leurs destinataires et les transferts éventuels à l'extérieur de l'UE.

De manière succincte, il est également nécessaires de lister les mesures de sécurité – organisationnelles (ex. qui a accès aux données, journalisation des accès) et techniques (mots de passe, chiffrement, sauvegardes etc.) – dont les traitements font l'objet.

Réaliser dès maintenant une étude d'impact

Une fois identifiés les traitements comportant des données sensibles au regard du Règlement, il est fortement recommandé, de réaliser dès maintenant une étude d'impact (même

> ***Pour la première fois, une législation européenne est clairement extraterritoriale***

si elle n'est légalement requise qu'à partir du 25 mai 2018) pour évaluer les risques de violation de ces données et pouvoir les réduire au maximum.

En effet, les données sensibles exigent un dispositif de protection renforcé qui devra être tenu à disposition de la CNIL en cas d'audit. L'étude d'impact est aussi utile dans le cadre de l'élaboration d'une cartographie des risques à soumettre au comité d'audit créé au sein du conseil d'administration, s'il en est.

Veiller à se doter de processus de contrôle interne efficaces

Au-delà de cette démarche ponctuelle d'évaluation des risques auxquels peuvent être exposés les traitements de données sensibles, les entreprises devront, veiller à se doter de processus de contrôle interne efficaces.

Il leur reviendra en cas d'incident de démontrer à la CNIL, ainsi qu'aux autorités judiciaires s'il y a lieu, qu'elles avaient pris en compte l'impératif de protection des données « dès la conception » de leurs systèmes d'information (*privacy by design ou by default*). Ceci suppose entre autres que ces systèmes permettent de satisfaire à l'exercice de leurs droits par les personnes concernées : les systèmes d'information doivent intégrer notamment la nécessité de répondre rapidement aux demandes de droit d'accès ou encore de garantir le droit à la portabilité des données (récupération de ses données pour les confier à un autre responsable de traitement).

> ***Le Règlement transforme le « Groupe de l'article 29 » réunissant les autorités de contrôle nationales qui est consultatif, en un « Comité européen de protection des données » dont les avis peuvent être contraignants***

Que ce soit en matière de respect des droits des personnes ou de cybersécurité, les entreprises doivent s'attacher à la revue des contrats qu'elles ont passés avec leurs prestataires de services afin de s'assurer qu'ils couvrent expressément ces obligations.

Le Règlement prévoit que ces contrats doivent comporter les instructions données par le responsable de traitement à son prestataire informatique afin que ce dernier assure le respect de ces obligations.

Contrôler les transferts de données vers des pays « tiers » hors EU

Les transferts de données vers des pays « tiers » hors EU demeurent étroitement contrôlés.

Sauf vers les pays ayant un niveau de protection semblable à celui de l'UE (et désignés comme tels par la Commission européenne), ces transferts restent soumis à autorisation, sous la forme éventuellement d'une adhésion à des clauses contractuelles définies par la Commission européenne.

Les transferts vers les entreprises aux Etats-Unis ayant souscrit au « *Privacy Shield* » sont en revanche libres. De façon générale, les multinationales ont tout intérêt à adopter des « règles contraignantes d'entreprise » à négocier avec la CNIL, car cela leur garantit une libre circulation de leurs données au sein du groupe où que se situent ses différentes entités.

L'élaboration de ces « *binding rules* » demande entre un an et dix-huit mois, mais ce temps est mis à profit pour passer en revue l'ensemble des dispositifs existants de protection des données ; ce qui revient, en quelque sorte, à effectuer l'inventaire qu'elles ont en tout état de cause à faire dans la perspective de l'entrée en vigueur du Règlement.

C'est aussi l'occasion de sensibiliser l'ensemble des personnels dans les filiales et non seulement au siège aux exigences du nouveau texte.

POUR CONCLURE

Pour conclure, notamment dans les secteurs d'activité et dans les domaines où a été poussée très loin la dématérialisation et où le *big data* est d'utilisation courante, c'est toute l'organisation interne de l'entreprise, et non seulement son dispositif de conformité, qui doivent évoluer : la plupart des entreprises ont choisi opportunément d'anticiper sur le Règlement en recrutant celui ou celle qui sera le délégué à la protection des données dont la mission devient centrale et sans commune mesure avec celle des actuels correspondants Informatique et Libertés.

En témoigne le fait que, à l'instar du directeur financier, le délégué « fait directement rapport au niveau le plus élevé de la direction » de l'entreprise (article 38 du Règlement). Ce qui ne signifie pas que le délégué ait compétence exclusive.

La conformité, en matière de protection des données comme en toute autre matière, requiert avant tout la mobilisation de l'ensemble des directions de l'entreprise, qui doivent se coordonner et coopérer.

A l'ère des cyberattaques, la protection des données ne peut qu'être l'œuvre de tous les acteurs de l'entreprise. ●