Approche générale du règlement

Marine0014/Fotolia.com

Le RGPD entre en vigueur le 25 mai 2018. À cette date, toutes les entreprises et les acteurs publics devront être conformes aux nouvelles dispositions relatives à la protection des données à caractère personnel. Les métiers de la sécurité et de la sûreté sont eux aussi impactés.

Toutes les personnes physiques ou morales qui traitent des données à caractère personnel (en dehors d'un usage purement personnel) sont concernées par le règlement européen sur la protection des données (RGPD).

La notion de traitement s'entend de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Les données à caractère personnel consistent en « *toute information se rapportant à une personne physique identifiée ou identifiable* [ci-après dénommée "personne concernée"] ; *est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Il s'agit donc de deux définitions extrêmement larges et l'on peut, sans se tromper, considérer que 100 % des entreprises, associations, fédérations ou entités publiques sont visées par le RGPD.

Le RGPD vise non seulement les personnes physiques ou morales établies sur le territoire de l'Union européenne mais également toutes les entreprises hors UE qui visent des personnes qui « se trouvent » sur le territoire de l'UE dès l'instant où les traitements sont liés :

- soit à une offre de biens ou de services qu'un paiement soit exigé ou non desdites personnes ;
- soit au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

▲ **Le RGPD a pour objectif de renforcer les droits des personnes et d'augmenter les obligations des entreprises qui traitent des données personnelles.**

QUEL EST SON OBJECTIF ?

L'objectif du RGPD est de renforcer les droits des personnes (autrement appelées « personnes concernées ») et, par voie de conséquence, d'augmenter très sensiblement

les obligations des personnes qui traitent des données personnelles (autrement appelées « responsables de traitement »).
Pour les entreprises, la seule bonne nouvelle (relative d'ailleurs) est la disparition de la plupart des démarches préalables. *Exit* en effet les déclarations et autorisations préalables délivrées par la Cnil.
Il est important de dire « la plupart » car il subsiste une procédure particulière dite « analyse d'impact » qui, dans des cas précis, impose de saisir l'autorité de contrôle (la Cnil) avant mise en œuvre du traitement. Cette analyse d'impact n'est cependant imposée que dans des cas particuliers :
• l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
• le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ;
• la surveillance systématique à grande échelle d'une zone accessible au public.

▲ Le RGPD vise les personnes physiques ou morales établies sur le territoire de l'Union européenne ainsi que les entreprises hors UE qui traitent les données des personnes qui « se trouvent » sur le territoire de l'UE.

LA TENUE D'UN REGISTRE

L'analyse d'impact sera aussi requise si la Cnil le décide. Aux démarches préalables seront substituées la tenue d'un « registre des opérations de traitement ». *Grosso modo* il s'agira pour l'entreprise ou l'acteur public de tenir lui-même, sous une forme ou une autre, un « registre » qu'il tiendra à la disposition de l'autorité de contrôle et qui comportera toutes les mentions imposées par l'article 30 du RGPD. Toutes les entreprises et acteurs publics sont tenus de disposer d'un tel registre s'ils ont plus de 250 employés. En deçà, tout dépendra de la nature des traitements.
Quel que soit le nombre d'employés, la tenue d'un registre sera obligatoire si le traitement est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

LE RÔLE DU DPO

RGPD rime pour beaucoup avec DPO ou DPD (*Data Protection Officer* ou délégué à la protection des données). Celui-ci viendrait remplacer le CIL (correspondant à la protection des données) actuel. Rien n'est plus faux… Le CIL était facultatif, le DPO est obligatoire dans trois cas :
• soit que le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
• soit que les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
• soit que les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.
Le CIL avait essentiellement pour mission de conseiller l'entreprise dans le cadre de la mise en œuvre de la loi du 6 janvier 1978. Le DPO est, pour sa part, supposé « contrôler » l'application du RGPD. De fait, sa responsabilité est aussi très différente.

ÉMERGENCE DE NOUVEAUX DROITS

Le RGPD est également l'occasion de créer de nouveaux droits ou de renforcer les droits existants : le droit à la portabilité ; le droit à l'information ; le droit à la transparence ; le droit de rectification ; le droit d'accès ; le droit à la limitation ; le droit au retrait du consentement ; le droit d'opposition.

UN ENGAGEMENT FORT EN TERMES DE SÉCURITÉ

L'impact le plus emblématique du RGPD est le renforcement des obligations en termes de protection d'une part et de sécurité d'autre part. Au titre de l'article 25, le responsable de traitement doit mettre en œuvre toutes

LE PRINCIPE D'ACCOUNTABILITY

Le RGPD modifie donc très sensiblement la donne en matière de données à caractère personnel mais son impact est plus profond encore par la mise en œuvre du principe d'*accountability.* Ne cherchez pas ce mot dans la version française du texte, on ne la trouve que dans la version anglaise, à l'article 5 *in fine.*
L'*accountability* est un principe selon lequel ce n'est plus comme aujourd'hui à la Cnil de démontrer la non-conformité d'un responsable de traitement aux obligations de la loi, mais à la personne concernée de démontrer sa conformité. En d'autres termes c'est un renversement complet de la charge de la preuve.
Ainsi, donc, non seulement les entreprises devront être conformes au RGPD mais aussi être en capacité de le démontrer. Ceci implique que chaque entreprise devra se doter d'une DPP *(Data Privacy Policy)* ou, dans la langue de Molière, d'une PIL (Politique informatique & libertés).

les mesures organisationnelles et techniques et assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. Au titre de l'article 32, le responsable de traitement devrait mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.
Si la formulation des articles 25 et 32 sont très proches il s'agit bien d'une double obligation car « protéger » et « sécuriser » ne sont pas synonymes.
Au titre de la « protection », l'objectif est très large et vise à limiter les risques de non-conformité avec le RGPD. Pour cela, le réglement met en avant la pseudonymisation et le nouveau principe de « minimisation » : minimisation des données (le moins de données possible) et minimisation des accès aux données.
Au titre de la sécurité, le responsable de traitement devra notamment raisonner en termes techniques et mettre en œuvre des moyens tels que : le chiffrement, la pseudonymisation, les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ou encore de traçabilité.
Enfin, un dernier impact important porte sur la relation entre un responsable de traitement et un sous-traitant (c'est-à-dire la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement). Au titre de l'article 28, lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

L'IMPACT SUR LES MÉTIERS DE LA SÉCURITÉ ET DE LA SÛRETÉ

On l'aura compris le RGPD impacte toutes les entreprises privées et les acteurs publics et au sein de ceux-ci, il impacte tous les métiers, au premier rang desquels les métiers relatifs à la sécurité ou la sûreté.
La sécurité et la sûreté sont d'abord impactées car elles utilisent, elles-mêmes, des applications ou des outils qui génèrent des données à caractère personnel à commencer par des logs de connexion. Ces traitements devront répondre aux exigences du RGPD et, s'il doit exister, figurer sur le registre des traitements.
La personne, le département ou la direction en charge de la sécurité/sûreté devra également travailler en étroite collaboration avec le DPO s'il en est désigné un.
Par ailleurs, certains outils au service de la sécurité ou de la sûreté sont considérés comme sensibles par nature. Il en est ainsi de la vidéoprotection et la biométrie.
Dans le premier cas on rappellera les dispositions de l'article 35 qui impose une analyse d'impact et une consultation préalable de l'autorité de contrôle dans le cas de surveillance systématique à grande échelle d'une zone accessible au public.
Il en est de même de la biométrie qui fait l'objet de dispositions *ad hoc* par la Cnil.

Tatomm/Fotolia.com

▲ **La sécurité et la sûreté sont impactées par le RGPD car elles utilisent des outils qui génèrent des données à caractère personnel.**

La mise en œuvre du RGPD est un projet à part entière et ne doit donc pas, *a priori,* reposer sur les épaules du responsable de la sécurité ou de la sûreté de l'entreprise ; mais il en est un des acteurs importants. À ce titre, il convient donc de lui trouver la « juste place » dans la gouvernance de la data que le responsable de traitement ne manquera pas de mettre en œuvre.
En pratique il conviendra :
• d'obtenir le soutien de la direction générale, car la mise en œuvre du RGPD est un projet d'entreprise qui nécessite des moyens humains, techniques et donc financiers ;
• de désigner la personne interne ou externe chargée de piloter le projet RGPD ;
• de désigner s'il y a lieu un DPO et, dans tous les cas, de définir une règle de gouvernance de la data pour définir les rôles et responsabilité de chacun en termes de données personnelles ;
• si cela n'a pas déjà été fait, de procéder à une cartographie des traitements existants ;
• de même, de procéder à une cartographie des sous-traitants et principalement ceux pour lesquels existeraient des flux de données hors UE ;
• de définir avec ces mêmes sous-traitants les dispositions contractuelles adaptées prescrites par le RGPD ;
• si nécessaire (et même dans les cas où cela n'est pas impératif), de mettre en œuvre le registre des traitements.
Il s'agit d'un plan bien spartiate par rapport aux 99 articles et les 173 considérants du RGPD… ■

Éric Barbry
Avocat Associé, Cabinet Racine
IP/IT & Data Privacy