Le nouveau cadre juridique de la protection des données

Par Patrick-Hubert Petit
Expert-comptable
et Commissaire aux comptes,
Associé KPMG SA,
Président de l'Audit
Committee Institute France

et Vincent Maret
Associé KPMG en charge des
activités Cyber sécurité et Protection
des données personnelles

La thématique des données, qui jusqu'à une date récente était considérée comme relevant du domaine des techniciens de l'informatique, est devenue aujourd'hui une préoccupation majeure pour le grand public, les entreprises et leurs organes de direction et de gouvernance, les décideurs publics et privés. Le législateur l'a bien compris avec la publication du Règlement Général sur la Protection des Données (RGPD)[1] entré en vigueur le 25 mai 2018.

Contexte

L'omniprésence du digital

Alors que la population mondiale a augmenté d'un tiers sur les 20 dernières années (pour atteindre aujourd'hui quelques 7,6 Mds), on constate sur la même période que :

- la population mondiale d'internautes est passée de 45 M à 5 Mds (soit les deux tiers de la population du globe) ;
- le nombre d'abonnements mobiles, inférieur à 100 M en 1995, est aujourd'hui supérieur à la population mondiale ;
- le nombre d'objets connectés, inexistants il y a 20 ans, atteint actuellement 7,3 Mds, soit quasiment un par habitant de la planète. Et ce chiffre pourrait être multiplié par 10 d'ici 2025 !

Un risque de cybercriminalité préoccupant

On « hacke » les entreprises, les administrations, les hôpitaux, les particuliers... Les données personnelles peuvent tomber dans des mains malveillantes, ce qui génère des risques sérieux pour les personnes concernées : usurpation d'identité, fraude, atteinte à la réputation, discrimination, divulgation de secret, etc. C'est une réalité : les collectes et traitements massifs de données personnelles peuvent entraîner des « externalités négatives » pour les individus comme pour les organisations.

Une prise de conscience face à cet environnement hyperdigitalisé

Les individus sont de plus en plus soucieux de la protection et de la confidentialité de leurs données personnelles, attente fortement relayée par l'opinion publique. Cette inquiétude se traduit à deux niveaux :

- les entreprises qui collectent des données ont-elles un comportement loyal, transparent et éthique dans leur utilisation ? ;
- protègent-elles suffisamment les données ainsi collectées par rapport à des tiers mal intentionnés ?

Le nouvel environnement juridique de la protection des données

Le RGPD a modernisé les principes énoncés dans la Directive européenne de 1995. S'agissant d'un règlement, il est d'application immédiate dans les pays membres de l'Union européenne. Il définit les droits des personnes physiques et fixe des obligations aux organisations qui effectuent le traitement des données et à celles qui sont responsables de ces traitements. Il fixe également les méthodes visant à assurer le respect des dispositions prévues, ainsi que l'étendue des sanctions imposées à ceux qui enfreignent les règles.

Quelques définitions et précisions

- **Par donnée à caractère personnel**, il convient d'entendre toute information se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire 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 propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- **Le traitement** s'entend de toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles 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.
- **Champ d'application** : Le RGPD concerne toutes les organisations (entreprises, mais aussi administrations et associations) établies dans l'Union européenne et celles établies hors cette zone mais traitant de données de membres de l'Union européenne.

Quelles nouvelles obligations ?

- **Un changement dans le paradigme de la régulation des données**

D'un système d'autorisations données par des régulateurs et où il existait peu de

1. Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

sanctions, on s'oriente vers un dispositif qui n'est plus fondé sur des déclarations et autorisations et où les sanctions peuvent être lourdes et au sein desquelles la responsabilisation des entreprises (« *accountability* ») se renforce avec notamment l'obligation pour les organisations de :

- respecter les droits des personnes physiques concernées, notamment droit à la portabilité des données et droit à l'oubli ;
- tenir un registre documentant tous leurs traitements de données personnelles (pour les entreprises de plus de 250 salariés) ;
- nommer, dans certains cas, un « délégué à la protection des données » (DPO) ;
- notifier à l'autorité de contrôle, et dans certains cas aux personnes concernées, en cas de fuite de données personnelles ;
- respecter une approche double de « *privacy by design* » (intégration de cet enjeu avec des mesures *ex-ante*, dès la phase de conception de tout processus de collecte et traitement des données) et de « *privacy by default* » (sécurisation ex-post de la centralisation, du stockage et de l'utilisation des données) ;
- réaliser des analyses d'impact sur la vie privée (PIA) dans le cas des traitements les plus risqués.

En outre, les sous-traitants sont désormais potentiellement responsables en cas de violations de la règlementation, ce qui n'exonère pas pour autant les responsables de traitement.

Les amendes, en cas de non-conformité constatée lors des contrôles a posteriori qu'effectuera la CNIL, peuvent aller jusqu'à un plafond de 4 % du chiffre d'affaires annuel global de l'entreprise, ou 20 M€ (montant le plus élevé retenu).

Comment se mettre en conformité ?

Une première étape : l'inventaire

La première étape, la plus importante, consiste à réaliser un inventaire des traitements de données à caractère personnel existant au sein de l'entreprise. Cela permet de construire le registre des traitements. Mais c'est surtout un préalable à toute opération d'analyse d'écart avec le RGPD et de construction d'un plan d'actions de mise en conformité.

L'on pourrait penser que les entreprises connaissent bien les traitements de données à caractère personnel qu'elles effectuent et savent où les trouver. En effet, elles étaient soumises jusqu'à maintenant, avec la loi *Informatique et Libertés*, à une obligation de déclarations des traitements. En outre, on a coutume de dire que les données sont le nouvel « or noir ». Il semblerait donc logique que les entreprises connaissent très précisément les « gisements » de cet « or noir ». Or, dans la pratique, c'est loin d'être le cas.
Du fait de la numérisation des processus métiers, les traitements de données personnelles sont partout dans les entreprises et il n'existait pas, pour la plupart d'entre elles, de cartographie claire et complète de ces traitements. L'un des effets du RGPD est donc de forcer les entreprises à mieux connaître leurs traitements et leurs données. Cela met également en évidence le caractère éminemment transverse du sujet des données personnelles qui concerne les métiers, le marketing, les RH, la communication, le juridique, l'informatique, la conformité, etc.

Une deuxième étape : l'adaptation des processus

Une fois l'inventaire des traitements réalisé, une analyse d'écart doit être menée afin de vérifier que les exigences du RGPD sont respectées, qu'elles portent sur des traitements spécifiques (problème du consentement par exemple, ou de la protection des données), ou qu'elles soient transverses (par exemple rôle du DPO).
Dans la plupart des entreprises, des mesures de gestion et de protection des données personnelles sont en place car, ne l'oublions pas, 80 % des exigences du RGPD étaient déjà présentes dans la loi « Informatique et Libertés », entrée en vigueur il y a 40 ans. Toutefois, on constate souvent des lacunes, ou des procédures qui n'ont pas évolué depuis des années et qui ne se sont pas adaptées aux immenses mutations en termes de technologies et d'usages.

Dans certains cas, la mise en conformité passera par une adaptation des processus métiers, voire par l'arrêt de certains traitements qui ne sont plus possibles selon le RGPD. Un gros travail de documentation doit également être réalisé pour se conformer à l'exigence d' « *accountability* ».

Un processus évolutif

En fonction de la taille de l'entreprise et de son exposition aux données personnelles, quelques semaines à quelques mois sont nécessaires pour mener à bien ces deux premières étapes. Le projet RGPD n'en est pas pour autant terminé !
En effet, il va être nécessaire de faire vivre la conformité au RGPD au quotidien, dans le cas de demandes d'exercice des droits des personnes par exemple, ou en cas de nouveaux projets. Parallèlement, des procédures mises en place rapidement, en mode manuel notamment, pourront être optimisées et outillées.

La mise en conformité au RGPD passe aussi par l'adaptation des systèmes d'information à un certain nombre d'exigences : protection des données bien sûr, mais aussi durée de rétention, droit à la portabilité, droit à l'oubli. Ce chantier ne fait que commencer pour la plupart des entreprises et, dans certaines, il prendra plusieurs années...

Le RGPD : un projet de conformité uniquement ?

Le RGPD est avant tout un projet de conformité. Mais les entreprises peuvent l'utiliser pour aller au-delà, par exemple, pour améliorer la relation client en augmentant le degré de confiance.
C'est aussi l'occasion de mieux connaître les données collectées et éventuellement d'identifier dans quelle mesure elles pourraient être mieux utilisées et exploitées pour créer de la valeur pour l'entreprise.
Cela peut enfin permettre d'optimiser les processus et de réduire les coûts, notamment ceux liés à des collectes ou stockages de données inutiles. Ce sont autant de dimensions qu'il peut être intéressant de prendre en compte dans un projet de mise en conformité au RGPD.
La gestion des risques liés aux données exige donc un changement complet de paradigme qui requiert :

- d'étendre le périmètre des fonctions de contrôle ;
- d'intégrer, dès le début des projets, la dimension cybersécurité ;
- de positionner au bon niveau de l'organisation le délégué à la protection des données et d'instaurer une communication harmonieuse et fluide entre les métiers et la fonction cyber afin de maximiser le niveau de sécurité ;
- de mettre à jour en permanence la cartographie des risques et menaces, en essayant notamment de se mettre à la place de l'attaquant ;
- d'inscrire la problématique de la protection des données personnelles dans la durée, au-delà de l'effort initial de mise en conformité avec les exigences du RGPD.

***

Le monde hypertrophié de la data, caractérisant l'environnement social et économique dans lequel se déroule les opérations et transactions, conduit à une véritable explosion de la surface d'exposition qui touche aujourd'hui non seulement les entreprises travaillant

directement sur les données, mais aussi de façon plus large les organisations et entreprises publiques et privées ainsi que leurs parties prenantes.

La « professionnalisation des hackers », se caractérisant par une double expertise - technologique et métiers - constitue un réel danger auquel toutes les organisations se doivent d'être extrêmement sensibilisées afin de mettre en place des systèmes adaptés de protection, d'alerte et de remédiation rapide.

Ceci suppose un effort important de la part des organisations, en termes de ressources humaines dédiées, d'organisation et d'outils informatiques pour s'adapter à ce nouvel univers.

Il apparaît donc que la protection des données et la cybersécurité deviennent aujourd'hui des sujets d'ordre stratégique, relevant des préoccupations des organes de gouvernance des organisations, et non plus uniquement des responsables IT et/ou de la conformité. ■