RGPD
La Cnil accompagne les professionnels dans leur mise en conformité

SOPHIE NERBONNE
Directrice chargée de co-régulation
économique
Commission Nationale de l'Informatique
et des Libertés (Cnil)

Le RGPD instaure une nouvelle gouvernance européenne qui implique les autorités de contrôle de chaque État membre. En France, la Cnil doit s'adapter à cette nouvelle configuration et à ses nouvelles missions pour accompagner les professionnels dans la mise en conformité aux obligations réglementaires RGPD. En aura-t-elle les moyens ?*

De nombreuses incertitudes existent avec la mise en place du RGPD

La prise de conscience généralisée par les professionnels des obligations issues de ce texte fondant la protection des données du XXIe siècle a provoqué une vague d'inquiétude à laquelle la Cnil a répondu par un discours apaisant et de nombreux outils d'aide à la mise en conformité, disponibles sur son site. Responsable de traitement et sous-traitant doivent penser leur mise en conformité en prenant en compte :
les actions de conformité immédiates : registre (cf. le modèle simplifié) et dispositions contractuelles (cf. guide sous-traitant) ;
le rôle central du nouvel acteur qu'est le délégué à la protection des données (DPO) ;
la maîtrise progressive des nouveaux outils, obligatoires ou facultatifs, de conformité : analyses d'impact (cf. guide méthodologique et logiciel téléchargeable), certification, codes de conduite…
Régulateur pragmatique, la Cnil considère que les obligations s'apprécient en fonction de la taille de l'entreprise et de la sensibilité des traitements. Elle a également entrepris la transformation de son patrimoine normatif afin d'apporter de la sécurité juridique aux acteurs. De même, elle a publié la liste des traitements devant faire l'objet d'une analyse d'impact ainsi que des lignes directrices synthétiques permettant aux responsables de traitement concernés de savoir plus précisément s'ils sont ou non soumis à cette obligation. Elle suit les travaux relatifs à une dizaine de codes de conduite, portant notamment sur la recherche médicale et les infrastructures dites de cloud et a développé un MOOC pour se familiariser avec les principes fondamentaux du RGPD, qui sera prochainement accessible.

Une gouvernance européenne
Pour les traitements transfrontaliers de données, la Cnil fait en effet désormais partie d'un mécanisme de prise de décision européenne. Il s'agit d'un modèle novateur, participatif et distribué et non pas centralisé à Bruxelles, qui implique toutes les autorités de contrôle concernées. L'autorité chef de file propose une décision en matière de traitements transfrontaliers qui est analysée par ses pairs. En l'absence de consensus, le comité européen peut émettre un avis contraignant.
Face à ces nouveaux enjeux, les moyens dont dispose la Cnil restent sous-dimensionnés au regard du nombre d'acteurs concernés, à savoir toutes les entreprises, collectivités territoriales, organismes publics, associations… C'est également vrai au regard des moyens dont disposent ses homologues : 200 personnes dans les services de la Cnil, plus de 600 pour l'Autorité britannique.

Une nouvelle mission de certification
La certification succède à la labellisation que la Cnil a pratiquée ces dernières années en matière de formation, de gouvernance « informatique et libertés », d'audit de traitement et de coffre-fort électronique. Elle a adapté au RGPD les deux premiers référentiels et pourrait les transformer en référentiels de certification. En la matière, ce seront des tiers certificateurs qui délivreront les certifications. Le premier référentiel adopté par la Cnil porte sur la certification des compétences des DPO, ce qui intéresse de nombreux organismes dont l'International Association of Privacy Professionals (IAPP), une structure à l'origine américaine s'installant dans l'Union européenne.
Le marché de la certification pourra prendre en compte le besoin des acteurs et développer par exemple des offres de coffres-forts numériques combinés avec d'autres services, des mécanismes d'anonymisation ou de limitation de la durée de conservation des données.

Qu'en est-il des suites législatives post-RGPD ?
Le RGPD est un règlement européen, texte d'application directe, contrairement à la précédente directive de 1995. Pour autant, le législateur national est intervenu pour que la loi du 6 janvier 1978 permette d'opérer les « raccords » entre le règlement et les procédures nationales, en matière de mesures répressives notamment. Cette loi a aussi permis l'utilisation, modérée, des marges de manœuvre nationales spécifiques laissées aux États membres par le RGPD et transpose la directive « police-justice » relative aux traitements régaliens. Une ordonnance est venue boucler ce dispositif, quasi complet en attendant la sortie du décret d'application.

Le recueil des besoins des professionnels
Le passage au RGPD a multiplié les demandes d'accompagnement venant d'opérateurs ou de collectifs professionnels présentant des niveaux de maturité variables en matière d'appropriation du règlement, parfois peu informés ou souhaitant au contraire d'emblée se saisir pleinement de toutes les potentialités des nouveaux outils de conformité. Afin de répondre à la prise de conscience massive par les entreprises de la nécessité d'intégrer la protection des données personnelles dans leurs chantiers numériques, la Cnil a complété son dispositif d'accompagnement des acteurs économiques.
Elle met systématiquement en consultation ses projets de référentiels. Elle déploie une stratégie dite des « têtes de réseaux », qui sont des interlocuteurs de référence capables de lui remonter les problématiques spécifiques des acteurs concernés et de relayer ses recommandations auprès d'eux dans un processus continu et évolutif. Elle facilite la montée en compétence desdites « têtes des réseaux » et la mutualisation des bonnes pratiques dans les secteurs où elle n'existe pas encore.
Le délégué à la protection des données (DPO), un nouvel acteur de la protection des données
La sortie des lignes directrices européennes sur le DPO n'a pas épuisé les questions susceptibles de se poser, sur son statut et ses missions et les interactions des professionnels avec le service des DPO ont progressé pour y répondre ou faire remonter au niveau européen les cas les plus délicats. En février 2019, plus de 45 000 organismes ont déclaré via le téléservice de la Cnil, un DPO.
Pour le secteur public, il y a une obligation de désignation d'un DPO, qui peut être mutualisé pour plusieurs entités, ce qui est particulièrement utile pour les petites structures homogènes (notaires, huissiers de justice, municipalités…). L'obligation de désignation ne vaut dans le secteur privé que pour les traitements à large échelle soit de données sensibles soit s'il s'agit d'un suivi systématique et régulier des personnes, ce qui est le cas des banques ou sociétés d'assurance par exemple.

L'ensemble des Cnil européennes recommande en toutes hypothèses de désigner un DPO, bonne pratique permettant de disposer d'un pilote de la conformité RGPD, gage tout à la fois de confiance mais aussi de compétitivité économique car il s'agit de développer un modèle d'innovation responsable, embarquant dès la conception des produits ou services, la protection des droits des personnes concernées.

Le consentement dans le cadre du RGPD

Il a été beaucoup question du consentement des personnes concernées par la collecte de leurs données, alors que le consentement constitue une base légale du traitement parmi d'autres, telles que l'obligation légale (pour les traitements de lutte antiblanchiment par exemple) ou l'intérêt légitime du responsable de traitement (pour les traitements de lutte contre la fraude ou de prospection commerciale). Afin que le consentement soit valable, les modalités de son recueil doivent garantir qu'il est libre, éclairé et spécifique. Cela signifie qu'il ne peut être mélangé avec l'acceptation des conditions générales d'utilisation d'un site ou résulter d'une case précochée, par exemple. À côté du cadre général posé par le RGPD, s'applique la directive « ePrivacy » transposée dans le code des communications électroniques qui fixe le principe du consentement pour certains cookies et fait l'objet de travaux européens à l'échéance assez peu claire.

S'adapter rapidement aux changements

Les acteurs économiques ont réalisé que le principe de « responsabilisation » mis en avant par le RGPD, à savoir être en mesure de démontrer qu'ils respectent leurs obligations, s'avère au final plus lourd que les formalités préalables qui ont quasiment disparu, sauf dans la recherche médicale. Cette nouvelle logique garantit pourtant une application effective du RGPD, au bénéfice du respect des règles du jeu par tous les acteurs économiques, qu'ils soient situés en Europe ou non. C'est au final le respect des droits et libertés de chacun d'entre nous qui se trouve ainsi mieux protégé.

La Cnil entend dès lors offrir un accompagnement renouvelé de cette trajectoire des acteurs au moyen d'un premier niveau de service de sensibilisation sur la conformité RGPD et sur toute la gamme d'instruments de corégulation disponible (référentiels, codes de conduite, mécanismes de certification, etc.), amorcer un dialogue sectoriel structuré avec l'ensemble des secteurs économiques (corégulation) et davantage articuler, dans un souci de lisibilité pour les acteurs économiques, les différents corpus normatifs avec les autres régulateurs économiques (interrégulation). Un guide AFA Cnil « protection des données et lutte anticorruption » devrait ainsi prochainement sortir.

Quid du droit à la portabilité ? Gadget inutile ou véritable atout ?

Il s'agit là d'un droit nouveau qui devrait constituer un double atout. Ce droit à la portabilité a été voulu par le législateur européen pour éviter aux individus d'être dépendants des plates-formes ou entités disposant de leurs données numériques, qu'ils souhaiteraient basculer chez un autre opérateur. Il a aussi été instauré dans l'optique de stimuler la concurrence et l'innovation technologique. Son utilisation devrait mener à la création de nouveaux services, démontrant ainsi que la réglementation peut être à la source d'innovations.

En conclusion, je souhaitais souligner le déploiement de la stratégie de la Cnil à destination des « têtes de réseaux » économiques. Il s'agit de créer une nouvelle dynamique avec les collectifs, de quelque nature qu'ils soient, représentatifs des secteurs d'activité, professions, thématiques, pour répondre à leurs besoins et produire un travail de régulation plus opérationnel. Il s'agit aussi de réussir le passage à l'échelle, avec un effet levier permettant de démultiplier les actions de conformité. La construction de liens permettant une étroite

collaboration avec le secteur financier remonte déjà à plusieurs années et cette dernière devrait se trouver régénérée par cette nouvelle approche.