RGPD, trois ans après, où en est-on ?

Par **Marie-Laure DENIS**
Conseiller d'État, présidente de la CNIL

Alors que le règlement général sur la protection des données (RGPD) fêtera son troisième anniversaire le 25 mai 2021, force est de constater que ce texte reste très mobilisateur à tous les niveaux, ainsi que très présent dans l'agenda politique et médiatique mondial.

Afin d'évaluer le chemin parcouru, rappelons brièvement **en quoi consiste le RGPD et les enjeux de son succès opérationnel**.

Le RGPD, un texte au service de la confiance dans le numérique

Rappel de ses principes

Depuis la création de l'informatique, la société s'est numérisée dans toutes ses sphères. Les données personnelles sont devenues le pilier de l'activité commerciale des entreprises, qui tendent à en collecter toujours plus pour affiner la connaissance de leurs clients, et personnaliser en conséquence leurs produits et services. Le développement des objets connectés, des techniques de profilage, des outils de contrôle et algorithmes en tous genres, l'augmentation des cyberattaques, ainsi que les révélations d'Edward Snowden en 2013, ont nourri une prise de conscience collective sur la nécessité de revoir à la hausse le niveau de protection accordé aux données personnelles.

Au-delà des risques pour la vie privée liés à une mauvaise gestion et à une sécurisation insuffisante des données personnelles, certains traitements informatiques présentent aussi de réels risques pour les libertés individuelles et publiques. Par exemple, un recours disproportionné à la vidéosurveillance ou à la cybersurveillance peut placer les personnes dans une situation de contrôle quasi-permanent et peut générer des réflexes d'auto-censure.

Le RGPD n'est pas né d'un droit hors-sol. L'Europe, riche de sa tradition philosophique héritée des Lumières, a consacré une nouvelle génération de droits de l'Homme, celle des « droits-système » afin d'organiser l'univers sous-jacent du numérique, après avoir conceptualisé les droits et libertés, les droits patrimoniaux et les droits sociaux afin de garantir un niveau de protection maximal à la vie privée et aux libertés des personnes.

Le RGPD a ainsi été élaboré autour de trois axes majeurs :

- le renforcement des droits des citoyens européens, tant sur le plan qualitatif, avec la possibilité de mieux comprendre et contrôler l'usage qui est fait de leurs données, que quantitatif, avec l'apparition de nouveaux droits comme le droit à la portabilité ;
- une nouvelle logique de responsabilisation de l'ensemble des acteurs de traitement de données des citoyens européens, quelle que soit leur localisation, remettant sur un pied d'égalité l'ensemble des acteurs européens et internationaux au regard du droit applicable ;
- et le renforcement du pouvoir de sanction des CNIL européennes (Commission nationale de l'informatique et des libertés), avec une hausse des seuils à 20 millions d'euros ou 4 % du chiffre d'affaires mondial des entreprises.

De cette manière, l'Europe a fourni une réponse moderne et innovante aux problématiques d'utilisation des données personnelles, faisant des valeurs de la confiance et de la transparence la clé de voûte de la régulation économique et d'un déploiement durable du numérique dans tous les aspects de l'activité humaine.

Nouveaux mécanismes de régulation à l'échelle européenne

Pour éviter le risque de *forum shopping* qui a pu affaiblir les réglementations du numérique des années 2000, le RGPD a mis en place une mécanique inédite de coopération en réseau d'autorités nationales, une sorte d'intégration décentralisée impliquant de profonds changements dans les méthodes de travail des autorités nationales. Autrement dit, il y a désormais un guichet unique pour les entreprises, à savoir l'autorité de protection des données de son établissement principal, et un guichet unique pour les citoyens, l'autorité de protection des données de son pays. Si l'entreprise n'a qu'un seul interlocuteur parmi les autorités, les décisions qui la concernent sont prises en commun, afin de prononcer une décision applicable à l'échelle de l'Union européenne. En cas de désaccord entre autorités, c'est le comité européen à la protection des données (CEPD), nouvel organe de l'Union européenne, qui arbitre.

Les conséquences pour les entreprises

Bien sûr, pour les entreprises, le RGPD représente un défi de taille : celui de la mise en conformité, pour laquelle il n'existe pas de solution passe-partout. Chaque secteur d'activité et chaque métier appellent des réponses adaptées. C'est là le tout nouveau rôle d'« évangélisation » du délégué à la protection des données, chargé d'aider l'entreprise à procéder à un changement général de posture, en application du principe de responsabilité, pour constamment avoir l'assurance que les politiques et les procédures encadrant l'innovation technologique restent valides sur la durée et à tous les niveaux. Un des nouveaux leviers prônés par le RGPD est le principe de protection des données dès la conception et par défaut (*data protection by design and by default*). Il implique la prise en compte de la vie privée très en amont des projets, par des mesures préventives ou des choix technologiques limitant les risques éventuels de violation de données personnelles.

Cette exigence éthique de mise en conformité dynamique et globale peut nécessiter des investissements importants sur le plan financier et humain. Mais, d'une part, ces principes sont en réalité connus depuis plus de 40 ans avec la loi Informatique et Libertés (loi du 6 janvier 1978) ; d'autre part, ils peuvent également être un vecteur de croissance pour les entreprises, qui sécuriseront leurs consommateurs sur l'utilisation, la qualité et la pertinence des données collectées. En tout état de cause, la protection des données est désormais un sujet de gouvernance interne des entreprises, à la croisée des compétences informatique, juridique, commerciale et de communication.

Ces fondements posés, la responsabilité collective d'être à la hauteur de ces enjeux, de concrétiser les promesses du RGPD et de le faire mieux rayonner se dégage. **Quel a été le bilan de ces trois ans d'effectivité ?**

Bilan à trois ans

À l'échelle de la France

A l'échelle de la France tout d'abord, les chiffres montrent que la mise en œuvre de ce nouveau modèle est plus qu'enclenchée.

L'effet RGPD s'est ressenti du côté des professionnels : plus de 24 000 délégués à la protection des données, représentant plus de 72 000 organismes, étaient déclarés en France fin 2020. Près de 6 000 notifications de violation de données personnelles ont été reçues depuis 2018, avec près de 1 200 dossiers en 2018, 2 300 en 2019 et plus de 2 500 en 2020, ce qui a permis à la CNIL de mieux orienter son action de conseil et de répression, et de mieux jouer son rôle dans l'écosystème de la cybersécurité.

Du côté des particuliers également, le nombre cumulé de visites du site de la CNIL, d'appels et de consultations des questions/réponses disponibles en ligne a enregistré une hausse très importante,

de 60 % depuis 2018, donnant un bon indicateur du besoin d'information sur le RGPD. En 2019, la CNIL a reçu un nombre record de 14 137 plaintes, en augmentation de 27 % par rapport à 2018 et en augmentation de 79 % sur les cinq dernières années. À ce stade, si les chiffres consolidés de 2020 ne sont pas encore connus, on peut tout de même dire que le nombre de plaintes a continué d'augmenter, avec une évolution sensible des demandes d'informations liées à la crise sanitaire.

Ces augmentations apportent un éclairage essentiel sur la structure des problématiques quotidiennes des Français et reflètent leurs trois préoccupations majeures :

- conserver la maîtrise de leurs données et éviter qu'elles soient traitées à leur insu, ce qui est illustré par les 13 % d'augmentation des plaintes relatives au déréférencement ;
- ne pas être dérangé, être entendu et considéré, avec 15 % des plaintes relatives à la réception de prospection commerciale, associative ou politique ;
- et faire prendre en compte leurs droits, tant auprès des employeurs que des services publics, avec notamment 42 % d'augmentation des plaintes liées à l'accès au dossier médical.

En ce qui concerne les sanctions, la CNIL conduit en moyenne 300 contrôles formels par an. Le nombre de mesures correctrices est quant à lui en hausse chaque année, puisque, dans un premier temps, la CNIL a concentré ses efforts sur son action pédagogique auprès des acteurs économiques, en entretenant un dialogue étroit avec les têtes de réseau pour démultiplier son accompagnement, et en produisant de nombreux outils facilitant la mise en conformité, comme le MOOC RGPD, le guide à destination des TPE et PME, et les outils d'analyse d'impact qui sont disponibles sur son site Internet. Cette période de transition étant désormais terminée, la CNIL a prononcé une quinzaine de sanctions en 2020 pour un montant cumulé d'environ 139 millions d'euros, contre 8 sanctions en 2019, ce qui a activé ainsi les nouveaux montants permis par le RGPD.

À l'échelle de l'Europe

Au niveau européen, la coopération est également devenue une réalité quotidienne pour les autorités de régulation. Plus de 1 300 cas transfrontaliers ont été identifiés, 450 procédures dites de « guichet unique » ont été lancées et plus de 150 décisions finales ont été adoptées en application des mécanismes de coopération et de cohérence. Fin 2020, le CEPD a également adopté sa première décision contraignante afin d'arbitrer un différend entre l'autorité irlandaise et les autres autorités européennes concernant Twitter ; il a aussi adopté une vingtaine de lignes directrices, sur différents sujets relatifs à l'application du RGPD, comme notamment son champ d'application territorial, le ciblage des utilisations sur les réseaux sociaux ou le *Privacy by design*, contribuant à une véritable doctrine européenne en matière de protection des données.

S'il n'y a pas de statistiques officielles tenues par le CEPD sur le nombre de sanctions à l'échelle européenne, certains sites privés indiquent qu'à la fin de novembre 2020 environ 420 sanctions avaient été émises, représentant plus de 260 millions d'euros d'amende.

À l'échelle mondiale

Enfin, même au niveau mondial, nous constatons qu'il y a eu un avant et un après 25 mai 2018. Le caractère extraterritorial du RGPD remettant les acteurs internationaux et européens sur un même plan, ainsi que la libre-circulation des données permise sur le territoire sont autant de signaux forts affirmant la volonté de souveraineté numérique européenne. Il ne s'agit pas ici de protectionnisme, mais bien d'affirmer un modèle de régulation basé sur la défense du droit des personnes, notamment par rapport aux GAFAM (acronyme pour Google, Apple, Facebook, Amazon et Microsoft) et en matière de cybersécurité. S'il faut se garder de tout triomphalisme, le RGPD est véritablement devenu une source d'inspiration mondiale.

Certains pays ont procédé à une mise à jour de leur cadre national en matière de protection des données, afin de continuer à commercer avec l'Europe. C'est le cas notamment du Japon, de la Corée du Sud, du Bénin ou encore de l'Australie. Un processus législatif en ce sens est également en cours en Suisse, en Tunisie et au Burkina Faso.

D'autres États ont aussi, pour la première fois, adopté un cadre juridique général encadrant les traitements de données personnelles, dont les principales dispositions peuvent se rapprocher de celles du RGPD. C'est le cas de la Californie avec le "California Consumer Privacy Act" adopté en octobre 2018 et entré en application au 1er janvier 2020, mais aussi du Brésil avec la "Lei Geral de Proteçao de Dados" adoptée en 2019. En Inde, où la Cour suprême a consacré en 2017 le droit à la vie privée comme droit fondamental, un projet de loi est actuellement en discussion au Parlement. Le RGPD est donc devenu un instrument de *soft power* dans la diplomatie actuelle de la donnée.

Focus sur les enjeux de 2020, année de la mise à l'épreuve

De nombreuses études de cas réels ont eu lieu en 2020, testant de fait l'application d'une grande quantité des dispositions du RGPD, qui auraient pu être durement mises à l'épreuve durant l'année qui vient de se terminer.

Les leçons de la crise du COVID

Une des conséquences de la pandémie, tout d'abord, aura été de placer les enjeux de protection des libertés fondamentales et des données à caractère personnel au cœur des débats publics, et de faire émerger d'importants points de tension, susceptibles de déplacer les perceptions et les préoccupations concernant la protection de la vie privée. La CNIL en tire plusieurs leçons.

La première : la grande robustesse des principes posés par le RGPD, qui ont permis d'éviter le détournement de l'encadrement de l'usage des données sensibles et se sont révélés suffisamment souples pour permettre aux États membres de prendre en compte la nécessité de traiter et partager des informations dans un contexte exceptionnel.

Concrètement, les principes de finalité (est-ce que le but de la collecte est clair et précis ?), de nécessité (quelle utilité ?), de proportionnalité (existe-t-il un moyen moins intrusif ?), de minimisation des données (seules les données nécessaires sont-elles collectées ?) et de limitation de la conservation des données (est-ce que les données seront effacées quand le traitement aura atteint son but ?) ont constitué des éléments essentiels de la confiance dans les traitements de données en situation d'urgence, et ils continueront de servir de fil rouge aux décisions dans un monde post-Covid. La crise aura également particulièrement bien montré l'intérêt des approches *by design* préventives que les différents porteurs de projet se sont efforcés d'intégrer dans leurs protocoles de gestion de données.

La deuxième leçon concerne la fonction d'accompagnement et de contrôle du régulateur, indispensable au principe de responsabilisation des acteurs. Le rôle de la CNIL comme guide des administrations et des entreprises privées, mais aussi comme garante des libertés et de la vie privée, est apparu essentiel pour accompagner les pouvoirs publics et les acteurs privés. Cela confirme l'utilité pour la CNIL de communiquer de manière régulière sur sa doctrine afin que les acteurs puissent s'en saisir le plus en amont possible dans le cadre de leurs projets.

Les défis à l'échelle européenne

2020 aura également été marquée par d'autres rebondissements majeurs rebattant les cartes économiques : l'arrêt Schrems II rendu par la Cour de justice européenne, annulant le "Privacy Shield" qui permettait le transfert de données entre l'Europe et les États-Unis ; l'engagement de transférer l'hébergement par Microsoft du Health Data Hub vers une plateforme européenne

dans un délai de deux ans ; les initiatives législatives européennes en matière de marché unique européen avec le "Digital Governance Act", le "Digital Services Act" et le "Digital Markets Act", prochainement suivis du "Data Act" ; et le plan de relance économique volontariste en France.

Ce contexte exceptionnel offre un alignement assez inédit des intérêts entre notre régulation et notre politique industrielle. Il est de notre responsabilité de parvenir à nous en saisir collectivement en vue de mener une politique ambitieuse en matière de souveraineté numérique européenne, pour laquelle le respect du RGPD sera un facteur essentiel de succès.