CNIL

590

« Le RGPD a eu un impact direct : le nombre de plaintes auprès de la CNIL a augmenté d'un tiers en un an »

Un an après l'entrée en application du règlement général sur la protection des données, le 25 mai 2018 *(RGPD - PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016)*, Marie-Laure Denis, présidente de la Commission nationale informatique et libertés (CNIL) nommée en février dernier, dresse un premier bilan et revient sur les grands enjeux de sa présidence.

La Semaine Juridique, Édition générale : Comment définiriez-vous le rôle de la CNIL ?

Marie-Laure Denis : Le rôle d'une autorité de régulation telle que la CNIL est d'une part, d'aider à rendre le droit intelligible et praticable pour les usagers et d'autre part, de s'assurer du respect des règles, au besoin en sanctionnant les manquements. Cette fonction dissuasive est d'autant plus importante que depuis l'entrée en vigueur du RGPD, la CNIL a des capacités de sanctions renforcées pouvant aller jusqu'à 4 % du chiffre d'affaires annuel.

La CNIL doit aussi veiller à la sécurité juridique de l'ensemble des concitoyens dans l'interprétation des textes. En cela, elle a un rôle important à jouer de régulateur en phase tant avec la réalité économique qu'avec les usages des citoyens dans un contexte technologique mouvant. À cet effet, la CNIL utilise tous les instruments, y compris de droit souple (référentiels, lignes directrices, etc.), pour favoriser l'appropriation des règles et des bonnes pratiques par les différents acteurs.

Une autre de ses missions, moins connue mais structurante, est sa mission consultative auprès des pouvoirs publics. Le collège de la CNIL rend de nombreux avis sur des projets de textes (en 2018, 120 avis). Elle a

Entretien avec **MARIE-LAURE DENIS,** présidente de la CNIL

par exemple examiné le projet de décret, dernière pièce à l'édifice de l'adaptation du droit national au paquet européen sur le RGPD *(D. n° 2019-536, 29 mai 2019 : JO 30 mai 2019, texte n° 16)*. De surcroît, du fait du caractère transversal de la protection des données, la CNIL a été auditionnée 30 fois devant le Parlement.

La CNIL intervient enfin pour articuler le droit horizontal de protection des données avec toutes les législations sectorielles, en lien avec d'autres administrations, comme l'illustre le futur guide élaboré avec l'Agence française anticorruption (AFA) sur les alertes professionnelles.

JCP G : Quel bilan tirez-vous de la première année d'application du RGPD ?

M.-L. D. : Tout d'abord, le RGPD a eu un impact direct sur les Français. Depuis son entrée en application, nous constatons une plus forte appétence de nos concitoyens sur la thématique de la protection des données personnelles. Le nombre de plaintes auprès de la CNIL a augmenté d'un tiers en un an, tout comme le nombre de visiteurs sur le site qui a explosé (8 millions de visiteurs soit une augmentation de plus de 80 %), et le nombre de consultations des FAQ (Foire aux questions), en hausse de 60 %.

Ces chiffres traduisent une demande forte des personnes quant à la protection de leurs droits et une quête d'informations de la part des organismes publics ou privés. Les entreprises peuvent parfois envisager le RGPD comme une contrainte, mais il y a en réalité un indéniable intérêt commercial et concurrentiel à prendre en compte cette problématique dès la conception des services proposés aux clients (le privacy-by-design).

Le RGPD vise à renforcer la confiance dans l'économie numérique. C'est ce vers quoi convergent toutes les actions de la CNIL.

JCP G : Quelles ont été les principales actions de la CNIL pendant cette première année d'application ?

M.-L. D. : L'année 2018 a été centrée sur l'accompagnement global des entreprises et des pouvoirs publics. Un certain nombre d'instruments a été mis à leur disposition comme un guide à l'égard des TPE et des PME. Le 11 mars dernier, la CNIL a lancé une formation en ligne, le Mooc Atelier RGPD, à destination des DPO (data protection officer) et des professionnels principalement, mais aussi de toutes les personnes intéressées. Ce cours ludique de 5 heures permet la délivrance d'une attestation de suivi de cours. 35 000 comptes ont été ouverts. Par ailleurs, depuis le RGPD, 52 000 organismes et 18 000 DPO ont été nommés. Comme il n'est pas possible d'accompagner individuellement 4 millions d'entreprises, la CNIL s'adresse aux têtes de réseaux sectoriels et aux fédérations. Au second semestre, l'action sera ciblée sur les collectivités locales et les petites communes qui peuvent se trouver dépourvues. Un guide sera mis à leur disposition. Une stratégie en direction des start-up est également mise en oeuvre avec des ateliers à la Station F notamment sur le privacy-by-design et des contenus dédiés sur le site.

En outre, en tant qu'autorité de régulation, l'une des spécificités de la CNIL est d'être à la fois une autorité protectrice de droits et un régulateur économique horizontal. La CNIL privilégie ainsi l'interrégulation entre les AAI (autorités administratives indépendantes) des différents secteurs.

Il y a de nombreuses synergies avec les autres autorités. Par exemple, le cadre juridique de l'ouverture des données publiques (open data) et son articulation avec la réglementation relative à la protection des données personnelles ont suscité de nombreuses interrogations de la part des différents acteurs concernés, par exemple sur les catégories de documents pouvant être publiés ou les conditions dans lesquelles ces mêmes documents peuvent être réutilisés.

Dans ce contexte, la CNIL et la CADA (Commission d'accès aux documents administratifs) ont élaboré un guide pratique sur la publication en ligne et la réutilisation des données publiques qui permettra de clarifier le cadre juridique applicable et de répondre aux principales problématiques. Une consultation qui a pris fin en avril a permis de recueillir 120 contributions. Le guide est en cours de finalisation et sera publié prochainement.

Qui prononce les sanctions ?

Le collège de la CNIL est composé de 18 membres : 6 représentants des hautes juridictions (2 conseillers d'État, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes), 6 personnalités qualifiées, 4 parlementaires (2 députés, 2 sénateurs), 2 membres du Conseil économique, social et environnemental, 1 membre de la CADA (Commission d'accès aux documents administratifs).

La formation restreinte, chargée de prononcer les sanctions, est composée de 5 membres issus du collège et d'un président distinct du président de la CNIL. Elle peut prononcer diverses sanctions à l'égard des responsables de traitement qui ne respecteraient pas la loi. Avec le RGPD, le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces sanctions pécuniaires peuvent être rendues publiques.

Le président de la CNIL peut prononcer des mises en demeure ou encore saisir la formation restreinte.

JCP G : La CNIL va-t-elle renforcer ses contrôles ?

M.-L. D. : La CNIL va poursuivre sa mission d'accompagnement tout en intensifiant les contrôles ciblés sur le RGPD. La première année a en effet été marquée par une forme de tolérance particulière de la CNIL, concernant les obligations nouvelles issues du RGPD. Désormais, nous devons faire passer le message que, sans renoncer à son action d'accompagnement et tout en faisant preuve de discernement dans son action répressive, la CNIL n'hésitera pas à passer aux sanctions.

La démarche d'accompagnement n'a en effet de sens que si la CNIL vérifie ensuite que les recommandations sont bien suivies d'effet. C'est tout le changement de paradigme du règlement RGPD d'être passé d'un système administratif de déclarations à une responsabilisation des entreprises. Ce que les anglo-saxons appellent l'accountability et qui désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Ce temps d'adaptation laissé aux entreprises n'a toutefois pas empêché la CNIL d'effectuer 310 contrôles en 2018 qui ont donné lieu à 40 mises en demeure et à une dizaine de sanctions financières. La plupart de ces sanctions portait sur des questions de sécurité – étant rappelé que l'obligation de protéger les données personnelles est bien plus ancienne que le RGPD.

> « C'est tout le changement de paradigme du règlement RGPD d'être passé d'un système administratif de déclarations à une responsabilisation des entreprises. »

L'un des axes intéressant du RGPD est d'avoir renforcé le rôle de la CNIL en tant qu'acteur de la cyber sécurité. Les violations de données doivent lui être notifiées sous 72 heures. Les entreprises doivent tenir un registre qui consigne tous les incidents de sécurité. Si la violation de données peut avoir des risques élevés pour les personnes concernées, celles-ci doivent également être tenues informées.

À cet effet, la CNIL a mis à disposition un téléservice dédié permettant aux entreprises de caractériser leurs violations de données, de les déclarer à la CNIL et de s'interroger sur leur obligation éventuelle d'informer les personnes.

JCP G : Comment s'organisent les contrôles ?

M.-L. D. : Les contrôles interviennent soit à la suite d'une plainte, soit à l'initiative de la CNIL. En 2019, différentes priorités sont fixées.

La CNIL veillera à **exploiter de plus en plus les plaintes**, afin d'être en phase avec l'actualité de terrain et de répondre aux attentes des usagers. À cet égard, 20 % des plaintes sont traitées à l'échelle de la coopération européenne entre les différentes CNIL européennes au sein du Comité européen de la protection des données (CEPD, ancien G29). Nous nous réunissons chaque mois avec les présidents des 28 CNIL européennes pour élaborer des lignes directrices et donner un cap aux actions à l'échelon européen, notamment dans le traitement des plaintes.

Le focus sera mis sur **le RGPD** selon 3 axes :

- La protection des droits et le contrôle de la réalité de l'exercice de ces droits : le droit à être informé de la collecte des données, le droit d'opposition, le droit à l'oubli et la suite donnée aux demandes de déférencement (en forte augmentation) ;
- L'articulation entre les responsabilités des donneurs d'ordres et des sous-traitants, que le RGPD a rendu également responsables de la protection des données ;
- Les droits des mineurs : notamment la nécessité du recueil du consentement de l'autorité parentale pour les jeunes de moins de 15 ans pour un certain nombre d'activités sur les réseaux sociaux.

JCP G : Comment la CNIL fait-elle face au changement d'échelle de son activité à la suite du RGPD ?

M.-L. D. : La CNIL essaye de rationnaliser autant que possible ses moyens d'action, en proposant au plus grand nombre des outils accessibles et en privilégiant les interventions en amont.

Fin 2018, la CNIL comptait 200 collaborateurs, très loin derrière ses homologues européens (900 en Angleterre). Ces chiffres placent la France très en-dessous de la moyenne avec le 3e rapport population/nombre d'agents le plus faible des 28 États européens.

L'augmentation des effectifs reste un enjeu important pour la CNIL à la fois pour répondre aux attentes de nos concitoyens, traiter les plaintes, fournir aux opérateurs l'accompagnement qu'ils attendent, et exercer de la meilleure façon les contrôles, tout en conservant son rôle prépondérant sur le terrain de la diplomatie de la donnée européenne.

JCP G : La CNIL doit-elle contrôler en priorité les GAFA ?

M.-L. D. : Google a été sanctionné cette année par la CNIL et a payé une amende de 50 millions d'euros. Cette sanction a été très médiatisée parce qu'il s'agissait de la première sanction en Europe prononcée au titre du RGPD et qu'elle concernait Google. La société vient de former un recours devant le Conseil d'État.

> « Il ne s'agit toutefois pas de faire un sort particulier aux GAFA, et ce même si ces entreprises ont un impact fort sur l'économie numérique. »

Il ne s'agit toutefois pas de faire un sort particulier aux GAFA, et ce même si ces entreprises ont un impact fort sur l'économie numérique. S'agissant d'acteurs implantés dans tous les pays, il doit par ailleurs y avoir une coopération européenne sur le sujet.

Il n'est pas question de sous-estimer les sanctions contre les acteurs plus modestes. À condition d'être proportionnées, ces sanctions peuvent permettre d'avoir un effet dissuasif et pédagogique auprès d'un secteur professionnel par exemple.

La mise en œuvre du RGPD est un objectif prioritaire des CNIL européennes. Le RGPD a en effet une portée extraterritoriale : une entreprise qui n'est pas installée en Europe et qui traite les données de citoyens européens doit appliquer le RGPD.

Le RGPD a ainsi créé un standard de protection des données. Il existe une bulle de protection des données personnelles en Europe et il est nécessaire que la même bulle de garanties existe ailleurs. Aux États-Unis, où je viens d'assister au Congrès mondial sur la protection des données personnelles, il y a un fort intérêt pour le RGPD. Les américains s'interrogent sur l'élaboration d'une loi fédérale sur la protection des données après que la Californie (6e économie mondiale) en a adopté une qui entrera en vigueur en janvier prochain. Le Brésil également a adopté une loi sur la protection des données qui s'inspire du RGPD européen. Le Japon a conclu un accord d'adéquation avec la Commission européenne.

JCP G : L'exportation de nos données vers les États-Unis suscite des inquiétudes. À tort ou à raison ?

M.-L. D. : Nos données personnelles peuvent en effet être hébergées sur des serveurs à l'étranger, et le RGPD organise une continuité de la protection dans ce cas de figure. Pour ce qui est des États-Unis, un accord, le Privacy Shield entré en vigueur depuis 1er août 2016, a été signé avec l'Union européenne pour apporter des garanties en matière de protection de la vie privée à l'occasion de transfert de données Outre-Atlantique.

La Commission européenne et le Comité des CNIL européennes (CEPD) font une fois par an la « revue » de cet accord. À cette occasion il est question des garanties apportées par les américains. L'impératif de convergence des standards en la matière est désormais aussi important que dans le secteur du commerce. Il y a en effet un commerce de la donnée pour lequel le cadre juridique est en construction. La CNIL, première AAI en France, a 40 ans d'existence et doit continuer à peser sur ces sujets. La France doit rester moteur, il y a un vrai enjeu de souveraineté numérique sur ces questions. Le Sénat a d'ailleurs créé une mission d'information sur le sujet.

JCP G : Quelles sont les autres priorités d'action de la CNIL ?

M.-L. D. : Un autre axe important vise à renforcer l'expertise technologique de la CNIL pour avoir une régulation qui se fasse au plus près de la réalité des usages du numérique. Après l'intelligence artificielle et les algorithmes l'an passé, l'attention se porte plus particulièrement en 2019 sur les assistants vocaux et le cloud computing.

Sur ces sujets, l'objectif est de rendre lisibles des écosystèmes complexes et de formuler des recommandations très concrètes afin de parvenir à une régulation la plus réaliste possible dans un monde technologique très mouvant.

JCP G : Comment la CNIL se positionne-t-elle dans ce nouvel écosystème technologique ?

M.-L. D. : Notre rôle de régulateur doit être ancré dans la réalité des usages technologiques. À la CNIL, nous disposons d'un fort pôle de compétences. Nous comptons par exemple dans nos équipes un designer pour promouvoir l'émergence d'un design des interfaces plus responsable et respectueux des principes de protection des données. À l'instar des questions juridiques et techniques, le design des interfaces doit désormais être au centre des préoccupations du régulateur, tout comme il est déjà au cœur des relations entre les individus et les fournisseurs de services. C'est l'objet du dernier cahier Innovation et Prospective intitulé « La forme des choix », paru en janvier. Nous venons de lancer une plateforme d'échanges entre les designers pour diffuser des bonnes pratiques.

Ce sont des nouveaux outils de régulation très innovants.

Propos recueillis par Florence Creux-Thomas

Pour aller plus loin

J. Lessi, Un nouveau chapitre de la protection des données, Bilan d'activité 2018 de la CNIL : JCP G 2019, act. 503.

A. Bellotti, Google lourdement sanctionnée par la CNIL pour méconnaissance du RGPD : CNIL, délib. n° SAN-2019-001, 21 janv. 2019 : JurisData n° 2019-000477 ; JCP G 2019, act. 350.

J. Deroulez, Google condamné à une sanction pécuniaire de 50 millions d'euros par la CNIL : la révolution du consentement ? : JCP G 2019, act. 57.

Le Data Protection Officer, au coeur du réacteur : JCP G 2018, act. 1200, Portrait.

D. n° 2018-687, 1er août 2018 et Ord. n° 2018-1125, 12 déc. 2018.

A. Debet, Libertés et protection des personnes : L. n° 2018-493, 20 juin 2018 : JCP G 2018, doctr. 907.

N. Martial-Braz, Quand la French Touch contribue à complexifier l'édifice du droit de l'Union européenne ! À propos de L. n° 2018-493, 20 juin 2018 : JCP G 2018, act. 786.

N. Lenoir, Protection des données personnelles et responsabilités plurielles : JCP G 2018, doctr. 1059.

L. n° 2016-1321, 7 oct. 2016, pour une République numérique : JO 8 oct. 2016, texte n° 235.