

## 50 Projet de loi CNIL3 : l'impossible défi

**POINTS CLÉS** > Le Parlement va débattre début 2018 d'un projet de loi relatif à la protection des données personnelles > Ce projet vise à modifier la loi Informatique et Libertés pour la rendre compatible avec le règlement européen 2016/679 dit règlement général sur la protection des données (RGPD), mais aussi pour adopter les options nationales prévues par ce règlement et pour transposer la directive 2016/680 sur les traitements de données dans un cadre pénal > Cet enchevêtrement d'objectifs rend la rédaction malaisée, et la CNIL s'alarme du manque de lisibilité du résultat > Au-delà des amendements proposés par la CNIL, d'autres amendements sont possibles pour réduire les divergences entre le droit national et le RGPD, et pour mettre à jour les articles du Code pénal réprimant les atteintes aux données personnelles

Fabrice MATTATIA,

ingénieur général des mines, docteur en droit,  
chercheur associé à l'université Paris 1

**D**EPUIS le lancement en 2012 du chantier qui devait aboutir au règlement européen 2016/679 dit règlement général sur la protection des données (RGPD), l'évolution prévisible du cadre juridique des données personnelles pouvait paraître simple : le RGPD, d'application directe, allait remplacer notre bonne vieille loi *Informatique et Libertés* (L. n° 78-17, 6 janv. 1978), et fournir ainsi un nouveau cadre européen unifié. Voire ! C'était oublier que le RGPD ne s'applique qu'à certains types de traitements, qu'il prévoit plus de cinquante options à déterminer par le droit national, qu'en parallèle il faut transposer la directive 2016/680 sur la protection des données dans les cas d'enquêtes et de poursuites pénales, et que, de toute façon, les traitements qui échappent à la compétence de l'Union européenne, notamment les traitements de souveraineté, ne peuvent être régis que par le droit national. Le projet de loi relatif à la protection des données personnelles déposé par le Gouvernement le 13 décembre dernier (*Proj. de loi AN n° 490, 13 déc. 2017 : JCP A 2017, act. 857*) vise donc à traiter en même temps tous ces aspects (1). Toutefois, dans son avis (CNIL, *délib. n° 2017-299, 30 nov. 2017*), après avoir salué cette adaptation du droit français au nouveau cadre européen, la CNIL regrette une « occasion manquée de procéder à un réexamen global du droit », qui aboutit à un texte manquant de lisibilité. Elle suggère à cette occasion plusieurs amendements. Il nous semble utile de compléter ces suggestions de la CNIL par d'autres pistes, visant notamment à diminuer les écarts entre la future loi modifiée dite « CNIL3 » et le RGPD, et à compléter le projet par une mise en cohérence du volet pénal (2).

### 1. Un projet de loi complexe

#### A. - Nécessité de légiférer

La loi *Informatique et Libertés*, qui date de 1978, a connu de nombreuses modifications depuis cette époque, notamment en 2004 à l'occasion de la transposition de la directive européenne 95/46/CE, et dernièrement par la loi du 7 octobre 2016 pour une République numérique (L. n° 2016-1321, 7 oct. 2016 : JO 8 oct. 2016 ; JCPA 2016, act. 774).

Toutefois, cette loi doit à nouveau impérativement être modifiée avant l'entrée en application le 25 mai 2018 du RGPD, et également pour transposer la directive européenne 2016/680 sur la protection des données dans les cas d'enquêtes et de poursuites pénales. Mais pourquoi donc le RGPD, qui est d'application directe, impose-t-il de légiférer ? Il y a plusieurs raisons à cela.

Tout d'abord, il est nécessaire d'abroger les dispositions nationales contraires au RGPD, par exemple le montant des sanctions de la CNIL, et de modifier celles dont la rédaction présente des différences notables avec celle des dispositions équivalentes du RGPD, par exemple la liste limitative des données dites « sensibles ». Il est également indispensable de revoir dans son intégralité le régime des formalités préalables, celles-ci étant dans la majorité des cas supprimées par le RGPD – bien entendu, des formalités nationales peuvent subsister en parallèle pour les traitements ne relevant pas du champ du RGPD.

Ensuite, le RGPD prévoit 56 marges de manœuvres nationales, pour lesquelles chaque État membre peut décider d'adopter des dispositions spécifiques – ou pas : ainsi pour les modalités des actions collectives, ou pour l'âge à partir duquel un mineur peut

consentir à un traitement de données lié à l'offre directe de services de la société de l'information.

## B. - Le projet de loi

Le projet se divise en cinq titres.

Le titre I traite des dispositions communes au RGPD et à la directive. Il modifie notamment les missions et les compétences de la CNIL, ainsi que ses procédures de sanction, créant par exemple une injonction sous astreinte à 100 000 euros par jour.

Le titre II du projet de loi traite des marges de manœuvre permises par le RGPD. Il ajoute notamment à la loi n° 78-17 un article 5-1 nouveau précisant le champ d'application territoriale de ces marges de manœuvre. Concernant les formalités préalables, il supprime le régime de déclaration actuel, ainsi que la plupart des formalités. Certaines subsistent, soit dans les cas prévus par le RGPD, comme l'utilisation du numéro de sécurité sociale, soit pour les traitements ne relevant pas du RGPD. Concernant les données de santé, le projet de loi procède à une réécriture complète du chapitre IX de la loi qui leur est consacré.

Le titre III du projet de loi transpose la directive 2016/680 sur la protection des données dans les cas d'enquêtes et de poursuites pénales. La nature de ces traitements justifie que les obligations des responsables ainsi que les droits des personnes soient adaptés : on comprendra aisément que le droit d'information ou le droit d'opposition puissent y être restreints.

Le titre IV du projet de loi prévoit une habilitation à ordonnance. Comme l'indique le texte, « *sans remettre en cause les choix du législateur dans le cadre du présent projet de loi, l'habilitation a pour objet de permettre au Gouvernement de prendre, dans un délai de six mois, une ordonnance pour procéder à une réécriture de l'ensemble de la loi du 6 janvier 1978 afin notamment d'améliorer son intelligibilité, de mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel et d'en prévoir l'application à l'outre-mer* ».

Enfin, le titre V du projet de loi, consacré aux dispositions finales, met notamment à jour les références internes de la loi, et fixe la date d'entrée en vigueur de la loi au 25 mai 2018.

## 2. Pistes d'amendements

Il convient tout d'abord de souligner la difficulté que représentait la rédaction de ce projet de loi. Comme rappelé plus haut, la future loi modifiée doit articuler les dispositions applicables aux traitements relevant respectivement du RGPD, de ses options nationales, de la directive 2016/680, ou du droit strictement national, avec à chaque fois éventuellement des droits et des obligations différents. En outre, il est temps de reconnaître que le RGPD lui-même est un monstre de 99 articles négociés dans l'urgence, souvent peu lisibles, chaque règle admettant des exceptions, et qu'il contient parfois des contradictions internes. Par conséquent, l'interprétation du RGPD est parfois délicate et sujette à caution, comme le reconnaît l'étude d'impact du projet de loi au détour d'un article (p. 94) : « *Le mécanisme mis en place par l'article 35.10 du règlement semble être le suivant (...)* ».

Dans ces conditions, on ne peut que saluer les efforts déployés pour rénover une loi qui fait figure de symbole, voire d'icône, tout en conservant la structure fondamentale.

### A. - Nécessité d'amender le projet

À la fin du projet de loi, l'habilitation du gouvernement à récrire le droit par ordonnance répond à une raison simple : le droit positif résultant de l'adoption du projet de loi manquera de lisibilité. Comme le souligne la CNIL dans son avis, « *la loi pourra induire en erreur le lecteur sur la portée de ses droits et obligations. En effet, des*

*dispositions formellement inchangées et toujours en vigueur de la loi de 1978 ne seront en réalité plus applicables, car substituées, dans leur champ, par les dispositions du règlement (...), tandis que la loi nationale ne comportera aucun écho à certains nouveaux droits ou nouvelles obligations posés par le règlement. D'autre part, la loi du 6 janvier 1978 ne donnera pas de grille de lecture permettant aux citoyens et aux responsables de traitement de comprendre les droits et obligations différenciés qui existeront demain dans les trois grands compartiments de la protection des données que seront le champ du règlement (à savoir les fichiers « civils et commerciaux », mais également certains fichiers relevant de l'administration), celui de la Directive (...) et, enfin, ce qui ne relève pas du champ du droit de l'Union ou relève du seul chapitre 2 du titre V du traité sur l'Union européenne (traitements intéressant la sûreté de l'État et la défense) ». Par conséquent, « la Commission appelle dès lors de ses vœux l'adoption des plus rapprochées de l'ordonnance annoncée, ainsi qu'une réécriture du droit français conforme aux principes ci-dessus, de manière à ce que la loi du 6 janvier 1978 puisse donner un mode d'emploi clair, ce qui est démocratiquement l'une de ses vocations ».*

En outre, la CNIL formule dans son avis quelques amendements qui lui semblent nécessaires au projet de loi.

De notre côté, il nous semble utile d'y ajouter quelques pistes d'amendements.

### B. - Suggestions supplémentaires

Dans l'attente de l'ordonnance, pendant plusieurs mois, responsables de traitements et personnes concernées risquent de demeurer dans l'incertitude quant à leurs droits et à leurs obligations.

La principale source de conflit réside dans la coexistence de dispositions de la loi Informatique et libertés et de dispositions différentes du RGPD. On pourrait être tenté d'abroger simplement les articles de la loi n° 78-17 redondants avec des articles du RGPD. Mais dans ce cas, plus aucune disposition n'existerait pour les traitements non couverts par le RGPD. Il faut donc, soit systématiquement recopier mot à mot ce dernier dans la loi, soit insérer dans toutes les dispositions nationales concernées un renvoi aux dispositions du RGPD correspondantes, en précisant leur champ d'application : ou bien elles ne s'appliquent que dans le champ du RGPD, ou bien on décide de les étendre aux traitements non concernés par le RGPD.

On peut noter que cet exercice a été effectué une fois dans le projet de loi : ce dernier ajoute à l'article 35 de la loi n° 78-17, consacré aux sous-traitants, un alinéa ainsi rédigé : « *Toutefois, dans le champ d'application du règlement (UE) 2016/679, le sous-traitant respecte les conditions prévues au chapitre IV de ce règlement* ».

Il est donc suggéré de généraliser cette solution, en l'adaptant bien entendu pour chaque disposition. Sont notamment concernés les articles 6, 7, 32, 34, 34 bis, 38, 39 et 40 de la loi, dont la rédaction diffère significativement des articles correspondants du RGPD.

Plus délicat est le cas du champ d'application territoriale. Alors que la loi actuelle s'applique (art. 5) lorsque le responsable de traitement ou les moyens de traitement se trouvent en France, le RGPD s'appliquera (art. 3) lorsque le responsable de traitement ou la personne concernée se trouveront dans l'Union européenne, ce à quoi le projet ajoute à la loi un article 5-1 nouveau selon lequel les options nationales du RGPD s'appliqueront pour les personnes résidant en France. Outre qu'il n'est pas évident pour le public de savoir, dans la future loi, quelles dispositions relèvent de chacun de ces champs, cette superposition de trois régimes d'application territoriale risque de mener à des contradictions ou à des conflits d'applicabilité dans leur mise en œuvre. Pour atténuer cette difficulté, il est suggéré d'aligner l'article 5 de la loi Informatique et libertés sur l'article 3 du RGPD.

Enfin, alors que le RGPD augmente sensiblement les sanctions financières en cas de violation de ses dispositions, le projet de loi harmonise les montants de l'article 45 de la loi, mais pas les articles 226-16 et suivants du Code pénal visés à l'article 50, ni son article 51 réprimant « *l'entrave à la CNIL* ». En outre, la rédaction de ces articles du Code pénal n'est plus adaptée à la situation, ignorant les obligations du RGPD et faisant référence à des formalités abrogées (demande d'avis, déclaration, norme simplifiée...). Il est

donc suggéré de profiter de ce projet de loi pour aligner les montants des amendes pénales sur les sanctions financières du RGPD, et pour rectifier la rédaction de ces articles quand nécessaire. Il conviendra de ne pas oublier les articles R. 625-10 à R. 625-13 du Code pénal, actuellement simples contraventions, mais qui répriment des infractions (non-respect des droits d'accès, de rectification, etc.) particulièrement sanctionnées par le RGPD : une requalification en délits s'impose.