26 janvier 2016

# A la une

**Département Protection des données personnelles - vie privée**

# LE PROJET DE LOI POUR UNE REPUBLIQUE NUMERIQUE OU UN AVANT-GOUT DU REGLEMENT GENERAL EUROPEEN SUR LA PROTECTION DES DONNEES

**Le projet de loi, s'il est adopté en l'état, permettra à la CNIL de prononcer des sanctions de plusieurs millions d'euros**

L'Assemblée nationale va voter aujourd'hui, le projet de loi pour une République numérique[1].

Ce projet de loi prévoit un grand nombre de dispositions dans des domaines très différents : par exemple sur l'ouverture des données publiques (open data), ou encore sur l'amélioration de l'accès de tous les citoyens au numérique, mais **apporte également un certain nombre de modifications importantes à la loi informatique et libertés.**

Certaines de ces modifications devancent purement et simplement le règlement général européen sur la protection des données (ci-après le « règlement européen »).

En effet, au mois de décembre 2015, le trilogue a trouvé un accord sur le texte du règlement européen[2] qui devrait être adopté définitivement au cours du premier semestre de cette année. Cependant, le législateur européen a décidé de laisser un délai de 2 ans aux organismes pour se préparer à l'entrée en vigueur de ce texte. Or, avec le projet de loi pour une République numérique, certaines dispositions proches de celles du règlement européen pourront entrer en vigueur bien avant. C'est, par exemple, le cas des dispositions concernant **le montant des sanctions financières pouvant être prononcées par la CNIL qui passent d'un maximum de 150 000 euros à 20 millions d'euros ou à 4% du chiffre d'affaires mondial d'une entreprise** dans certaines hypothèses.

Il est également intéressant de noter que des dispositions particulièrement importantes du règlement européen, qui consistent à consacrer la responsabilité des sous-traitants, ne sont pas reprises par le projet de loi. Les responsables de traitement seront donc les seuls à supporter la charge de la sanction prononcée.

Les principales évolutions du projet de réforme vont, tout comme le règlement européen, dans le sens de l'accroissement des droits des personnes (1ère partie) et de l'alourdissement des actions et sanctions à l'encontre des responsables de traitement (2ème partie).

## 1 - L'ACCROISSEMENT DE LA TRANSPARENCE ET DES DROITS DES PERSONNES

L'article 26 du projet de loi ajoute tout d'abord un alinéa à l'article 1er de la loi qui pose le principe selon lequel : *« Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ».*

### 1.1. La création du droit à la récupération et à la portabilité de données[3]

En l'état actuel du projet de loi, ce droit n'est pas inséré dans la loi informatique et libertés mais dans le Code de la consommation, et il est restreint aux services de courrier électronique et de stockage des données en ligne, alors même que le principe de portabilité des données prévu par le futur règlement européen s'appliquera à tous types de services.

Ainsi, les fournisseurs d'un service de courrier électronique devront permettre au consommateur de transférer les messages émis ou reçus, ainsi que la liste des contacts conservés par le système d'informations du fournisseur d'origine vers un autre fournisseur de service de courrier électronique, **et ce gratuitement**.

[1] http://www.assemblee-nationale.fr/14/dossiers/republique_numerique.asp
[2] http://europa.eu/rapid/press-release_IP-15-6321_en.htm

[3] Article 21 du projet de loi pour une République numérique

Par ailleurs, les fournisseurs d'un service de communication au public en ligne (c'est-à-dire les éditeurs de sites internet) devront proposer **gratuitement** une fonctionnalité permettant la récupération de tous fichiers mis en ligne par le consommateur, de toutes données résultant de l'utilisation du compte d'utilisateur et consultables en ligne, et des autres données associées au compte utilisateur.

Les fournisseurs devront également prendre *« toutes les mesures nécessaires à cette fin, en termes d'interface de programmation et de transmission des informations nécessaires au changement de fournisseur ».*

### 1.2. Le droit d'obtenir l'effacement des données concernant les mineurs et les personnes décédées

L'article 32 du projet de loi pour une République numérique prévoit la possibilité pour toute personne d'obtenir **l'effacement des données la concernant, collectées lorsqu'elle était mineure,** dans le cadre de l'offre de services de la société de l'information[4].

Cet article prévoit également un droit de conservation, d'effacement et de communication des données d'une personne **après son décès**.

Ainsi, toute personne pourra faire part de ses dernières volontés par le biais de **directives générales** et/ou de **directives particulières** :

- les **directives générales porteront sur l'ensemble des données** la concernant et seront confiées à un tiers de confiance numérique certifié par la CNIL,

- les **directives particulières seront destinées à des responsables de traitement désignés par ces directives** : une personne pourra ainsi rédiger des directives particulières destinées par exemple à Facebook concernant les données de son compte.

  Bien entendu, les directives particulières pourront être adressées à tous types de responsables de traitement, comme par exemple à l'employeur de la personne concernée, ou à son opérateur de communications électroniques.

Si le projet de loi prévoit que les directives générales seront conservées par un tiers de confiance, en l'état actuel du texte rien n'est prévu sur les modalités pratiques de la conservation des directives particulières par les responsables de traitement : ainsi les organismes et entreprises devront-ils conserver, parfois pendant des années, ces directives rédigées par des personnes dont ils traitent des données (salariés, clients, prospects, etc…) ?

### 1.3. La liste publique des formalités déposées auprès de la CNIL

Depuis son adoption en 1978, la loi informatique et libertés prévoit que toute personne peut demander à la CNIL la transmission de la liste des formalités déposées auprès de ses services par les responsables de traitement.

Cette disposition est relativement méconnue, et ses modalités d'exercice sont aujourd'hui peu aisées, puisqu'il convient d'adresser un courrier ou une télécopie à la CNIL, qui répond dans un délai très variable pouvant aller de plusieurs jours à plusieurs semaines.

Le projet de loi pour une République numérique comporte un article 26 ter prévoyant que la liste des formalités sera désormais accessible au public *« dans un format ouvert et aisément réutilisable*[5] *».*

Cette modification pourra, par exemple, permettre aux clients, aux salariés, ou encore aux concurrents d'une entreprise, mais aussi aux syndicats ou à des associations de consommateurs, de connaître aisément les formalités effectuées par les entreprises, et d'en déduire les formalités manquantes et ainsi le niveau de conformité de l'organisme ou de l'entreprise à la loi.

### 1.4. L'information sur la durée de conservation

Le projet de loi rajoute, tout comme le projet de règlement européen, l'obligation d'informer les personnes sur la durée pendant laquelle les données les concernant sont conservées.

Ceci signifie que les responsables de traitement devront modifier leurs mentions d'information des personnes, une première fois lors de l'entrée en vigueur du projet de loi pour une République numérique, et une nouvelle fois lors de l'entrée en vigueur du règlement européen.

En effet, l'obligation d'information des personnes telle qu'elle résulte du futur règlement européen sera encore bien plus lourde que celle qui résultera de la loi informatique et libertés modifiée par le projet de loi pour une République numérique.

Or, pour certaines organisations, le changement des mentions d'information représente aujourd'hui déjà, une charge de travail relativement importante.

### 1.5. L'exercice du droit d'accès en ligne

L'article 28 du projet de loi impose aux responsables de traitement qui ont collecté les données par voie électronique, de permettre aux personnes concernées d'exercer leurs droits d'accès, de rectification, de mise à jour, de verrouillage, d'effacement par voie électronique.

Le législateur considère en effet que l'exercice des droits des personnes s'effectue plus facilement et plus efficacement lorsqu'ils sont exercés par voie électronique plutôt que lorsqu'ils le sont par voie postale.

## 2. L'ALOURDISSEMENT DES SANCTIONS ET DES ACTIONS POSSIBLES A L'ENCONTRE DES RESPONSABLES DE TRAITEMENT

Les dispositions du projet de loi pour une République numérique les plus importantes sont incontestablement celles qui prévoient un alourdissement des sanctions susceptibles d'être prononcées par la CNIL.

[4] Ce principe connait un certain nombre d'exceptions lorsque par exemple le traitement des données est nécessaire pour exercer le droit à la liberté d'expression et d'information, ou pour respecter une obligation légale par exemple

[5] Il faut comprendre ici, accessible par internet

### 2.1. La possibilité pour la CNIL de prononcer certaines sanctions même lorsque la violation de la loi a cessé

A l'heure actuelle, **lorsqu'un responsable de traitement a violé la loi informatique et libertés mais que cette violation a cessé lors de l'intervention de la CNIL, la Commission ne peut pas prononcer d'autres sanctions qu'un avertissement**.

C'est le cas par exemple lorsqu'une entreprise perd, du fait d'une faille de sécurité, plusieurs millions de données, mais qu'elle prend des mesures correctives avant que la CNIL ne soit informée de cette faille : dans une telle hypothèse, la seule sanction encourue est l'avertissement.

Si le projet de loi est adopté en l'état, la CNIL pourra, dans une telle hypothèse, prononcer un avertissement, mais également une sanction financière ou une injonction de cesser le traitement.

### 2.2. Le montant maximal des sanctions est fixé à 20 millions d'euros et à 4% du chiffre d'affaires mondial pour les entreprises

Actuellement, la CNIL peut prononcer des sanctions financières d'un montant maximal de 150 000 euros et de 300 000 euros en cas de récidive.

Le projet de loi prévoit d'aligner le montant maximum des sanctions encourues sur celui prévu par le règlement européen, à savoir :

- à un montant maximal de 20 million d'euros pour tous les responsables de traitement (entreprises, organismes publics, associations, etc…)[6] **ou**

- pour les entreprises à 4% du chiffre d'affaires annuel total au niveau mondial, si ce montant est supérieur à 20 millions d'euros.

En cas de violation de l'obligation de sécurité, il est prévu un maximum moins important, à savoir une sanction maximale de 10 millions d'euros pour l'ensemble des responsables de traitement ou de 2% du chiffre d'affaires au niveau mondial pour les entreprises, si ce montant est supérieur à 10 millions d'euros.

A cet égard, étant donné que le projet de loi pour une République numérique ne prévoit aucune sanction à l'encontre des sous-traitants, en cas de survenance d'une faille de sécurité, seul le responsable de traitement risquera une sanction pouvant aller jusqu'à 10 millions d'euros ou 2% de son chiffre d'affaire mondial, et ce même si la faille de sécurité est survenue en partie à cause du sous-traitant.

Si ces dispositions sont adoptées en l'état, et dans l'attente de l'entrée en vigueur du règlement européen, la CNIL sera très vraisemblablement l'autorité de protection des données personnelles disposant du pouvoir de prononcer les sanctions les plus lourdes.

Ceci représentera incontestablement un bouleversement pour les responsables de traitement, dans la mesure où, à l'exception de Google - à l'encontre de laquelle la CNIL a prononcé des sanctions de 100 000 euros et de 150 000 euros - le montant des sanctions prononcées par la CNIL sur une année est relativement faible.

En effet, pour l'année :

- 2013 le montant total[7] des sanctions financières prononcées par la CNIL s'élève à 43 000 euros.
- 2014, le montant total des sanctions s'élève à 229 001 euros, dont une sanction de 150 000 euros à l'encontre de Google.
- 2015, en l'état actuel des informations diffusées par la CNIL, le montant total des sanctions financières s'élève à 17 000 euros.

Une hausse significative du montant des sanctions prononcées par la CNIL est donc inévitable. En effet, la Commission perdrait toute crédibilité si elle continuait à prononcer un montant total de sanction de 17 000 euros sur une année, alors même que le montant maximal prévu par la loi aura augmenté dans des proportions considérables.

A noter enfin que le projet de loi n'a pas, en dépit de la lourdeur des sanctions, pris le soin d'instaurer un double degré de juridiction.

Ce qui signifie qu'un responsable de traitement qui se sera vu infliger une sanction de 20 millions d'euros disposera seulement d'un recours devant le Conseil d'Etat en premier et dernier ressort.

Il convient d'ajouter à cela que les décisions de la CNIL sont exécutoires de plein droit, et que le recours n'est pas suspensif : le responsable de traitement devra donc payer l'amende prononcée par la CNIL, sauf à obtenir la suspension de la décision de sanction par le biais d'une procédure de référé, toujours devant le Conseil d'Etat.

### 2.3. La condamnation à informer les personnes concernées de l'existence de la sanction

Si la réforme de la loi informatique et libertés est adoptée en l'état, la décision de la CNIL prononçant la sanction pourra également contraindre le responsable de traitement à informer individuellement chacune des personnes concernées de l'existence de la sanction.

Bien entendu, le coût de cette information individuelle sera supporté par le responsable de traitement sanctionné.

### 2.4. La création d'actions collectives en cas de violation de la loi informatique et libertés

Conformément à la volonté de la Présidente de la CNIL, le projet de loi prévoit également la création **d'actions collectives** devant les juridictions civiles afin **d'obtenir la cessation d'une violation de la loi informatique et libertés.**

Les organisations désignées par le projet de loi comme pouvant agir sont :

- Les associations ayant pour objet la protection de la vie privée et des données personnelles,

- Les associations de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 411-1 du Code de la consommation,

- Les organisations syndicales de salariés concernant les traitements portant sur des salariés,

[6] La seule exception prévue aujourd'hui par le projet de loi est l'Etat, qui ne pourra pas recevoir de sanction financière

[7] Il convient de noter que le montant d'une sanction prononcée par la CNIL n'a pas été rendu public

- Toute organisation formée aux seules fins d'entreprendre l'action collective concernée.

Il convient de noter cependant que l'organisme ne pourra pas saisir la juridiction compétente sans avoir, au préalable, effectué des démarches auprès du responsable de traitement en vue d'obtenir la cessation de la violation.

## 3. A QUOI S'ATTENDRE DANS LES PROCHAINS MOIS ?

Bien entendu le processus d'adoption du texte n'est pas achevé, et il appartient désormais au Sénat de se prononcer, mais si le projet venait à être peu modifié d'ici à son adoption, son entrée en vigueur risque d'entraîner des bouleversements importants.

A cet égard, l'accroissement considérable des sanctions combiné à l'impossibilité de prononcer des sanctions à l'égard des sous-traitants va compliquer singulièrement les négociations des contrats, notamment des contrats informatiques. Les clients ne pouvant, encore moins qu'auparavant, admettre les limitations, voire les exclusions de responsabilité que l'on trouve dans certains contrats.

Ce projet de loi, s'il est adopté en l'état risque également de changer le quotidien de nombreux CIL[8]:

- ceci permettra une adaptation progressive à l'entrée en vigueur du règlement européen, prévue pour 2018.

- dans les groupes multinationaux, les maisons mères étrangères chercheront certainement, encore plus qu'aujourd'hui, à intervenir dans le choix du CIL. Elles voudront en effet s'assurer que le CIL français est en mesure d'assumer une telle responsabilité.

- Certains CIL pourraient ressentir une certaine pression dans le cadre de leur mission qui consiste essentiellement à veiller au respect de la loi informatique et libertés. Quel CIL ne réfléchira pas à deux fois lors de l'étude d'un projet en se disant qu'une erreur de jugement de sa part pourrait, dans le pire des cas, conduire au prononcé d'une sanction de plusieurs millions d'euros à l'encontre de son organisme ?

- Pour les entreprises ou organismes qui disposent de CIL à temps partiel ou ayant peu de moyens, les dirigeants risquent de devoir réagir assez vite, et se demander si n'est pas venu le temps de changer l'organisation : allouer plus de temps ou de moyens au CIL ? mettre en place un accompagnement en interne ou en externe du CIL ? approfondir sa formation ?

Pour terminer, et même si l'on imagine bien que les sanctions les plus lourdes seront réservées à des sociétés très importantes, le projet de loi prévoit que, pour définir le montant de la sanction, la CNIL devra prendre en compte notamment la gravité du manquement ou encore le type de données personnelles concernées.

Or, de nos jours, des start-up peuvent traiter des données très sensibles et commettre des infractions très graves, parce qu'elles n'ont ni le temps ni les moyens de faire valider leur projet d'un point de vue juridique.

Que fera la CNIL dans une telle hypothèse ? Est-ce qu'elle estimera que la sanction doit-être légère à partir du moment où le responsable de traitement n'a pas les moyens d'assumer la charge d'une sanction financière lourde ? Ou prononcera-t-elle une sanction à la hauteur de la gravité des faits, quitte à mettre en jeu la survie de l'entreprise ?

Il ne s'agit pas là d'une hypothèse d'école, en effet, aujourd'hui beaucoup de personnes utilisent les produits et/ou services de PME lorsqu'elles acquièrent certains objets connectés, ou utilisent des applications mobiles, et ces outils peuvent bien souvent collecter des données particulièrement sensibles.

**EN BREF :**

- ✓ Introduction d'un **droit à la portabilité des données** pour les services de courrier électronique de stockage des données en ligne
- ✓ Possibilité de faire part de **ses volontés concernant le traitement de ses données après sa mort** par le biais de directives générales et particulières
- ✓ Une **information plus claire et plus complète** sur les traitements réalisés, avec l'introduction des **durées de conservation** sur les mentions d'information
- ✓ Les pouvoirs de sanction de la CNIL seront portés à **20 millions d'euros ou à 4% du chiffre d'affaire annuel mondial pour les entreprise**s, si ce montant est supérieur ;
- ✓ Possibilité pour la CNIL, lors du prononcé d'une sanction, de contraindre le responsable de traitement à **informer individuellement** toutes les personnes concernées de **l'existence de la sanction**
- ✓ Création **d'actions collectives** afin d'obtenir la cession de violation à la loi informatique et libertés.

**P.D.G.B Société d'Avocats**
174, avenue Victor Hugo
75116 Paris
Tél. : 00 (33) 01.44.05.21.21
www.pdgb.com
helene.lebon@pdgb.com

Hélène LEBON - Sandra TUBERT

[8] « CIL » pour correspondant informatique et libertés ou correspondant à la protection des données