Commission Nationale de l'Informatique et des Libertés

**13 janvier 2015**

# Propositions de la CNIL sur les évolutions de la loi informatique et libertés dans le cadre du projet de loi numérique

Le Gouvernement avait annoncé, au mois de février 2013, à l'occasion d'un séminaire sur le numérique, son intention de déposer un projet de loi au cours de la législature. La CNIL a alors engagé une réflexion qui l'a conduite, en mars 2014, à présenter plusieurs propositions d'évolution législative au Gouvernement.

Plusieurs rapports ont depuis contribué à enrichir le débat, parmi lesquels l'étude annuelle 2014 du Conseil d'Etat sur le numérique et les droits fondamentaux.

Dans le cadre de la consultation confiée au Conseil national du numérique, la CNIL verse au débat public les propositions qu'elle avait présentées au Gouvernement. Elle s'est en outre fortement engagée dans la journée contributive du 9 janvier, à Strasbourg (animation de deux ateliers participatifs). Lors du discours d'ouverture, la Présidente de la CNIL, Isabelle Falque-Pierrotin y a notamment rappelé, les principes fondamentaux qui doivent structurer les réflexions et actions concrètes en matière de protection des données.

Ces propositions concernent les quatre principaux acteurs de l'écosystème « informatique et libertés » : la personne, les entreprises, les pouvoirs publics et la CNIL.

Concrètement, cinq axes peuvent se dégager :

1. **Le renforcement de l'effectivité des droits pour les personnes**
2. **La simplification des formalités et des règles applicables pour les entreprises**
3. **L'amélioration du cadre juridique de certains traitements publics**
4. **Le renforcement des relations entre la CNIL et les pouvoirs publics**
5. **L'adaptation des pouvoirs de la CNIL, notamment en vue de renforcer l'efficacité et la crédibilité de la politique de contrôle et de sanction**

Les propositions de modifications législatives doivent être combinées avec trois exigences qu'il convient de garder à l'esprit. La première est la discussion actuelle sur **le projet de règlement européen** ; les modifications éventuelles de la loi informatique et libertés devront naturellement être compatibles avec le règlement à venir dont l'adoption définitive est attendue au cours de l'année 2015. La deuxième tient au cadre juridique actuel, issu de **la directive de 1995**, que les modifications ne sauraient contredire. La troisième tient à la portée économique croissante de la législation sur les données personnelles, qui conduit à **veiller à la cohérence des dispositions envisagées par rapport aux dispositions applicables dans les autres pays de l'Union**. En revanche, ces mêmes modifications peuvent être l'occasion de valoriser les bonnes pratiques en la matière, qui constituent, dans l'univers numérique, un élément de compétitivité.

Enfin, la discussion autour d'une réforme du cadre juridique prescrit par loi ordinaire pourrait être utilement complétée par une réflexion sur la constitutionnalisation du droit à la protection des données personnelles.

## 1. Le renforcement de l'effectivité des droits pour les personnes

Face à cet objectif global de faire de l'univers numérique un espace de droits et de libertés, l'individu a un rôle particulier à jouer et il est essentiel de renforcer ses droits. La principale difficulté, sur ce point, tient à l'articulation avec le futur règlement qui prévoit de nouveaux droits au bénéfice de l'individu (droit à l'oubli, à la portabilité des données, etc.)
Cependant, plusieurs propositions peuvent d'ores et déjà être retenues à cadre européen constant :

- **Le renforcement du droit d'accès : parmi les droits actuellement reconnus, le droit d'accès apparaît comme peu utilisé, alors qu'il est « premier » en ce qu'il permet à toute personne de savoir ce qu'un responsable de traitement a sur elle. Ce droit – qui pourrait être renommé « droit à la connaissance de ses données » ou « droit à la transparence des données » - pourrait être utilement renforcé, à la fois dans son contenu et dans ses modalités**. Dans son contenu, l'article 39 de la loi pourrait être modifié pour donner aux individus un accès aux informations relatives aux durées de conservation et, de manière plus systématique, sur l'origine des données, sur demande effectuée auprès du responsable de traitement. S'agissant des modalités, il est proposé d'introduire explicitement, dans une logique de simplification, **la possibilité pour les individus d'exercer les droits conférés par les articles 38 à 40 (opposition, accès, rectification) aussi par voie électronique**. Une telle possibilité n'ouvrirait pas de risques de fraude supplémentaire, dans la mesure où l'article 92 du décret n° 2005-1309 du 20 octobre 2005 prévoit que toute demande écrite tendant à l'exercice de ces droits doit être accompagnée, pour être recevable, de la copie d'un titre d'identité. De même, pourrait être introduite l'obligation du responsable de traitement de **transmettre aux personnes une preuve de l'exercice de leurs droits afin de faciliter le régime de la preuve** (par exemple, permettre aux personnes, exerçant leur droit d'opposition via un lien de désabonnement, de recevoir un email prouvant l'exercice de ce droit, constitutif d'une preuve en cas de non-respect de celui-ci).

- **La protection des mineurs** : **la loi de 1978 ne comporte aucune disposition propre aux mineurs,** alors même que l'immense majorité d'entre eux utilise, notamment, les réseaux sociaux, et que les questions de e-réputation sont régulièrement liées à des données mises en ligne avant l'âge de la majorité. Il pourrait donc être proposé d'introduire dans la loi la possibilité d'obtenir l'effacement, notamment en ligne, de données à caractère personnel de mineurs, via l'exercice du droit d'opposition. Il conviendrait, soit de prévoir que l'exercice d'un tel droit est inconditionnel s'agissant des données portant sur une personne mineure (ce qui reviendrait à supprimer l'exigence d'un « motif légitime », actuellement prévu à l'article 38, dans cette hypothèse), soit de considérer que le fait que les données portent sur une personne mineure constitue en soi un motif légitime. Ce droit pourrait être exercé sur toute donnée collectée, traitée ou mise en ligne avant les 18 ans de la personne concernée. Ceci permettrait ainsi d'exercer un « droit à l'oubli » protecteur de la vie privée des intéressés, qui sont les plus vulnérables dans l'univers numérique.

## 2. La simplification des formalités et des règles applicables pour les entreprises

Dans la logique du projet de règlement et des efforts engagés par la CNIL depuis déjà plusieurs mois, il parait opportun d'alléger les formalités pesant sur les responsables de traitement.

- **Simplifier les formalités relatives aux transferts internationaux lorsque les entreprises s'engagent dans un régime de garanties substantielles :** les demandes d'autorisation pour les transferts internationaux de données connaissent une forte croissance (près de 1500 autorisations en 2013). En outre, l'outil des « BCR » (*binding corporate rules* ou règles d'entreprise contraignantes), développé par les CNILs européennes, a fait ses preuves, mais ne se traduit pas par une simplification substantielle des formalités : en effet, une entreprise qui adopte des BCR doit continuer à présenter des demandes d'autorisations de transferts auprès de la CNIL, celles-ci faisant simplement l'objet d'un examen allégé. Si les BCR ne semblent pas pouvoir constituer des autorisations de transferts en tant que telles au regard des termes de la directive de 1995, leur existence juridique pourrait cependant être consacrée dans les textes, et donner lieu à l'adoption systématique d'une autorisation unique délivrée à l'entreprise pour les transferts intervenant dans ce cadre.

Parallèlement, la CNIL poursuit le processus de simplification administrative à travers les trois outils que sont les dispenses de déclarations, les normes simplifiées et les autorisations uniques, une disposition législative n'apparaissant pas nécessaire sur ce point.

## 3. L'amélioration du cadre juridique de certains traitements publics

Les relations avec les pouvoirs publics et le contrôle des fichiers publics constitue l'un des enjeux de la loi sur le numérique.

- **L'évolution des règles dans le domaine des fichiers de police et de souveraineté :**

Comme les révélations d'Edward Snowden l'ont récemment dévoilé, il est nécessaire de donner des garanties supplémentaires au public en matière de contrôle des fichiers de souveraineté. Ceux-ci peuvent en effet être, en vertu de l'article 44 de la loi de 1978, exonérés de tout contrôle de la CNIL, autre que l'examen de fiches particulières dans le cadre de l'exercice du droit d'accès indirect. Ces fichiers (DCRI, DGSE,…) sont ainsi les seuls, en France, à ne pouvoir faire l'objet d'un contrôle de la CNIL, et plus généralement d'une autorité administrative indépendante. Il est proposé d'étendre à ces fichiers le contrôle par la CNIL, selon des modalités tenant compte de leurs spécificités (contrôle par les seuls commissaires du droit d'accès indirect, qui ont déjà accès à ces fichiers, selon la procédure 'confidentiel défense', avec résultats communiqués au seul ministre de tutelle et au Premier ministre). Il convient de souligner que ce contrôle ne porterait naturellement que sur le respect de la loi informatique et libertés, dans les conditions de mise en œuvre desdits fichiers, et en aucun cas sur l'activité des services de renseignement. Plus généralement, d'autres mesures pourraient être envisagées :

- **L'instauration d'un droit d'accès direct aux fichiers d'antécédents pour les victimes** : il est proposé de permettre un accès direct aux données contenues dans les fichiers d'antécédents judiciaires pour les personnes non mises en cause à quelque titre que ce soit (victimes, plaignants…). Une telle faculté serait exclue pour une personne ayant à la fois le statut de victime et de mis en cause ; le droit d'accès indirect ne se justifie en effet que par la nécessité d'empêcher qu'une personne mise en cause sache exactement ce que les services de police savent sur elle (plaintes, etc.). En revanche, une victime ou un plaignant ne peut, par construction, être soumis aux mêmes exigences. Outre que cela permettrait de désengorger partiellement l'activité de la CNIL et des services de police et de gendarmerie en matière de droit d'accès indirect, une telle mesure accroitrait la transparence de ces fichiers.

- **La mise en place d'un régime d'expérimentation pour les fichiers des articles 26 et 27 (autorisation des traitements publics sensibles après avis de la CNIL) :** ceci fait l'objet d'une demande forte, notamment dans la mesure où la constitution de bases de données est souvent précédée d'expérimentations ponctuelles et, potentiellement, sans lendemain. A titre d'exemple, l'expérimentation pendant quelques mois d'un dispositif biométrique à l'entrée de locaux « secret défense » nécessiterait l'adoption d'un décret en Conseil d'Etat. Il pourrait donc être envisagé d'alléger le niveau d'exigence du dossier technique, lorsqu'il s'agit de traitements mis en œuvre pour une durée, sur un territoire et pour une population limités. S'agissant des formalités préalables, si une telle évolution était retenue, il conviendrait de compenser l'allègement des exigences techniques par un renforcement du contrôle de la CNIL, qui devrait alors autoriser ces expérimentations, en statuant dans un délai court (deux mois). Pour les administrations concernées, cela se traduirait en tout état de cause par des délais de mise en œuvre plus courts (puisque les articles 26 et 27 requièrent l'adoption d'un acte réglementaire). En outre, de telles expérimentations devraient faire l'objet de contrôles *a posteriori* systématiques dès lors que les administrations responsables décideraient de les généraliser ou de les étendre.

### 4. Le renforcement des relations entre la CNIL et les pouvoirs publics

Plusieurs évolutions, sur lesquelles la Commission a déjà été amenée à prendre position, pourraient être apportées :

- **La saisine de la Commission sur les propositions de loi** : actuellement, la CNIL participe à plus d'une trentaine d'auditions par an au Parlement, ce qui témoigne de l'importance et de la fréquence du recours à son expertise. Donner la possibilité, pour les présidents des deux assemblées parlementaires, de saisir la Commission pour avis sur les propositions de loi, serait dès lors particulièrement opportun. Une telle faculté

serait enfermée dans des délais spécifiques afin de ne pas ralentir la procédure parlementaire,

- Par ailleurs**, il est proposé d'opérer une clarification de l'article 11 4°) a), relative aux saisines de la CNIL sur les projets de loi.** Cet article prévoit en effet actuellement que la CNIL est saisie pour avis sur « tout projet de loi ou de décret relatif à la protection des données personnelles », ce qui conduit parfois à des interprétations divergentes, la création d'un fichier par la loi n'étant pas toujours regardée comme relevant de la « protection » des données personnelles au sens de cet article.

## 5. L'adaptation des pouvoirs de la CNIL, notamment en vue de renforcer l'efficacité et la crédibilité de la politique de contrôle et de sanction

Face à certaines faiblesses et difficultés constatées, plusieurs modifications pourraient permettre de rendre la politique de contrôle et de sanction de la Commission plus crédible, efficace et rapide, et ainsi plus adaptée à la nouvelle réalité de son activité.

### 5.1. La coopération internationale

- **L'échange d'informations confidentielles entre la Commission et ses homologues non européens** : il est proposé que la Commission soit désormais autorisée à échanger des informations confidentielles, diligenter des contrôles ou initier des procédures coercitives dans le cadre de ses actions de coopération avec ses homologues non européens, comme elle peut d'ores et déjà le faire avec ses partenaires des Etats membres de l'Union européenne en vertu de l'article 49 de la loi du 6 janvier 1978. En effet, l'habilitation actuelle est limitée à ces seuls pays, interdisant ainsi une coopération administrative sur des dossiers particuliers avec des autorités tierces, y compris pour les pays reconnus comme offrant une protection adéquate au sens de l'article 25 de la Directive 95/46/CE. Une telle coopération serait subordonnée à des conditions strictes fixées par la loi, et à la conclusion d'une convention bilatérale entre autorités. L'Autorité des marchés financiers, l'autorité de contrôle prudentiel ou l'autorité de la concurrence disposent d'ores et déjà de ce pouvoir de coopération internationale dans des conditions similaires (article L632-7 du CMF ; article L462-9 du Code de commerce, modifié par Ordonnance n°2008-1161 du 13 novembre 2008).

### 5.2. Le renforcement de l'efficacité et de la crédibilité des pouvoirs répressifs

La procédure retenue pour la CNIL, qui distingue les pouvoirs d'instruction (contrôle, mise en demeure, désignation d'un rapporteur pour saisine de la formation restreinte), relevant des pouvoirs propres du président, et les pouvoirs de sanction, relevant de la seule formation restreinte, ont été regardés par le Conseil d'Etat comme conformes aux exigences constitutionnelles par une décision de mars 2012. Cette procédure est d'ailleurs l'une des références dans les réflexions qui ont conduit à l'évolution des procédures devant d'autres autorités. Elle n'a donc pas vocation à évoluer sur un plan procédural.

En revanche, quelques adaptations de fond pourraient être envisagées :

- **Etudier la possibilité, lorsque l'urgence et la gravité particulière des faits le justifient, d'ordonner la suspension du traitement le temps de la mise en demeure :** actuellement, lorsqu'un traitement est mis en œuvre illégalement ou porte une atteinte grave à la vie privée, seule la formation restreinte peut ordonner la cessation de celui-ci, au terme d'une procédure de mise en demeure puis sanction. Le président de la CNIL peut donc mettre en demeure un responsable de traitement de se mettre en conformité, tout en laissant « vivre » un traitement illégal pendant ce temps. Il est donc proposé d'engager une étude juridique approfondie sur la possibilité pour le bureau, soit d'ordonner la suspension du traitement litigieux jusqu'à ce que la mise en conformité soit effective ou que la formation restreinte se soit prononcée, soit de saisir le juge en référé.

- **Elargir le champ du référé judiciaire** : actuellement la CNIL a la possibilité de saisir le juge des référés, mais uniquement pour que soient mises en œuvre, sous astreinte, les « mesures de sécurité » nécessaires. Il est proposé de supprimer les mots « de sécurité » pour que la CNIL puisse, de manière générale, saisir le juge des référés de toute demande tendant, notamment, à l'exécution de ses décisions de sanctions ou à la suspension d'un traitement (cf. § précédent).

- **Créer une action collective** en matière de protection des données personnelles est également régulièrement évoquée : la CNIL soutient une telle proposition. Toutefois, la question se pose de savoir si une telle action spécifique doit être introduite à l'occasion du projet de loi numérique, ou si elle a vocation à constituer une déclinaison d'une action collective qui serait inscrite dans un cadre plus général, appréciation qui relève du Parlement.

- **Augmenter le montant maximal des sanctions, qui est de 150 000 euros maximum aujourd'hui.** Le projet de règlement à venir prévoit une augmentation substantielle du niveau de sanction (5% du chiffre d'affaires mondial dans la limite d'un milliard d'euros dans la version de compromis adoptée par le Parlement européen), mais il n'entrera pas en vigueur, en tout état de cause, avant deux ans. Une modification du montant de sanction est donc envisageable dans cette attente. Un tel montant pourrait utilement être exprimé en valeur absolue et en pourcentage du chiffre d'affaires, ce double plafond étant de nature à couvrir les hypothèses où il n'y a pas de chiffre d'affaires (associations, par exemple) et à garantir, dans les autres cas, la proportionnalité du dispositif par rapport à la capacité financière de l'entité sanctionnée.

- **Accélérer le possible déclenchement d'une procédure de sanction pécuniaire :** actuellement, lorsque la situation est particulièrement urgente ou que le manquement n'appelle plus de correction, le président de la CNIL peut décider de saisir directement la formation restreinte, sans mise en demeure préalable. Toutefois, cette formation ne peut alors prononcer qu'un avertissement, le cas échéant public, alors même qu'il s'agit souvent de cas graves mais limités dans le temps (comme, par exemple, une faille de sécurité ponctuelle qui n'appelle plus de mise en conformité – donc de mise en demeure – mais qui, pour autant, a effectivement causé un préjudice). Pourrait donc

être introduite la possibilité, pour le président, de désigner directement, sans mise en demeure préalable, un rapporteur aux fins de proposer à la formation restreinte le prononcé d'une sanction pécuniaire, le cas échéant publique, notamment lorsque le manquement constaté n'appelle plus, à la date de décision, de mesure de correction.

- **Reconnaître une coresponsabilité (coresponsable de traitement)** : actuellement, la reconnaissance d'une éventuelle coresponsabilité, si elle est admise par la directive 95/46, n'a jamais été transposée explicitement en droit interne. Pourtant, elle constituerait une réponse juridique pertinente face à certaines incohérences révélées par l'articulation entre responsables de traitements et sous traitants. La consécration d'un statut de coresponsabilité permettrait ainsi de mieux refléter la réalité de l'implication de différents organismes dans la mise en œuvre d'un traitement « en chaîne ».