N° 330

SÉNAT

SESSION ORDINAIRE DE 2009-2010

Enregistré à la Présidence du Sénat le 24 février 2010

RAPPORT

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de loi de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER visant à **mieux garantir** *le* **droit** *à la* **vie privée** *à l'***heure** *du* **numérique**,

Par M. Christian COINTAT,

Sénateur

(1) Cette commission est composée de : M. Jean-Jacques Hyest*, président ;* M. Nicolas Alfonsi, Mme Nicole Borvo Cohen-Seat, MM. Patrice Gélard, Jean-René Lecerf, Jean-Claude Peyronnet, Jean-Pierre Sueur, Mme Catherine Troendle, M. François Zocchetto*, vice-présidents ;* MM. Laurent Béteille, Christian Cointat, Charles Gautier, Jacques Mahéas*, secrétaires ;* M. Alain Anziani, Mmes Éliane Assassi, Nicole Bonnefoy, Alima Boumediene-Thiery, MM. Elie Brun, François-Noël Buffet, Gérard Collomb, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Marie-Hélène Des Esgaulx, M. Yves Détraigne, Mme Anne-Marie Escoffier, MM. Pierre Fauchon, Louis-Constant Fleming, Gaston Flosse, Christophe-André Frassa, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Mmes Jacqueline Gourault, Virginie Klès, MM. Antoine Lefèvre, Dominique de Legge, Mme Josiane Mathon-Poinat, MM. Jacques Mézard, Jean-Pierre Michel, François Pillet, Hugues Portelli, Bernard Saugey, Simon Sutour, Richard Tuheiava, Alex Türk, Jean-Pierre Vial, Jean-Paul Virapoullé, Richard Yung.

Voir le(s) numéro(s) :

Sénat : **93**, **317** et **329** (2009-2010)

S O M M A I R E

LES CONCLUSIONS DE LA COMMISSION DES LOIS

La commission des lois, réunie le mercredi 24 février 2010 sous la présidence de **M. Jean-Jacques Hyest, président**, a procédé à l'examen du **rapport** de **M. Christian Cointat** et du **texte proposé** par la **commission** pour la **proposition** de **loi n° 93** (2009-2010), présentée par Mme Anne-Marie Escoffier et M. Yves Détraigne, **tendant** à **mieux garantir le droit à la vie privée à l'heure du numérique.**

M. Christian Cointat, rapporteur, a souligné que la proposition de loi traduisait nombre de recommandations figurant dans le rapport d'information des mêmes auteurs.

Tout en souscrivant largement aux objectifs de cette proposition de loi, la commission a cherché à parvenir à un meilleur équilibre entre la protection des données et la liberté des acteurs.

La commission a intégré au texte de la proposition de loi **22 amendements de son rapporteur**, ainsi que **4 amendements** du Gouvernement, de la commission de la culture et de nos collègues M. Alex Türk et M. Charles Gautier.

Ces amendements tendent principalement à :

- **assouplir le principe de consentement préalable en matière de « cookies »** dans le double souci de ne pas entraver la fluidité de la navigation des internautes et de ne pas remettre en cause le modèle économique d'Internet (article 6) ;

- clarifier l'exercice du « **droit à l'oubli** » ;

- **conforter le statut et les missions du Correspondant « informatique et libertés » (CIL),** dont elle a confirmé le **caractère obligatoire** lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre (article 3) ; elle a par ailleurs rétabli le principe d'un avis simple de la CNIL (et non d'un avis conforme comme le prévoyait la proposition de loi) pour la démission d'office du CIL ;

- **renforcer l'efficacité et la légitimité de la CNIL**, en précisant que les quatre parlementaires membres de la CNIL doivent être désignés *« de manière à assurer une représentation pluraliste »* (article 2 *bis*), en prévoyant la publicité des avis de la CNIL chaque fois qu'un fichier de police est créé (article 5 *bis*) et en permettant à la CNIL d'effectuer des visites inopinées après autorisation préalable du juge des libertés et de la détention (article 9 *bis*) ;

- **mieux encadrer par rapport au droit actuel la création des fichiers de police** en prévoyant que tout fichier créé par arrêté ou par décret doit appartenir à au moins une des finalités que la commission a limitativement énumérées. A défaut, seul le législateur est compétent (article 4) ;

La commission des lois a adopté la proposition de loi **ainsi rédigée**.

Mesdames, Messieurs,

« *L'informatique a apporté un changement de dimension : elle a introduit, en effet, une capacité de mémorisation considérable au point que certains peuvent craindre qu'elle ne porte atteinte à l'un des droits les plus fondamentaux de l'être humain : le droit à l'oubli* ».

De manière prémonitoire, ce constat d'une brûlante actualité a été établi il y a plus de trente ans par notre regretté collègue M. Jacques Thyraud dans son rapport, fait au nom de la commission des lois du Sénat, sur le projet de loi qui a abouti à la loi du 6 janvier 1978 « informatique et libertés »[1].

La progression fulgurante d'**Internet** depuis une dizaine d'années donne un **relief particulier** à ce propos visionnaire. En effet, les informations mises en ligne deviennent instantanément universelles dans l'espace et le temps, d'autant plus que, même diffusées sur des sites très variés et sur des périodes très étendues, elles peuvent aisément resurgir au moyen des moteurs de recherche qui permettent en un seul clic d'agréger des sources d'information qu'il aurait été pratiquement impossible de réunir auparavant.

Face à ce constat, votre commission des lois a confié à nos collègues Anne-Marie Escoffier et Yves Détraigne une réflexion sur le respect de la vie privée à l'heure des mémoires numériques. Les recommandations qu'ils ont formulées dans leur rapport d'information, publié au nom de la commission des lois le 27 mai 2009, ont été **traduites** pour partie dans la présente **proposition de loi**.

Ce texte vise, tout d'abord, à rendre l'individu **acteur de sa propre protection** en le sensibilisant, au cours de sa scolarité, aux dangers de l'exposition de soi et d'autrui sur Internet. Il propose également de donner une plus grande effectivité au **droit à l'oubli numérique**. Il comporte enfin de **nombreuses autres dispositions** tendant à renforcer la protection des données personnelles.

Tout en souscrivant largement aux objectifs de cette proposition de loi, votre commission a souhaité la **modifier** afin de parvenir à un **meilleur équilibre** entre la protection des données et la liberté des acteurs. Elle souhaite par ailleurs que cette proposition de loi soit perçue à l'étranger comme un nouveau signal fort de notre pays en faveur d'un renforcement de la

[1] *Rapport n° 72, 1977-1978*.

protection des données personnelles, à l'heure où des initiatives sont lancées pour faire évoluer le cadre juridique communautaire -et à terme international- dans ce domaine, trente ans après la loi « informatique et libertés », précurseur en la matière.

I. LA LOI « INFORMATIQUE ET LIBERTÉS » : UN CADRE JURIDIQUE PROTECTEUR DE LA VIE PRIVÉE

A. DE NOUVELLES MENACES POUR LA VIE PRIVÉE…

Comme nos collègues Anne-Marie Escoffier et Yves Détraigne le soulignent dans leur rapport d'information sur « *la vie privée à l'heure des mémoires numériques* »[1], la vie privée, valeur fondamentale de nos sociétés, n'en est pas moins confrontée, depuis quelques années, à l'apparition de « *nouvelles mémoires numériques* », conséquence de nombreuses évolutions technologiques ayant pour effet principal ou incident de collecter des données permettant de suivre un individu dans le temps et l'espace.

Trois grandes évolutions sont ainsi identifiées dans le rapport :

- la recherche d'une sécurité collective toujours plus infaillible ;

Le droit à la vie privée est né historiquement de la volonté de protéger la sphère privée de l'individu des immixtions de la puissance publique. Pourtant, depuis une décennie, la demande de sécurité dans la société a relevé le seuil de tolérance vis-à-vis des systèmes de surveillance et de contrôle, ce qui s'est traduit par des **arbitrages en défaveur du droit à la vie privée**. Les nouvelles technologies sont perçues comme de **nouvelles possibilités de lutte contre l'insécurité** et de nombreuses personnes ne voient plus d'inconvénient majeur à être « tracées » ou surveillées dès lors que, disent-elles, « *elles n'ont rien à se reprocher, ni à cacher* ».

Cette tendance à l'acceptation d'une « **surveillance institutionnelle** » est complétée par deux évolutions nouvelles qui ont en commun d'exposer la vie privée à une nouvelle menace : **la surveillance par les acteurs privés**. Ces tendances sont l'accélération des progrès technologiques et l'exposition de soi et d'autrui sur Internet.

- l'accélération des progrès technologiques ;

On assiste depuis quelques années à des développements technologiques tels que la géolocalisation, la technologie « bluetooth », les puces RFID[2], les nanotechnologies, etc., qui donnent naissance à des **usages**

---

[1] *Rapport d'information n° 441 (2008-2009) du 27 mai 2009 de M. Yves Détraigne et Mme Anne-Marie Escoffier, fait au nom de la commission des lois.*

[2] *RFID (Radio Frequency Identification) désigne une technologie qui permet d'identifier et de localiser sans contact des objets ou des personnes grâce à une micropuce (également dénommée étiquette ou tag) qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à une dizaine de mètres.*

toujours plus nombreux et dans **des domaines les plus variés** : transports, ergonomie, publicité, etc. Si tous visent à apporter de nouvelles facilités aux utilisateurs, ils sont également **porteurs de risques nouveaux au regard du droit à la vie privée**. A titre d'exemple, si chacun comprend l'intérêt du GPS pour trouver plus facilement son chemin, ce système permet aussi de suivre les déplacements des individus et doit de ce fait être encadré pour éviter toute dérive.

De même, si la technologie RFID peut apporter certains progrès en permettant, par exemple, d'améliorer la ponctualité des vols dans l'hypothèse où les cartes d'embarquement, dotés de cette technologie, permettent de localiser rapidement les passagers en retard, elles constituent un **défi nouveau au regard du droit à la vie privée et de la liberté d'aller et venir.**

Enfin, si les puces RFID offrent des fonctionnalités nouvelles et intéressantes pour les utilisateurs (badge d'accès à une voiture, un parking, étiquettes sur un produit alimentaire qui permettront bientôt à un réfrigérateur de lire les dates de péremption…), il convient d'interdire à des tiers non autorisés l'accès à ces informations qui, dans certains cas, « racontent une portion de vie d'un individu ».

Le danger est d'autant plus grand à l'heure des nanotechnologies, qui permettent de fabriquer des puces à l'échelle du nanomètre, c'est-à-dire du millionième de mètre, ce qui les rend invisibles.

- la tendance à l'exposition de soi et d'autrui ;

L'apparition de nouvelles formes de sociabilité sur Internet s'exprimant par le biais de *blogs* ou de réseaux sociaux (tels que Facebook, MySpace, Twitter…) a fait naitre une nouvelle tendance sociologique forte : **l'exposition volontaire de soi et d'autrui**. Or, cette tendance, mue par certains facteurs tels que le mimétisme social, mais aussi l'adhésion aux nouvelles valeurs d'échange et de partage, sur un mode largement informel et décontracté, n'est pas sans risques au regard du droit à la vie privée.

Certes, d'aucuns pourraient penser que les données sont paradoxalement protégées par leur profusion et leur éparpillement ; toutefois, la **capacité agrégative des moteurs de recherche** sur Internet est telle qu'il est désormais possible, en quelques clics, d'établir des **profils détaillés** sur la plupart d'entre nous.

B. … AUXQUELLES LE DROIT EN VIGUEUR APPORTE DES RÉPONSES LARGEMENT ADAPTÉES ET PÉRENNES

Si ces trois nouvelles tendances constituent de **nouveaux défis** au regard du droit à la vie privée, il n'en demeure pas moins que notre cadre juridique sur la protection des données personnelles y apporte, dans une très large mesure, des **réponses adaptées et pérennes**, peut-être, paradoxalement, parce qu'il les a **précédées**.

La France a été ainsi l'un des premiers pays au monde à se doter d'une loi de protection des données personnelles, au travers de la loi n° 78-17 du 6 janvier 1978 dite loi « informatique et libertés ».

Par ailleurs, l'Union européenne s'est dotée, dès 1995, d'une directive sur la protection des données personnelles[1]. Le choix a alors été fait de ne pas adopter de dispositions spécifiques à certaines technologies ou applications et de fixer des **principes intemporels** (« neutralité technologique ») dont la souplesse apparaît comme un **gage de protection**.

Ces principes, inspirés des dispositions de la loi « informatique et libertés » de janvier 1978 et renforcés à l'occasion de la transposition de la directive par la loi n° 2004-801 du 6 août 2004, sont les suivants : finalité, proportionnalité, sécurité des données, droit à l'information, droits d'accès, de rectification et d'opposition et droit au consentement préalable. Si le choix avait été fait de s'engager sur la voie de législations spécifiques pour certaines technologies ou applications, il aurait nécessairement conduit à des vides juridiques, le temps technologique étant plus rapide que le temps démocratique d'élaboration des normes.

En outre, l'Union européenne a opportunément décidé de **renforcer les pouvoirs des autorités nationales de protection des données**, notamment en les dotant d'un pouvoir de sanction.

II. LA PROPOSITION DE LOI : DES ADAPTATIONS NÉCESSAIRES AU DROIT ACTUEL

La proposition de loi vise à adapter le cadre juridique ainsi décrit, d'une part, à l'évolution des **pratiques**, en particulier l'utilisation croissante d'Internet et la multiplication des traitements informatiques, et, d'autre part, aux nouvelles **attentes** de notre société en matière de respect de la vie privée.

Le texte entend également tirer les conséquences, sur deux points importants, de **l'évolution du droit communautaire**.

A. FAIRE DU CITOYEN UN « HOMO NUMERICUS » RESPONSABLE, PROTECTEUR DE SES PROPRES DONNÉES

1. Confier à l'Education nationale une mission d'information sur la protection des données personnelles

Face à la triple évolution décrite plus haut, la proposition de loi considère que la première réponse réside dans **l'implication pleine et entière des individus dans leur propre protection**. Elle reprend en cela la première recommandation du rapport d'information sur *« la vie privée à l'heure des*

[1] *Directive 95/46/CE du 24 octobre 1995*

mémoires numériques », relative au *« renforcement de la place accordée à la sensibilisation aux questions de protection de la vie privée et des données personnelles dans les programmes scolaires ».*

A cette fin, l'article premier du texte complète l'article L. 312-9 du code de l'éducation afin que l'initiation des élèves à l'usage d'Internet intègre autant les questions liées au téléchargement illégal que celles, tout aussi essentielles, de la **protection des données personnelles** et, plus généralement, de la vie privée. Le rapport d'information précité souligne en effet que, s'il incombe aux parents de transmettre à leurs enfants les valeurs de tolérance et de respect ainsi que les notions de pudeur, d'intimité et de droit à l'image, principes qui s'appliquent autant à la « vie réelle » qu'à la vie numérique, il n'en demeure pas moins qu'ils sont souvent **dépassés et démunis** face aux nouvelles technologies et aux nouveaux usages qui en résultent.

La pratique des « **sextos** » en est une dramatique illustration : elle consiste en la transmission de photos dénudées entre mineurs par messageries instantanées ou par téléphones portables, souvent sans le consentement des personnes, afin de leur nuire ou d'accomplir une vengeance. On notera, à cet égard, qu'interrogée récemment par notre collègue Anne-Marie Escoffier sur cette pratique inquiétante, Mme Michèle Alliot-Marie, ministre d'Etat, garde des sceaux, ministre de la justice et des libertés, a répondu que l'arsenal juridique était aujourd'hui satisfaisant mais a reconnu que **l'éducation des jeunes était un enjeu essentiel**[1].

La proposition de loi considère qu'il appartient donc à l'Education nationale d'informer les élèves sur les risques liés aux usages d'Internet au regard du droit à la vie privée, le brevet « informatique et Internet » semblant, aujourd'hui, insuffisant pour répondre à ce défi majeur.

2. Adapter le régime juridique des « cookies »

L'article 6 de la proposition de loi comporte **deux modifications importantes du régime juridique des « cookies »**, petits fichiers qui constituent des « mouchards » électroniques introduits sur le disque dur de l'internaute à des fins techniques ou publicitaires.

D'une part, il renforce l'obligation d'information incombant au responsable du traitement : l'utilisateur devra donc recevoir une information **spécifique, claire, accessible et permanente** sur les **finalités des cookies comportementaux,** c'est-à-dire ceux qui visent à délivrer une **publicité ciblée.**

---

[1] *Question orale sans débat n° 0745S de Mme Anne-Marie Escoffier publiée dans le JO Sénat du 17/12/2009 - page 2909 ; réponse de la garde des sceaux publiée dans le JO Sénat du 03/02/2010 - page 756 ; la question et la réponse sont disponibles sur Internet : http://www.senat.fr/questions/base/2009/qSEQ09120745S.html*

D'autre part, il impose le **consentement** de l'utilisateur avant tout stockage de cookies sur son ordinateur : la proposition de loi entend ainsi se conformer au nouvel article 5-3 de la directive 2002/58/CE « Vie privée et Communications Electroniques » du 12 juillet 2002, tel que modifié récemment par la directive 2009/136/CE du 18 décembre 2009 adoptée dans le cadre du « Paquet Télécom »[1].

3. Garantir une meilleure traçabilité des transferts de données

Deux mesures de la proposition de loi garantissent une meilleure **traçabilité des transferts de données** et permettent de mieux lutter contre **leur dissémination** :

- l'information spécifique, claire et accessible donnée aux personnes, avant tout traitement mais également de manière permanente, sur le site Internet du responsable du traitement, des *« destinataires ou catégories de destinataires des données »* (article 6) ;

- la possibilité de connaître, au titre du droit d'accès, l'origine de la donnée personnelle, alors que n'est actuellement prévue que la communication des informations **disponibles** quant à cette origine (article 9).

B. DONNER UNE PLUS GRANDE EFFECTIVITÉ AU DROIT À L'OUBLI NUMÉRIQUE

La proposition de loi propose également de donner une plus grande effectivité au **droit à l'oubli numérique,** à travers plusieurs mesures :

- l'obligation pour la CNIL de préciser, pour chacun des traitements qu'elle met à la disposition du public, la **durée de conservation des données** (article 5) ;

- l'obligation de fournir aux internautes une information **claire, accessible et spécifique** sur la durée de conservation de leurs données personnelles (article 6) ;

- l'exercice **plus facile du droit à la suppression des données** dans la mesure où la proposition de loi permet d'exercer ce droit non seulement gratuitement mais également, après identification, par **voie électronique**, alors que les responsables de traitement prévoient aujourd'hui généralement la seule

---

[1] *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.*

transmission par courrier postal, qui paraît de nature à décourager les personnes concernées (articles 6 et 8) ;

- la possibilité de **saisir plus facilement et plus efficacement qu'aujourd'hui les juridictions civiles,** notamment en cas d'impossibilité pour les personnes d'exercer leur droit à la suppression des données. Elles pourraient désormais saisir la juridiction la plus proche de leur domicile et même appuyer leur requête d'une observation écrite de la CNIL, qui ne serait pas tenue d'envoyer un de ses représentants à l'audience pour développer son point de vue (article 13).

C. PROMOUVOIR LA DIFFUSION D'UNE CULTURE « INFORMATIQUE ET LIBERTÉS »

1. Diffuser une culture « informatique et libertés » dans les entreprises et les administrations

L'article 3 de la proposition de loi rend **obligatoires les correspondants « informatique et libertés »** lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre. Le bilan de l'action de ces correspondants, qui ont vu le jour en 2005-2006, apparaît en effet pleinement satisfaisant tant ils ont permis la diffusion de la culture « informatique et libertés » dans les structures dans lesquelles ils ont été désignés.

2. Conforter le statut et les pouvoirs de la CNIL

Quatre articles de la proposition de loi visent à conforter le **statut et les pouvoirs de la CNIL.**

L'article 10 rend publiques les audiences de la formation restreinte de la CNIL afin de tirer les conséquences d'une ordonnance du Conseil d'État du 19 février 2008 qui reconnaît le caractère juridictionnel de cette formation.

L'article 11 rend plus aisée la publicité des sanctions les plus graves prononcées par la CNIL, publicité aujourd'hui conditionnée à la « *mauvaise foi du responsable du traitement* ». L'article supprime cette condition.

L'article 12 renforce les pouvoirs de sanction de la CNIL en lui permettant de prononcer des sanctions financières d'un montant plus important. Les auteurs de la proposition de loi estiment que ce relèvement du plafond légal incitera la CNIL à faire preuve d'une plus grande **fermeté**, à l'image de l'agence espagnole qui, sur la seule année 2008, a infligé des sanctions d'un montant total de 22,6 millions d'euros alors que la formation restreinte de la CNIL, depuis sa création en 2005, a, pour sa part, prononcé des sanctions dont le montant cumulé ne s'élève qu'à 520 400 euros.

L'article 13 renforce les possibilités d'actions juridictionnelles de la CNIL en cas de méconnaissance, par un responsable du traitement, des dispositions de la loi « informatique et libertés » : la CNIL pourrait présenter des observations devant les juridictions, d'office ou à la demande des parties. En outre, sur le modèle de ce qui existe désormais en droit de la consommation, toute personne s'estimant lésée par la non-application de la loi « informatique et libertés » pourrait faire valoir ses droits devant la juridiction civile du lieu où elle demeure.

3. Rendre obligatoires les notifications des failles de sécurité

L'article 7 de la proposition de loi tend à rendre obligatoire, pour les responsables de traitements de données à caractère personnel, l'information de la CNIL en cas de violation de l'intégrité ou de la confidentialité de ces traitements, afin de les inciter à mettre en œuvre les **mesures de protection adéquates**. La CNIL pourra ensuite, en cas d'atteinte portée aux données d'une ou plusieurs personnes physiques, exiger des responsables de traitement qu'ils avertissent ces personnes. Cet article transpose ainsi une disposition de la directive « Vie privée et Communications Électroniques » du 25 novembre 2009 précitée.

D. DES CLARIFICATIONS JURIDIQUES SOUHAITABLES

1. Clarifier le statut de l'adresse IP

L'article 2 de la proposition de loi vise à **clarifier le statut de l'adresse IP**. En effet, alors que cette adresse constitue, pour le rapport d'information précité, un moyen indiscutable d'identification, fût-elle indirecte, d'un internaute, au même titre qu'une adresse postale ou un numéro de téléphone, certaines juridictions ont récemment contesté le caractère de donnée personnelle de l'adresse IP. La clarification opérée par l'article 2 permet ainsi d'apporter aux données de connexion des internautes la protection de la loi « informatique et libertés ».

2. Réserver au législateur la compétence exclusive pour créer les catégories de fichiers nationaux de police

L'article 4 de la proposition de loi réserve au législateur la compétence exclusive pour autoriser les **catégories de fichiers nationaux de police (également appelés « fichiers de souveraineté »)** et pour définir les principales caractéristiques de ces catégories (services responsables, finalités et durée de conservation des informations traitées), alors que les fichiers de police peuvent actuellement, en vertu de l'article 26 de la loi « Informatique et libertés », être autorisés par arrêté ou, s'ils comportent des données sensibles, par décret en Conseil d'Etat. Les auteurs de la proposition de loi estiment en

effet que l'encadrement des fichiers de police relève de l'article 34 de la Constitution qui prévoit notamment que *« la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ».*

III. LA POSITION DE VOTRE COMMISSION

Outre 2 amendements rédactionnels ou de coordination, votre commission a adopté 25 amendements, 21 de votre rapporteur, un de Mme Morin-Desailly, rapporteur pour avis de la commission de la culture, un de M. Alex Türk, un de M. Charles Gautier et un du Gouvernement.

A. CONCILIER DE MANIÈRE ÉQUILIBRÉE LES DIFFÉRENTS INTÉRÊTS EN PRÉSENCE

1. Faciliter la mise en œuvre des traitements soumis à déclaration préalable

Consciente que la proposition de loi crée des **obligations nouvelles** pour les responsables de traitement, votre commission a cherché également, à l'initiative de votre rapporteur, à **simplifier** certaines démarches qu'ils accomplissent. Elle a ainsi adopté un article 2 *ter* afin de faciliter la mise en œuvre des traitements soumis à simple déclaration préalable auprès de la CNIL. En effet, dans sa rédaction actuelle, l'article 23 de la loi « informatique et libertés » subordonne la mise en œuvre de tels traitements à la transmission par la CNIL d'un récépissé.

Or, ce récépissé **retarde inutilement** la mise en œuvre du traitement.

En conséquence, l'amendement prévoit que *« le demandeur peut mettre en œuvre le traitement dès réception de la preuve de l'accomplissement de la formalité préalable ».* A titre d'exemple, cette preuve peut prendre la forme d'un accusé de réception postal si la déclaration a été adressée à la CNIL par lettre recommandée.

2. Conforter le statut et les missions du Correspondant « informatique et libertés »

Votre commission a adopté **un amendement** de son rapporteur à l'**article 3** de la proposition de loi afin de conforter le statut et les missions du Correspondant « informatique et libertés » (CIL).

Cet amendement :

- étend les hypothèses dans lesquelles le CIL est rendu obligatoire ; la commission a maintenu le critère retenu par la proposition de loi mais en a ajouté un second, alternatif : le CIL serait obligatoire non seulement dans les conditions prévues par la proposition de loi mais également lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel qui relève du **régime d'autorisation** en application des articles 25, 26 ou 27 de la loi « informatique et libertés ». Ce régime concerne les traitements sensibles qui ne peuvent être autorisés que par la CNIL (article 25) ou le Gouvernement (articles 26 et 27) après avis motivé et publié de la CNIL ;

- clarifie et étend les possibilités de désigner un seul et même CIL pour plusieurs structures (principe de « mutualisation ») ;

- renforce les missions du CIL ;

- rétablit le texte actuel de la loi « informatique et libertés » en matière de d'avis de la CNIL en cas de démission d'office du correspondant. Si la proposition de loi fait le choix d'un avis conforme, l'amendement préfère le terme actuel de consultation, qui implique un avis simple ;

- resserre les liens entre la CNIL et les CIL.

Par ailleurs, votre commission a adopté **un amendement** de votre rapporteur à l'**article 7** de la proposition de loi afin de **donner un rôle spécifique au CIL dans la gestion des failles de sécurité**. Votre commission a ainsi souhaité que le responsable d'un traitement affecté par une telle faille de sécurité ait l'obligation d'en informer le CIL, qui devra à son tour informer la CNIL. Le CIL pourra ainsi s'assurer que le responsable de traitement prend les mesures nécessaires pour rétablir la sécurité des données. Il aura également la charge de tenir un inventaire des atteintes aux traitements de données personnelles.

Votre commission a adopté **deux amendements** de votre rapporteur au même article pour préciser, d'une part qu'**en cas de « violation »** du traitement de données et non de simple « atteinte », l'information sur la faille de sécurité devrait être diffusée, d'autre part que l'obligation d'information ne s'appliquerait pas, pour des raisons évidentes, aux fichiers de police.

3. Renforcer l'efficacité et la légitimité de la CNIL

Votre commission a adopté trois amendements tendant à **renforcer l'efficacité et la légitimité de la CNIL**.

En premier lieu, elle a adopté, à l'initiative de votre rapporteur ainsi que de notre collègue M. Charles Gautier, un article 2 *bis* prévoyant que les deux députés et les deux sénateurs membres de la CNIL sont désignés *« de manière à assurer une représentation pluraliste ».* Au regard de l'importance

que revêt l'action de la CNIL dans le domaine de la protection des données à caractère personnel, il semble nécessaire que **l'opposition y soit représentée**. L'exigence de pluralisme s'appréciera au vu de l'ensemble des membres désignés au sein de la CNIL par les deux assemblées.

En second lieu, votre commission a adopté, à l'initiative de notre collègue M. Alex Türk, un article 5 *bis* afin d'apporter une précision importante en matière de **publicité des avis de la CNIL**. Elle a prévu que chaque fois qu'une loi renvoie à des textes règlementaires d'application pris « *après avis de la CNIL* », sans autre forme de précision, les avis de la CNIL sont par principe publics.

La question se pose surtout en matière de **fichiers de police** : en effet, en vertu de l'article 26 de la loi « informatique et libertés », ces fichiers font l'objet d'un avis public de la CNIL, mais sont souvent créés sans faire référence à cet article.

L'amendement, de portée générale, apporte donc une **opportune clarification**. Ainsi ne pourra-t-on plus interpréter le silence de la loi en matière d'application de l'article 26 précité comme remettant en cause la publicité de l'avis de cette Commission.

Enfin, votre commission a adopté, à l'initiative du Gouvernement, un article 9 *bis* afin de donner à la CNIL la possibilité de demander au juge des libertés et de la détention l'autorisation préalable d'effectuer une **visite inopinée** *« lorsque l'urgence, la gravité des faits justifiant le contrôle ou le risque de destruction ou de dissimulation de documents l'exigent ».*

En effet, tel qu'il est actuellement rédigé, l'article 44 de la loi « informatique et libertés » dispose que le responsable des lieux **peut s'opposer à une visite de la Commission.** Dans ce cas, la visite ne peut se dérouler qu'avec l'autorisation d'un juge, saisi à la requête du Président de la Commission.

Or, ce droit d'opposition est de nature à **restreindre considérablement la portée et l'efficacité des contrôles de la CNIL** puisque l'organisme contrôlé pourra bénéficier du temps nécessaire à l'obtention d'une ordonnance judiciaire pour effacer - ou dissimuler - des données informatiques qui seraient contraires à la loi.

En permettant au juge des libertés et de la détention, gardien des libertés individuelles, d'autoriser la CNIL à effectuer un contrôle inopiné, l'amendement renforce **l'efficacité de la CNIL dans sa mission de contrôle sans porter atteinte aux droits du responsable des lieux visités**. En effet, conformément à l'article 44 précité, la visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée et celui-ci peut décider l'arrêt ou la suspension de la visite à tout moment.

4. Mieux encadrer la création des fichiers de police

A l'initiative de votre rapporteur, votre commission, ayant constaté que la rédaction de l'article 4 risquait d'être considérée comme dépourvue de portée normative tout en prétendant lier le législateur, **a réécrit cet article afin d'encadrer directement les finalités auxquelles peuvent répondre les fichiers de police**. Dès lors, elle a choisi de reprendre, avec quelques modifications, l'ensemble des dispositions concernant les fichiers de police de la proposition de loi de simplification et d'amélioration de la qualité du droit, adoptée en 1ère lecture par l'Assemblée nationale le 2 décembre 2009.

Elle a ainsi d'abord adopté un amendement inscrivant une liste de 13 points énumérant les finalités possibles des fichiers de police, toute autre finalité que le gouvernement souhaiterait introduire impliquant dès lors le dépôt d'un projet de loi. Votre commission a également repris par cet amendement le principe d'une **procédure d'expérimentation** permettant à la CNIL et aux services de l'Etat de dialoguer en amont de la mise en production d'un fichier de police.

En outre, votre commission a adopté une série de six amendements afin de **renforcer l'encadrement** des procédures de création des fichiers de police et les **garanties** apportées aux libertés individuelles. Ces amendements permettent de :

-créer une formation spécialisée au sein de la CNIL, consacrée exclusivement aux fichiers de police (article 4 ter) ;

-confier au bureau de la CNIL la possibilité d'émettre des avis au nom de celle-ci dans le cadre de la démarche d'expérimentation précitée (article 4 quater) ;

-rendre obligatoire l'inscription des durées maximales de conservation des données dans l'acte réglementaire de création d'un fichier de police, ainsi que des modalités de traçabilité des consultations du fichier (article 4 quinquies) ;

-rendre obligatoire la transmission à la délégation parlementaire au renseignement de tout décret en Conseil d'État créant un traitement dont il a été prévu une dispense de publication (fichiers intéressant la sûreté nationale ou la défense) (article 4 sexies) ;

-renforcer l'efficacité du contrôle des fichiers d'antécédents judiciaires par le procureur de la République, notamment en fixant un délai maximal d'un mois pour le traitement des demandes de mise à jour de ces fichiers (article 4 septies) ;

-préciser les conditions d'utilisation des données figurant dans des fichiers d'antécédents judiciaires lors des procédures de comparution immédiate (article 4 octies).

Enfin, votre commission a adopté un amendement rédactionnel afin de tenir compte de la réécriture de l'article 26 de la loi « Informatique et libertés ».

5. Assouplir le principe de consentement préalable ou « Opt-in » en matière de cookies

Par un amendement de votre rapporteur, votre commission a cherché à **assouplir le principe de consentement préalable** ou « Opt-in » en matière de « cookies », principe inscrit à l'article 6 de la proposition de loi (alinéas 15 à 22).

Appliqué de manière trop rigide, ce principe obligerait en effet les internautes à réitérer continuellement leur souhait d'accepter ou de refuser les cookies pour chaque site consulté, voire chaque page web. Ils se verraient ainsi contraints en pratique d'interrompre leur navigation pour cliquer sur des fenêtres ou « pop-up » sur leur écran, ce qui, d'une part, constituerait une entrave à la navigation fluide et rapide des internautes, d'autre part, mettrait en grandes difficultés les professionnels du commerce en ligne.

Soucieuse de ne pas contrarier de manière excessive le développement du commerce en ligne ni la navigation sur Internet, votre commission a souhaité, d'une part, prévoir une information globale, et non au cas par cas, en matière de « cookies », d'autre part, que cette information renvoie l'utilisateur aux possibilités de paramétrage du navigateur Internet afin qu'il puisse **exprimer un choix préalable, quel qu'il soit,** en matière de « cookies », ce qui semble conforme aux choix récents du législateur communautaire.

6. Clarifier l'exercice du « droit à l'oubli »

A l'initiative de votre rapporteur, votre commission a adopté un amendement tendant à **clarifier l'exercice du « droit à l'oubli »,** c'est-à-dire du droit à la suppression des données (article 8).

Actuellement, ce droit est conditionné à des « motifs légitimes » et ne peut pas, en tout état de cause, être exercé dans deux hypothèses : lorsque le traitement répond à une obligation légale ou lorsque que l'exercice de ce droit a été écarté par une disposition expresse de l'acte autorisant le traitement.

L'amendement ne revient pas sur la notion actuelle de « motifs légitimes » mais cherche à mieux encadrer son expression. Votre commission a ainsi précisé que le droit à la suppression des données ne pourrait être exercé dans quatre **nouveaux cas de figure :**

- lorsque les données sont nécessaires à la finalité du traitement : il s'agit d'éviter que les données soient effacées dans le cas, par exemple, où un bien est toujours sous garantie ou n'a pas été entièrement réglé par le consommateur ;

- lorsque le traitement est nécessaire pour la sauvegarde, la constatation, l'exercice ou la défense d'un droit ;

- lorsque le droit de suppression porte atteinte à une liberté publique garantie par la loi : il s'agit essentiellement de protéger la liberté de la presse ;

- lorsque les données constituent un fait historique : le droit de suppression ne peut avoir pour objet ou pour effet de réécrire ou de falsifier l'histoire.

7. Clarifier ponctuellement le dispositif de la proposition de loi

A l'article 1er, votre commission des lois a adopté un amendement de la commission de la culture, tendant à insérer les dispositions relatives à l'information dispensée aux élèves par l'Education nationale sur la protection des données personnelles et le respect de la vie privée au sein de la partie du code de l'éducation consacrée à **l'éducation civique**.

A l'article 2, qui tend à qualifier expressément l'adresse IP de donnée à caractère personnel, votre commission, sur proposition de son rapporteur, a modifié la rédaction retenue afin de viser, non l'adresse MAC, mais l'adresse identifiant le **titulaire d'un accès à des services de communication au public en ligne.**

Enfin, à l'article 13, votre commission a supprimé les dispositions prévoyant la recevabilité des observations écrites de la CNIL quelle que soit la procédure applicable, craignant que de telles dispositions ne puissent être considérées comme contraires aux exigences du procès équitable.

B. EXERCER UNE INFLUENCE SUR LA FORMATION DES NORMES INTERNATIONALES

1. À court terme, au niveau communautaire : vers une révision de la directive de 1995 ?

Votre commission est consciente que la proposition de loi ne constitue qu'une **réponse française** à **un phénomène mondial**.

En particulier, elle regrette que la directive du 24 octobre 1995 ait, en son article 4, écarté son applicabilité aux traitements dont les responsables sont situés **en dehors de l'Union européenne**, même si lesdits traitements visent un **public français**. Autrement dit, les grands acteurs américains de l'Internet, tels que Google, Facebook…, sont soumis aux lois américaines de protection des données et aux juridictions des Etats fédérés, et non à la loi « informatique et libertés » : **les avancées contenues dans la présente proposition de loi ne leur seront donc pas opposables.**

Cette règle est **strictement appliquée** par les tribunaux : ainsi, en 2008, le tribunal de grande instance de Paris s'est prononcé sur une demande

en référé d'une personne qui demandait qu'il soit fait obligation à Google de supprimer de ses archives accessibles en ligne des messages postés par elle sur des forums de discussion, pour certains depuis 1998, et qui portaient sur sa vie privée.

La demanderesse s'appuyait sur les articles 6, 7 et 38 de la loi « informatique et libertés » (limitation de la durée de conservation des données, nécessité du consentement de la personne concernée, droit d'opposition). Dans son ordonnance, le tribunal a estimé que la loi informatique et libertés n'était pas applicable, en se fondant sur l'article 4 précité de la directive. Les serveurs de Google étant établis en Californie, il a considéré que le droit californien devait s'appliquer[1].

En conséquence, votre rapporteur partage la position des auteurs de la proposition de loi, exprimée lors de leur audition, tendant à faire évoluer la directive du 24 octobre 1995, sans remettre en cause le haut niveau de protection qu'elle accorde, afin de soumettre tous les responsables de traitement, **où qu'ils se trouvent**, aux juridictions et au droit français dès lors qu'ils visent bien un public français.

Cette évolution de la directive serait doublement cohérente :

- d'une part, elle serait conforme à la **solution en vigueur dans d'autres branches du droit** telles que le droit de la consommation, le droit de la presse, le droit de la propriété intellectuelle, et même le droit à la vie privée pourtant proche…

Une illustration en est donnée par une autre ordonnance de référé du tribunal de grande instance de Paris, portant sur des faits semblables à ceux décrits ci-dessus, mais basée sur d'autres textes. En 2006, cette juridiction avait été saisie par une personne demandant la suspension d'une page d'un blog hébergé par Google et contenant des éléments portant atteinte à sa vie privée. Cette demande était basée, non pas sur la loi informatique et libertés, mais sur l'article 9 du code civil consacrant le droit à la vie privée. Le tribunal avait constaté le manquement aux dispositions de cet article et ordonné à Google de retirer les éléments en cause[2].

Il est pour le moins curieux que, pour des atteintes commises en France, les acteurs non-communautaires de l'Internet soient régis par le droit français dans le domaine du droit à la vie privée et par leur droit national en matière de protection des données ;

---

[1] Tribunal de grande instance de Paris Ordonnance de référé 14 avril 2008 - Bénédicte S / Google Inc., Google France.

[2] TGI Paris, ordonnance de référé du 19 oct. 2006.

- d'autre part, l'évolution de la directive serait également conforme au **principe de réciprocité**. En effet, lorsqu'un site Internet, implanté en Europe, porte atteinte à la protection de données de résidents américains, par exemple, sur le fondement de la loi de protection des mineurs votée en 1998 (« Children's Online Privacy Protection Act »), les juridictions américaines se déclarent compétentes et appliquent leur droit national.

Pour ces deux raisons, la modification de l'article 4 de la directive apparaît **pleinement justifiée**.

Lors de leur audition, les auteurs de la proposition de loi ont indiqué à votre rapporteur avoir transmis ce point de vue, soutenu par la CNIL, à Mme Viviane Redding, nouveau commissaire en charge de la protection des données.

Rappelons que son prédécesseur, M. Jacques Barrot, avait ouvert une large consultation sur l'opportunité de faire évoluer la directive de 1995, consultation qui a pris fin le 31 décembre 2009.

Le 1er février 2010, Mme Viviane Reding a fait part de son intention de réviser, dans les mois prochains, la directive, considérant que *« le monde a changé depuis 1995 (...). L'Union européenne devra fournir un instrument juridique solide pour répondre aux défis posés par le rapide développement des nouvelles technologies et de l'évolution des menaces à la sécurité ».*

Mme Viviane Redding a notamment mis en avant la nécessité de protéger les données personnelles *« indépendamment du lieu où se trouve le responsable du traitement »,* ce qui semble clairement **aller dans le sens voulu par les auteurs de la proposition de loi.**

2. A long terme au niveau mondial : vers une convention sous l'égide de l'ONU ?

Parallèlement au processus de révision de la directive de 1995, qui pourrait être engagé à court terme, votre commission appelle de ses vœux la signature, à terme, d'un **traité international** dans le domaine de la protection des données.

Elle espère que la présente proposition de loi sera perçue comme un **signal fort** de la France pour aller dans ce sens, d'autant que notre pays s'est distingué en 1978 par sa loi visionnaire, qui a largement inspiré de nombreuses législations dans le monde.

On peut d'ores et déjà se réjouir que près de 80 autorités de protection des données aient adopté, le 5 novembre 2009, des **standards internationaux sur la protection des données personnelles et de la vie privée**, dans le cadre de la Conférence mondiale des Commissaires à la protection des données qui s'est tenue à Madrid.

Il s'agit d'un premier pas historique car cette Conférence mondiale est parvenue à élaborer un **corpus de règles communes** adaptées aux dernières évolutions technologiques : les grands principes de protection des données, les droits dont bénéficient les individus, les obligations incombant aux responsables de traitement, les procédures internes à mettre en place au sein des entreprises et administrations à l'échelle mondiale, etc.

La prochaine étape, éminemment délicate, consiste désormais à mettre en place, à terme, un **instrument juridique international ayant force juridique contraignante.**

Deux facteurs invitent à l'optimisme :

- d'une part, les Etats-Unis sont souvent présentés comme des adversaires d'une telle convention internationale, alors qu'en réalité la protection des données personnelles aux Etats-Unis est plus forte qu'on ne croit. Comme l'expliquent les auteurs de la proposition de loi dans leur rapport d'information précité, si les Etats-Unis protègent moins les bases de données privées qu'en Europe, en dehors de quelques lois sectorielles, il n'en est pas de même des données gérées par les pouvoirs publics.

A titre d'exemple, toutes les administrations fédérales **comprennent obligatoirement un « Chief Privacy Officer »,** comparable à un correspondant informatique et libertés mais aux pouvoirs plus étendus. De même, 45 Etats américains sur 50 disposent déjà d'une législation contraignante dans le domaine de la notification des failles de sécurité alors que, comme indiqué précédemment, l'Europe vient à peine de prévoir une telle obligation de notification ;

- d'autre part, on peut constater une **prise de conscience mondiale des internautes** dans le domaine de la protection des données, comme l'a clairement illustré la « cyber-révolte » des utilisateurs de Facebook lorsque le réseau social a annoncé, en février 2009, sa décision de modifier ses conditions générales d'utilisation afin de se **rendre propriétaire à vie des données** : pour le réseau, il s'agissait d'éviter que les informations qui figurent sur le profil de l'utilisateur ne disparaissent le jour où ce dernier se « désinscrit ».

Toutefois, cette démarche a été perçue comme une atteinte délibérée à la vie privée et de nombreux groupes de discussion se sont, en quelques heures, constituées sur Internet si bien que M. Mark Zuckerberg, le président et fondateur de Facebook, s'est vu obligé de **renoncer** à sa décision.

Votre commission des lois a adopté la proposition de loi **ainsi rédigée**.

EXAMEN DES ARTICLES

TITRE PREMIER
DISPOSITIONS PORTANT MODIFICATION DU CODE DE L'ÉDUCATION

Article premier
(art. L. 312-9 du code de l'éducation)
Sensibilisation des jeunes aux enjeux de la protection de la vie privée sur Internet

Cet article tend à confier à l'Education nationale une mission de sensibilisation aux enjeux de la protection de la vie privée sur Internet.

La question de la **sensibilisation des citoyens**, et notamment des plus jeunes d'entre eux, à l'usage des nouvelles technologies a constitué un des axes essentiels du rapport de nos collègues Anne-Marie Escoffier et Yves Détraigne. Ces derniers ont notamment souligné qu'une telle sensibilisation, en permettant à l'ensemble de nos concitoyens de se saisir pleinement des enjeux relatifs à la vie privée à l'heure du numérique, constituait un préalable indispensable à la protection des données personnelles.

Depuis 1985, la loi dispose qu'une initiation à la technologie et à l'usage de l'informatique doit être dispensée à tous les élèves et tous les étudiants[1].

Ces dispositions, ultérieurement insérées dans la partie législative du code de l'éducation, ont été complétées à l'initiative de la commission des affaires culturelles du Sénat à l'occasion de l'examen de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet[2]. Désormais, l'article L. 312-9 du code de l'éducation dispose que, « *notamment à l'occasion de la préparation du brevet informatique et internet des collégiens,* [les élèves et les étudiants] *reçoivent de la part d'enseignants préalablement sensibilisés sur le sujet une information sur les risques liés aux usages des services de communication au public en ligne, sur les dangers du téléchargement et de la mise à disposition illicites d'œuvres ou d'objets*

---

[1] *Loi n°85-1371 du 23 décembre 1985 de programme sur l'enseignement technologique et professionnel.*

[2] *Voir le rapport n° 53 (2008-2009) de notre collègue Michel Thiollière, fait au nom de la commission des affaires culturelles, déposé le 22 octobre 2008.*

protégés par un droit d'auteur ou un droit voisin pour la création artistique, ainsi que sur les sanctions encourues en cas de délit de contrefaçon. Cette information porte également sur l'existence d'une offre légale d'œuvres ou d'objets protégés par un droit d'auteur ou un droit voisin sur les services de communication au public en ligne ».

L'article 1er de la proposition de loi tend à compléter et renforcer ces dispositions en prévoyant :

- d'une part, que les élèves et les étudiants doivent recevoir une information sur les risques liés aux usages d'Internet au regard de la protection des données personnelles, et, plus généralement, du droit à la vie privée. Cette information mettrait l'accent sur les dangers de l'exposition de soi et d'autrui et porterait sur les droits d'opposition commerciale, de suppression, d'accès et de rectification ainsi que sur les missions de la CNIL ;

- d'autre part, que cette information doit être dispensée par des enseignants « *préalablement formés sur le sujet* ».

Votre commission souscrit pleinement aux objectifs poursuivis par le présent article. Elle rappelle que, dans leur rapport d'information précité, nos collègues Anne-Marie Escoffier et Yves Détraigne ont constaté qu'en dépit de la généralisation à l'ensemble de l'enseignement scolaire du brevet informatique et Internet (B2I) créé en 2001, la place accordée à la sensibilisation aux questions de protection de la vie privée et des données personnelles dans les programmes scolaires était encore **insuffisante**. Les dispositions prévues à l'article 1er de la proposition de loi permettront de donner une impulsion nouvelle en faveur d'une meilleure prise en compte de ces enjeux.

Votre rapporteur avait néanmoins estimé qu'il était nécessaire d'aménager la rédaction de l'article 1er :

- tout d'abord, il lui était paru souhaitable de mettre en évidence l'importance, pour notre société, de la notion de vie privée en plaçant les dispositions relatives à sa protection avant celles portant sur l'éducation au droit de la propriété intellectuelle ;

- en outre, plusieurs personnes entendues au cours des auditions avaient rappelé qu'Internet est également un outil de communication et d'information offrant de très nombreuses opportunités à nos concitoyens et qu'à ce titre, **il convient de ne pas le diaboliser**. Sensible à cette observation, votre rapporteur avait souhaité que l'article 1er de la proposition de loi fasse également référence aux aspects positifs d'Internet ;

- enfin, il lui avait semblé qu'il n'était pas nécessairement pertinent de confier cette sensibilisation à des enseignants spécialement « formés » sur le sujet. En effet, la sensibilisation aux enjeux de la protection de la vie privée relève moins d'une discipline académique que d'**une expérience et d'une appétence particulière de certains enseignants pour ce type de problématique**. Dans leur rapport précité, nos collègues Anne-Marie

Escoffier et Yves Détraigne avaient d'ailleurs estimé que cette sensibilisation pourrait être dispensée à l'occasion des **cours d'éducation civique**.

Ces préoccupations ont été partagées par la commission de la culture, de l'éducation et de la communication, qui s'est saisie pour avis de cette proposition de loi, et par son rapporteur pour avis, Mme Catherine Morin-Desailly. Votre commission a adopté un **amendement** présenté par cette dernière tendant à insérer les modifications introduites par l'article 1er de la proposition de loi au sein de l'article L. 312-15 du code de l'éducation, qui est consacré à l'enseignement d'éducation civique. Votre rapporteur a retiré son amendement au bénéfice de celui de la commission de la culture qui met l'accent sur la **responsabilisation** des jeunes vis-à-vis de leur propre image et de la protection de la vie privée.

Par coordination avec les modifications opérées à l'article 8, l'amendement a également remplacé les termes « *droit d'opposition commerciale* » par ceux, plus généraux, de « *droit d'opposition* ».

Votre commission a adopté l'article premier **ainsi modifié**.

TITRE II
DISPOSITIONS PORTANT MODIFICATION DE LA LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS

Article 2
(art. 2 de la loi « informatique et libertés »)
Qualification juridique de l'adresse IP

Cet article tend à **qualifier explicitement l'adresse IP de donnée à caractère personnel.**

A l'heure actuelle, l'article 2 de la loi « informatique et libertés » du 6 janvier 1978 qualifie de donnée à caractère personnel « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ».

Notion ambigüe et concept instable[1], l'adresse IP est aujourd'hui au cœur de la lutte contre le piratage, le téléchargement illicite et la lutte contre la contrefaçon. Néanmoins, son statut juridique fait l'objet de controverses qui ne peuvent que susciter un risque d'insécurité juridique.

---

[1] *Selon les termes utilisés par Marina Teller, « Les difficultés de l'identité numérique : quelle qualification juridique pour l'adresse IP ? », Recueil Dalloz 2009, page 1988.*

Qu'est-ce qu'une adresse IP ?

Sur Internet, les ordinateurs communiquent entre eux grâce au Protocole IP (*Internet Protocol*), qui utilise **des adresses numériques**, appelées adresses IP. Ces adresses sont composées de quatre nombres entiers compris chacun entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Chaque ordinateur relié à un réseau dispose d'une adresse IP unique, ce qui lui permet de communiquer avec les autres ordinateurs du même réseau. De même, chaque site Internet dispose d'une adresse IP, qui peut être convertie en nom de domaine. L'attribution des adresses IP publiques relève de l'ICANN (*Internet Corporation for Assigned Names and Numbers*).

Concrètement, chaque transmission de données sur le *web* donne lieu à l'envoi d'un « paquet de données » comprenant, quel que soit le type de communication (navigation sur le web, messagerie, téléphonie par Internet, etc.) l'adresse IP de l'expéditeur ainsi que celle du destinataire. Ainsi, lorsqu'un internaute consulte un site Internet, le serveur de ce dernier enregistre dans un fichier la date, l'heure et l'adresse IP de l'ordinateur à partir duquel la consultation a été effectuée, ainsi que les fichiers qui ont pu être envoyés. Le propriétaire du site a ainsi accès aux adresses IP des ordinateurs qui se sont connectés à son site. Dans le cas particulier des logiciels de « peer-to-peer » (logiciels permettant le partage de fichiers entre internautes), des tiers peuvent également récupérer assez facilement les adresses IP des internautes se livrant à la mise en ligne de fichiers piratés.

Source : « La vie privée à l'heure des mémoires numériques », rapport d'information n° 441 (2008-2009), Anne-Marie Escoffier et Yves Détraigne, 27 mai 2009

Comme le rappelle le rapport d'information de nos collègues Anne-Marie Escoffier et Yves Détraigne, et comme l'ont souligné un certain nombre de personnes entendues par votre rapporteur, **l'adresse IP ne permet pas, la plupart du temps, d'identifier directement l'internaute**. En effet, à la différence des entreprises ou des grandes institutions (telles que les universités), qui disposent en général d'une adresse IP fixe, les particuliers se voient attribuer la plupart du temps, par leur fournisseur d'accès, une adresse IP différente à chaque connexion. Dans ce cas, seul le fournisseur d'accès est capable de relier une adresse IP à une personne physique, à condition de disposer également de l'heure et de la date de connexion (et sous réserve que l'adresse IP n'ait pas fait l'objet d'une usurpation de la part d'internautes malveillants).

Ces arguments ont conduit la treizième chambre de la cour d'appel de Paris à estimer que l'adresse IP ne pouvait pas être considérée comme une donnée personnelle :

- dans un arrêt en date du 15 mai 2007, les juges ont considéré que « *cette série de chiffres* [ne constituait] *en rien une donnée indirectement nominative à la personne dans la mesure où* ***elle ne se rapporte qu'à une machine****, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* » ;

- puis, dans un arrêt daté du 27 avril 2007, la cour a estimé que « *l'adresse IP ne* [permettait] *pas d'identifier le ou les personnes qui ont*

utilisé cet ordinateur puisque ***seule l'autorité légitime*** *pour poursuivre l'enquête (police ou gendarmerie)* ***peut obtenir du fournisseur d'accès l'identité de l'utilisateur*** ».

Ces décisions ont suscité la réaction du **G29**[1], qui, dans **un avis du 20 juin 2007**, a rappelé que l'adresse IP attribuée à un internaute lors de ses communications devait être regardée comme une donnée à caractère personnel.

Cette position a été partagée par un certain nombre de juridictions françaises.

Ainsi, dans un arrêt daté du 6 septembre 2007 (*Ministère public, SCPP, SACEM c/ J.-P.*), le tribunal de grande instance de Saint-Brieuc a expressément qualifié l'adresse IP de donnée à caractère personnel, après avoir relevé qu' « *un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse W de la connexion associée au fournisseur d'accès* ***constitue un ensemble de moyens permettant de connaître le nom de l'utilisateur*** ».

Le tribunal de grande instance de Bobigny a également, dans un arrêt *Laurent F. c/ SACEM* daté du 14 décembre 2006, considéré que « *l'adresse IP* [constituait] *une donnée à caractère personnel en ce qu'elle permet d'identifier une personne en indiquant sans doute possible un ordinateur précis.* ***Le numéro IP établit la correspondance entre l'identifiant attribué lors de la connexion à l'internaute et l'identité de l'abonné*** »[2].

Cette solution a été confirmée à l'occasion de la révision de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques : la **directive 2006/24/CE**[3] dispose désormais dans son article 2 que les données à caractère personnel incluent les données relatives au trafic et les données de localisation ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur, ce qui inclut donc l'adresse IP.

En France, néanmoins, **la question demeure confuse**. Dans une décision rendue le 13 janvier 2009, la Chambre criminelle de la Cour de cassation a considéré que, lorsque la collecte des adresses IP s'effectue « *à la main* », et non au moyen d'un traitement informatique automatisé, l'autorisation de la CNIL n'est pas requise. Ce faisant, la Chambre criminelle n'a pas tranché le débat relatif au statut de l'adresse IP, ce qui semble particulièrement regrettable au regard du flou juridique qui subsiste sur cette question.

---

[1] Le G29 est un groupe de travail européen, créé par l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation, rassemblant les représentants de vingt-sept autorités indépendantes de protection des données nationales

[2] Voir également TGI Paris, réf., 5 mars 2009, Roland Magdane c/ Youtube.

[3] Relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE.

L'article 2 de la proposition de loi tend à **mettre un terme à ces divergences de jurisprudence** en incluant expressément l'adresse IP, qui serait définie comme « *toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication* », dans le champ des données à caractère personnel.

Votre commission **approuve cette démarche** qui permettra d'appliquer sans ambiguïté les garanties concernant la collecte de données à caractère personnel aux données de connexion des internautes.

Votre commission précise néanmoins que qualifier expressément l'adresse IP de donnée à caractère personnel ne revient pas à affirmer que celle-ci permet, à elle seule, d'identifier une personne physique. Il s'agit en revanche de préciser qu'elle constitue l'**un des éléments permettant d'identifier un internaute**. En cela, l'adresse IP répond aux critères posés par l'article 2 de la loi du 6 janvier 1978, qui définit la notion de donnée à caractère personnel comme « *toute information relative à une personne physique identifiée* ***ou qui peut être identifiée*** ». L'article 2 de la proposition de loi permettra ainsi de faire figurer l'adresse IP dans le « *faisceau d'indices permettant d'identifier l'internaute* »[1].

Néanmoins, sur proposition de son rapporteur, votre commission a souhaité modifier la rédaction de l'article 2 de la proposition de loi. En effet, son attention a été attirée sur le fait que la rédaction retenue visait l'adresse MAC de l'ordinateur[2], et non l'adresse IP attribuée par le fournisseur d'accès. Elle a donc souhaité **que soit visé « *tout numéro identifiant le titulaire d'un accès à des services de communication au public en ligne* »**. En outre, afin d'éviter toute ambiguïté, votre commission, sur proposition de son rapporteur, a souhaité **indiquer que l'adresse IP était incluse dans le champ des données à caractère personnel** visées à l'article 2 de la loi du 6 janvier 1978.

Votre commission a adopté l'article 2 **ainsi modifié**.

Article 2 bis (nouveau)
(art. 11 et 13 de la loi « informatique et libertés »)
Composition pluraliste de la CNIL

A l'initiative de votre rapporteur ainsi que de M. Charles Gautier et des membres du groupe socialiste apparentés et rattachés, votre commission a adopté un amendement de votre rapporteur tendant à insérer un article additionnel après l'article 2 afin d'assurer une **représentation pluraliste** lors de la désignation, par les présidents des assemblées parlementaires, des membres de ces assemblées appelés à siéger dans cette commission.

---

[1] *Marina Teller, article précité.*
[2] *Media Access Control Address. Une adresse MAC est l'identifiant unique de la carte physique indispensable pour la mise en réseau d'un ordinateur. Elle est spécifique à chaque constructeur.*

Cette mesure a été adoptée par l'Assemblée nationale à l'article 29 de la proposition de simplification et d'amélioration de la qualité du droit, telle que votée par les députés en première lecture[1]. Elle figurait déjà dans la proposition de loi n°1659 de Mme Delphine Batho et M. Jacques Alain Bénisti, adoptée à l'unanimité le 16 juin 2009 par la commission des lois de l'Assemblée nationale[2].

Elle prévoit que les deux députés et les deux sénateurs membres de la CNIL sont désignés *« de manière à assurer une représentation pluraliste »*. Au regard de l'importance que revêt l'action de la CNIL dans le domaine de la protection des données à caractère personnel, il semble nécessaire que **l'opposition y soit représentée**. L'exigence de pluralisme s'appréciera au vu de l'ensemble des membres désignés au sein de la CNIL par les deux assemblées.

Votre commission a adopté l'article 2 *bis* **ainsi rédigé.**

Article 2 ter (nouveau)
(art. 23 de la loi « informatique et libertés »)
Mise en œuvre plus rapide des traitements soumis à déclaration préalable

Votre commission a adopté un amendement tendant à insérer un article 2 *ter* afin de faciliter la mise en œuvre des traitements soumis à simple déclaration préalable auprès de la CNIL. En effet, dans sa rédaction actuelle, l'article 23 de la loi « informatique et libertés » subordonne la mise en œuvre de tels traitements à la transmission par la CNIL d'un **récépissé**.

Or, ce récépissé **retarde inutilement** la mise en œuvre du traitement.

En conséquence, l'amendement prévoit que *« le demandeur peut mettre en œuvre le traitement dès réception de la preuve de l'accomplissement de la formalité préalable »*. A titre d'exemple, cette preuve peut prendre la forme d'un accusé de réception postal si la déclaration a été adressée à la CNIL par lettre recommandée.

Cet amendement ne fait bien évidemment pas obstacle à l'exercice par la CNIL de ses pouvoirs de contrôle *a posteriori* si celle-ci constate que le responsable d'un traitement relevant de la formalité déclarative ne satisfait pas aux obligations résultant des dispositions de la loi « informatique et libertés ».

Votre commission a adopté l'article 2 *ter* **ainsi rédigé.**

---

[1] *Proposition de loi de simplification et d'amélioration de la qualité du droit, adoptée en 1ère lecture par l'Assemblée nationale le 2 décembre 2009, TA n° 376*

[2] Voir le rapport n° 1738 de Mme Delphine Batho et M. Jacques Alain Bénisti, au nom de la commission des Lois.

Article 3

(art. 31-1 nouveau de la loi « informatique et libertés »)

Renforcement du correspondant « informatique et libertés »

L'article 3 crée un article 31-1 dans la loi « informatique et libertés » afin de :

- rendre obligatoires les correspondants « informatique et libertés » (CIL) lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre ;

- mieux définir le rôle du CIL ;

- conforter son statut ;

- créer symboliquement, dans la loi « informatique et libertés », un chapitre et un article spécifiques consacrés au CIL.

En premier lieu, cet article traduit la recommandation n° 7 du rapport d'information précité sur « *la vie privée à l'heure des mémoires numériques* », à une réserve près : en effet, alors que le rapport recommandait de rendre obligatoires les correspondants « informatique et libertés » **dans les structures de plus de cinquante salariés,** la proposition de loi fait le choix de ne les rendre obligatoires que dans les structures où cinquante personnes ont soit directement **accès** au traitement, soit sont chargées de sa **mise en œuvre**. Il s'agit de ne pas imposer des correspondants dans des entreprises ou des administrations où travaillent certes plus de cinquante personnes mais où peu d'entre elles peuvent accéder aux bases de données personnelles ou les mettent en œuvre. On peut ainsi songer à une entreprise dont la majeure partie des salariés occupe des tâches d'exécution peu qualifiées.

Les CIL sont nés de la volonté du législateur, lors de l'examen du projet de loi qui a abouti à la loi n° 2004-801 du 6 août 2004[1], de donner la **possibilité** aux entreprises et administrations publiques d'identifier, en leur sein, des relais de la Commission nationale de l'informatique et des libertés (CNIL), garants du respect de la loi « informatique et libertés ». Cette possibilité était ouverte par le point 2 de l'article 18 de la directive du 24 octobre 1995[2]. En contrepartie, le législateur a décidé que les structures qui désigneraient un tel correspondant **ne seraient plus tenues d'adresser leurs déclarations à la CNIL**, le CIL étant chargé de recenser ces fichiers (article 22 de la loi « informatique et libertés »).

---

[1] *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

[2] *Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

Ces correspondants se sont mis en place peu de temps après la publication du décret n° 2005-1309 du 20 octobre 2005, soit à partir de 2005-2006.

Comme le souligne le rapport d'information précité, le bilan de l'action de ces correspondants apparaît **pleinement satisfaisant** tant ils ont permis la diffusion de la culture « informatique et libertés » dans les structures dans lesquelles ils ont été désignés mais également, symétriquement, la diffusion de la culture « administration » ou « entreprises » au sein de la CNIL. De même, le rapport d'information indique que, lors de leur audition, les représentants de la chambre de commerce américaine à Paris ont salué le rôle joué, dans l'administration fédérale américaine, des Chief Privacy Officers (CPO), équivalents des correspondants aux pouvoirs plus étendus, et se sont réjouis du caractère obligatoire des correspondants en Allemagne, présentés comme des « facilitateurs » pour la bonne marche de l'entreprise. A cet égard, on peut noter que de **nombreux autres pays européens ont rendu les correspondants obligatoires** : citons en particulier la Suisse (il est obligatoire pour les organes fédéraux), la Hongrie (il est obligatoire pour certaines catégories d'acteurs tels que les institutions financières, les fournisseurs d'accès à Internet...) ou encore la Slovaquie (il est obligatoire pour toute entité de plus de cinq employés).

En France, les correspondants sont en **augmentation constante** : au 1er janvier 2010, ils étaient 1466, regroupant quelque 5951 organismes, compte tenu des possibilités de mutualisation (*cf infra*). Ils sont toutefois faiblement implantés dans les collectivités territoriales et les ministères comme l'a souligné M. Alex Türk, président de la CNIL, lors de son audition par la commission des lois le 5 novembre 2008. Cette situation résulterait d'une certaine hostilité des autorités publiques à l'égard de personnes reconnues comme **indépendantes** dans l'exercice de leurs fonctions, indépendance qui s'accorderait mal avec le principe d'obéissance hiérarchique très ancré dans la fonction publique.

En second lieu, l'article 3 de la proposition de loi vise à préciser le rôle et les fonctions du CIL ; en effet, l'article 22 de la loi « informatique et libertés » ne définit que très succinctement sa mission : *« le correspondant est chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi ».* La proposition de loi complète ces dispositions en disposant que le CIL est également chargé d' *« informer l'ensemble des personnes travaillant pour le compte de l'autorité ou de l'organisme de la nécessité de protéger les données à caractère personnel ».*

En troisième lieu, l'article 3 de la proposition de loi conforte le statut du correspondant en subordonnant sa démission d'office à **l'accord de la CNIL**. Dans sa rédaction actuelle, l'article 22 de la loi « informatique et libertés » précise qu'*« en cas de manquement à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation de la CNIL ».* Le texte remplace la consultation par un **avis conforme** de la CNIL afin que cette dernière puisse juridiquement s'opposer à une démission qui ne

serait mue par des motifs d'opportunité, par exemple dans le cas de salariés dont les positions - pourtant conformes à la loi « informatique et liberté » - « gênent » la direction ou le responsable de traitement de l'organisme privé ou de l'autorité publique. La CNIL pourra ainsi refuser une démission quand aucune faute ne peut être reprochée au CIL dans l'exercice de ses fonctions.

Enfin, la proposition de loi crée symboliquement, dans la loi « informatique et libertés », **un chapitre et un article spécifiques** dédiés au CIL. La loi de 1978 ne traite aujourd'hui de ce correspondant que de manière incidente, à l'article 22 consacré aux formalités préalables à la mise en œuvre des traitements et aux possibilités d'exonération. En lui consacrant un chapitre et un article spécifiques, la proposition de loi entend conférer au CIL une **visibilité** dans la loi conforme à l'importance de sa mission.

Votre commission approuve largement **l'ensemble de ces modifications.** Elle considère en particulier que le principe d'indépendance n'est pas incompatible avec le statut de la fonction publique, comme l'illustre la présence, dans les ministères, de corps d'inspection et de contrôle ou de comptables.

Votre commission a toutefois adopté un amendement de réécriture des alinéas 4 à 7 afin d'apporter quelques **aménagements ou précisions**.

En premier lieu, votre rapporteur s'est longuement interrogé sur la pertinence du critère retenu par la proposition de loi pour déclencher l'obligation de désigner un CIL (cinquante personnes ayant un accès au traitement ou chargés de sa mise en œuvre). S'il juge favorablement l'évolution par rapport à la préconisation du rapport d'information (cinquante personnes sans plus de précision), il note que la rédaction proposée par le texte ne prend en compte :

- ni **les degrés d'intervention sur cette base** : ainsi « l'accès » ou « la mise en œuvre » n'impliquent pas nécessairement la possibilité d'extraire, de modifier ou de supprimer des noms ;

- ni l'**importance numérique de cette base,** c'est-à-dire le nombre de personnes concernées par le traitement : en effet, dix personnes peuvent avoir accès à une base comportant plusieurs millions de noms et, à l'inverse, des centaines de personnes peuvent avoir accès à une base très réduite ne comportant que quelques données : il est sans doute plus important, toutes choses égales par ailleurs, de créer un CIL dans le premier cas que dans le second ;

- ni **la nature des données traitées** : certaines données personnelles sont plus sensibles que d'autres (données médicales, religieuses, politiques…) et doivent donc être davantage protégées.

Votre commission a cherché à **formaliser ces nuances sans aboutir pour autant à une rédaction extrêmement complexe d'application.**

Elle a ainsi conservé le critère retenu par la proposition de loi mais en a ajouté un second, alternatif : le CIL serait **obligatoire non seulement dans les conditions prévues par la proposition de loi**[1] mais également lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel qui relève du **régime d'autorisation** en application des articles 25, 26 ou 27 de la loi « informatique et libertés ». Ce régime concerne les **traitements sensibles** qui ne peuvent être autorisés que par la CNIL (article 25) ou le Gouvernement (articles 26 et 27) après avis motivé et publié de la CNIL. Certes, il n'a pas échappé à votre rapporteur qu'une telle obligation n'aura pas de contrepartie pour les structures concernées : en effet, la présence obligatoire d'un CIL n'aura pas pour effet d'affranchir la structure publique ou privée d'obtenir l'autorisation susmentionnée. Toutefois, il paraît nécessaire que, eu égard à la nature des données traitées, ces structures soient toutes dotées d'un correspondant afin qu'elles intègrent de manière satisfaisante la culture « informatique et libertés ».

En second lieu, votre commission a apporté certaines **clarifications** au dispositif proposé.

D'une part, elle a précisé l'obligation de création d'un CIL dans certaines hypothèses ne remettait pas en cause la possibilité, **pour toute structure**, de mettre en place de tels correspondants et de bénéficier ainsi de la dispense des formalités déclaratives. A cet égard, votre rapporteur insiste sur le fait que le correspondant ne doit pas être perçu comme une **charge ou une contrainte** pour la structure, mais bel et bien comme une **aide, une garantie** et même un **élément de valorisation** vis-à-vis de ses clients ou usagers. D'autre part, votre commission a jugé fondées les craintes exprimées par certaines personnes entendues par votre rapporteur selon lesquelles la rédaction proposée par le texte pouvait laisser accroire que la **mutualisation** des CIL serait dorénavant exclue. Rappelons en effet que le décret précité du 20 octobre 2005 prévoit, en son article 44, des possibilités de mutualisation à une double condition :

- que plus de cinquante personnes soient chargées de la mise en œuvre ou aient directement accès aux traitements ;

- que les structures aient entre elles un lien économique (par le biais de filiales, de groupements d'intérêt économique, d'organismes professionnels…).

En conséquence, votre commission a précisé que la désignation obligatoire du CIL pouvait intervenir **dans un cadre mutualisé**. Elle a également rendu possible la mutualisation lorsque la création du CIL n'est pas obligatoire.

---

[1] *C'est-à-dire, rappelons-le, dans les structures où cinquante personnes ont soit directement accès au traitement, soit sont chargées de sa mise en œuvre.*

En troisième lieu, votre commission a **étendu** le rôle du correspondant. D'une part, elle a indiqué que ce dernier est investi d'une mission d'information, ce que prévoit la proposition de loi, mais également de **conseil** auprès de l'ensemble des personnes travaillant pour le compte de l'autorité ou de l'organisme. D'autre part, elle a précisé l'obligation pour le correspondant de tenir une liste des traitements effectués, en indiquant qu'il devait régulièrement la **mettre à jour** compte tenu de la création de plus en plus fréquente de listes. Nous verrons plus loin que votre commission a également souhaité que le correspondant joue un rôle central en matière de **failles de sécurité** (*cf commentaire de l'article 7*).

En quatrième lieu, votre commission a rétabli le texte actuel de la loi « informatique et libertés » en matière de d'avis de la CNIL en cas de démission d'office du correspondant. Si la proposition de loi fait le choix d'un avis conforme, l'amendement préfère le terme actuel de consultation, c'est-à-dire d'**avis simple**, ce qui préserve une **certaine souplesse de** gestion pour les structures concernées par l'obligation de désigner un CIL et répond aux critiques selon lesquelles le CIL serait un « salarié protégé ».

Enfin, votre commission a tenu à **resserrer les liens entre la CNIL et les CIL**, suivant en cela la logique de la proposition de loi elle-même qui a subordonné une démission d'office du CIL à l'accord de la CNIL (*cf supra*).

Ont ainsi été prévues :

- la possibilité pour la CNIL de **refuser** la désignation d'un CIL qui ne présente pas de **garanties suffisantes de compétence** ; certes, la loi prévoit aujourd'hui que toute désignation d'un CIL s'accompagne d'une notification à la CNIL qui comprend, aux termes de l'article 42 du décret précité de 2005, *« tout élément relatif aux qualifications ou références professionnelles du correspondant et, le cas échéant, de son préposé en rapport avec cette fonction »*. Mais ni la loi ni le décret ne permettent à la CNIL de s'opposer à la désignation d'un correspondant. Or, il apparaît légitime que la CNIL puisse refuser la nomination d'un correspondant si ses compétences semblent fragiles, en particulier dans le domaine du droit, de l'informatique, du conseil et du management (le correspondant a un rôle d'information et d'audit de l'organisme) ainsi que dans celui de la médiation et de la pédagogie (le correspondant vise à favoriser le dialogue entre le responsable du traitement, les personnes faisant l'objet du traitement et la CNIL) ;

- l'obligation pour le CIL de **saisir la CNIL des difficultés qu'il rencontre** ; aux termes de la rédaction actuelle de la loi (non modifiée par la proposition de loi), le correspondant « peut » saisir la CNIL des difficultés qu'il rencontre dans l'exercice de ses missions ; il est apparu préférable de prévoir une obligation et non une simple faculté ;

- l'obligation pour le CIL de transmettre à la CNIL son rapport annuel d'activité ; en effet, l'article 43 du décret précité de 2005 dispose que le CIL établit un bilan annuel de ses activités qu'il présente au responsable des traitements et **qu'il tient à la disposition de la commission**. Votre

commission a jugé opportun de faire évoluer cette formulation en transmission obligatoire à la CNIL et d'inscrire ce principe directement dans la loi, dans un souci de lisibilité.

D'une manière générale, votre rapporteur encourage toutes les initiatives visant à favoriser le **resserrement des liens entre la CNIL et son réseau de correspondants** à la fois pour mieux informer les responsables de traitement mais aussi pour permettre à la CNIL d'être davantage au fait des réalités et difficultés du terrain. Il note avec satisfaction que les CIL disposent :

- d'une ligne téléphonique et d'une adresse électronique dédiées, qui leur permettent d'avoir un accès rapide et privilégié aux services de la CNIL ;

- d'ateliers d'information sur la loi « informatique et libertés » et son application dans certains domaines clés (santé, ressources humaines, collectivités locales …) ;

- depuis le 4 mai 2009, d'un extranet proposant des services exclusifs et notamment des forums de discussion et des outils pratiques (modèles de lettres, de fiches techniques…) ; il s'agit d'un nouvel outil qui permet d'accompagner les CIL au quotidien dans l'exercice de leurs missions.

Votre commission a adopté l'article 3 **ainsi modifié**.

Article 4
(art. 26 de la loi « informatique et libertés »)
Autorisation de création des fichiers de police

Cet article tend à prévoir que **les grandes catégories de traitements de données personnelles intéressant la sécurité publique ou la lutte contre la délinquance et la criminalité, communément appelés « fichiers de police », ne peuvent être autorisées que par la loi**.

La notion de « fichiers de police » recouvre en réalité plusieurs types de traitements de données automatisés. Les principaux sont les suivants :

- **les fichiers d'antécédents judiciaires**, qui permettent de collecter des informations au cours des procédures judiciaires afin de faciliter la constatation des infractions pénales, le rassemblement des preuves des infractions et la recherche de leurs auteurs ; il s'agit du système de traitement des infractions constatées (STIC) de la police nationale et du système judiciaire de document et d'exploitation (JUDEX) de la gendarmerie nationale ;

- **les fichiers d'identification judiciaire**, qui ont pour finalité l'identification des auteurs d'infraction et des personnes disparues ; au sein de cet ensemble figurent le fichier automatisé des empreintes digitales (FAED) et le fichier national des empreintes génétiques (FNAEG), qui ont tous deux connu récemment une très forte croissance en terme de nombre de données collectées ;

- **les fichiers spécialisés** qui permettent de cibler certaines infractions comme le fichier des brigades spécialisées (FBS) et le fichier des véhicules volés (FVV) ;

- **les fichiers de renseignement**, tels que les récents fichiers relatifs respectivement à la prévention des atteintes à la sécurité publique et aux enquêtes administratives liées à la sécurité publique (décret n° 2009-1249 et n° 2009-1250 du 16 octobre 2009), faisant suite à l'abandon du projet de fichier « Edwige » ;

- d'origine plus récente, **les fichiers de rapprochements de faits ou de modes opératoires de délits sériels**, tels que le logiciel d'analyse criminel de la gendarmerie (ANACRIM) et le système d'analyse et de liens de la violence associés au crime (SALVAC).

En l'état actuel du droit, il existe deux possibilités distinctes pour créer de tels fichiers.

Tout d'abord, sur le fondement de l'article 26 de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, **peuvent être créés par arrêté ou décret en Conseil d'État, pris après avis motivé et publié de la CNIL**, les traitements de données « qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ». Un décret en Conseil d'État est nécessaire pour les fichiers de police qui portent sur des données sensibles définies à l'article 8 de la loi informatique et libertés (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale des personnes, santé et vie sexuelle).

En second lieu, le gouvernement peut être autorisé par le législateur à créer tel ou tel fichier de police. **Le nombre de ces habilitations législatives tend, ces dernières années, à augmenter de manière sensible, de telle sorte que le régime défini par la loi « Informatique et libertés » a été beaucoup moins appliqué**. À titre d'exemple, l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme autorise le ministère de l'intérieur à créer le fichier des passagers aériens et son article 8 le traitement automatisé de contrôle des données signalétiques des véhicules. De même, le fichier national des immatriculations a été créé par la loi n° 90-1131 du 19 décembre 1990, tandis que le fichier national automatisé des empreintes génétiques a été autorisé par la loi n° 98-468 du 17 juin 1998.

Toutefois, le gouvernement est revenu récemment à la méthode de création par la voie réglementaire. **Ont ainsi été créés par décrets deux nouveaux fichiers relatifs respectivement à la prévention des atteintes à la sécurité publique et aux enquêtes administratives liées à la sécurité publique**[1]. Cette création a fait suite à l'abandon du projet de fichier

---

[1] *Décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et décret n° 2009-*

« Edwige » (exploitation documentaire et valorisation de l'information générale) créé par un décret du 27 juin 2008, et qui avait suscité de fortes inquiétudes en autorisant la collecte d'informations sur toute personne jouant un rôle politique, social, religieux ou économique, y compris les données relatives à la santé et à l'orientation sexuelle.

En outre, certains fichiers sont mis en œuvre en dehors de tout cadre juridique. Tel est le cas d'un quart des fichiers environ, dont par exemple le fichier des objets signalés et le système de traitement des images des véhicules volés de la gendarmerie nationale, ou encore le fichier des brigades spécialisées de la police nationale.

Enfin, il arrive qu'un fichier de police créé par décret en Conseil d'État reçoive une base législative quelques années plus tard, ce qui semble quelque peu contraire à la hiérarchie des normes. Ainsi, le STIC a tout d'abord fait l'objet du décret n° 2001-583 du 5 juillet 2001 et s'est ensuite vu conférer une base législative par l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

Ceci reflète le caractère pragmatique et empirique du processus de création des fichiers de police. Les services de police et de gendarmerie conçoivent et mettent en œuvre les outils dont ils ont besoin. Une fois les fichiers pleinement opérationnels, ces services s'efforcent de leur donner une base juridique. L'acte juridique autorisant le traitement ne fait alors que reprendre et constater un simple état de fait.

Cette situation quelque peu confuse ainsi que l' « affaire » du fichier Edwige a suscité la rédaction d'un rapport d'information de la commission des lois de l'Assemblée nationale sur les fichiers de police, par Mme Delphine BATHO et M. Jacques Alain BÉNISTI, et une proposition de loi des mêmes auteurs « *visant à créer un cadre juridique régissant les fichiers tout en garantissant les conditions de leur modernisation* » déposée par les mêmes auteurs. **Le rapport préconise que l'article 26 de la loi du 6 janvier 1978 soit modifié pour prévoir que les fichiers ou toute catégorie de fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne soient autorisés que par la loi.**

Parallèlement, M. Yves Détraigne et Mme Anne-Marie Escoffier ont, dans le rapport d'information précité, relevé la confusion qui prévaut en la matière et estimé également qu'il **« semble légitime, compte tenu de l'importance de ces fichiers et des précautions qu'ils requièrent, qu'ils ne puissent plus être autorisés que par la loi** ».

Plutôt que de prévoir une autorisation législative pour chaque fichier de police, les auteurs de la proposition de loi ont souhaité inscrire une

---

1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique

autorisation **pour chaque catégorie de fichier de police,** une catégorie rassemblant « *les traitements qui répondent à une même finalité, portent sur les mêmes catégories de données et ont les mêmes catégories de destinataires* ». Ainsi, le gouvernement pourrait créer par des actes réglementaires une pluralité de traitements correspondant à une catégorie autorisée par la loi.

Deux catégories de fichiers disposent déjà d'un tel cadre fixé par la loi :

-les fichiers d'antécédents judiciaires sont encadrés par l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure : les décrets sur le système de traitement des infractions constatées (STIC) et sur le système judiciaire d'exploitation et de documentation (JUDEX) ont été pris pour application de ce texte respectivement le 14 octobre et 20 novembre 2006 ;

-les fichiers d'analyse sérielle, dont le régime est déterminé par l'article 21-1 de la loi de 2003 précitée, créé par la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales : il s'agit des fichiers SALVAC et ANACRIM cités ci-dessus.

Par ailleurs, le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), actuellement en cours d'examen à l'Assemblée nationale, comporte des dispositions de codification (dans le code de procédure pénale) de dispositions législatives intéressant les fichiers d'antécédents judiciaires et d'analyse sérielle.

La présente proposition de loi propose ainsi de **généraliser cette pratique d'autorisation par la loi des catégories de traitements intéressant la sécurité publique ou la lutte contre la délinquance et la criminalité**.

En outre, elle propose que chaque loi autorisant une catégorie de fichier porte mention des services responsables et des finalités des traitements appartenant à la catégorie ainsi que de la durée de conservation des données traitées.

Enfin, l'avis consultatif de la CNIL sur tout projet de loi autorisant la création d'une catégorie de fichiers devrait être transmis au Parlement simultanément au dépôt du projet de loi afin de garantir l'information la plus complète possible du législateur et d'inciter le gouvernement à associer davantage la CNIL en amont de la création des fichiers.

La position de la commission

Ce dispositif ne constituerait pas une totale innovation dans la mesure où, comme il a été dit ci-dessus, plusieurs fichiers ou catégories de fichiers de police ont récemment été créés par des lois, de sorte que le régime prévu par l'article 26 de la loi CNIL, qui prévoit que les décrets sont créés par arrêté ou décret après avis de la commission, apparait désormais plutôt comme l'exception.

Par ailleurs, il semble légitime de prévoir que le législateur puisse se prononcer sinon sur chaque fichier, du moins sur les catégories de fichiers ayant une même finalité, **dans la mesure où la question relève bien des « garanties fondamentales accordées au citoyen pour l'exercice des libertés publiques » pour lesquelles la loi fixe les règles selon l'article 34 de la Constitution**. Une telle intervention du législateur aurait sans doute été de nature à éviter certaines polémiques lors de la création par voie réglementaire du fichier EDVIGE, en garantissant un débat sur les finalités des fichiers de ce type, et en permettant d'atteindre un équilibre plus solide entre d'une part la nécessité de donner aux forces de l'ordre les instruments nécessaires pour qu'elles puissent exercer efficacement leurs missions et d'autre part la protection des libertés individuelles.

Toutefois, la formulation de la proposition de loi présente l'inconvénient de donner l'impression que le législateur prétend se lier lui-même en s'obligeant à intervenir dans le futur pour créer des catégories de fichiers de police. Sans censurer cette disposition, le Conseil constitutionnel, s'il en était saisi, relèverait très probablement son caractère non normatif.

En revanche, il appartient bien au législateur, s'agissant d'une matière qui relève de l'article 34 de la Constitution, de fixer les règles encadrant la création des fichiers de police.

Cette problématique a déjà été traitée par l'Assemblée nationale lors de l'examen de la proposition de loi précitée. Cette proposition présentait en effet ce même inconvénient de prétendre lier le législateur pour l'avenir, en prévoyant que tout nouveau fichier de police devrait être créé par la loi, sans fixer elle-même de cadre juridique détaillé pour ces fichiers. Il avait finalement été décidé de contourner cette difficulté **en encadrant davantage, par des dispositions législatives, le champ d'action du pouvoir réglementaire, par la fixation d'une liste de finalités**. **Tout fichier créé par arrêté ou par décret devrait ainsi appartenir à au moins une des finalités citées**. La rédaction de la liste de finalités permettait par ailleurs d'englober la plupart des fichiers existants, créés par des actes réglementaires ou sans fondement juridique spécifique. En revanche, cette rédaction impliquerait que le gouvernement dépose un nouveau projet de loi dès lors qu'il souhaiterait que les services de l'Etat puissent créer des fichiers de police dont les finalités ne sont pas couvertes par la liste.

Ces dispositions ont été introduites dans la proposition de loi de simplification et d'amélioration de la qualité du droit, telle que votée par les députés en première lecture[1].

---

[1] *Proposition de loi de simplification et d'amélioration de la qualité du droit, adoptée en 1ère lecture par l'Assemblée nationale le 2 décembre 2009, texte n° 130 (2009-2010) transmis au Sénat le 3 décembre 2009*

Votre commission a estimé qu'une telle solution présentait l'avantage capital **de faire « remonter » au niveau législatif l'ensemble des finalités des fichiers de police, alors que le gouvernement avait auparavant le choix entre un projet de loi et un simple arrêté ministériel**. Non seulement tout nouveau projet de création dont les finalités n'entreraient pas dans celles prévues par la loi devrait ainsi faire l'objet d'un nouveau projet de loi, mais, en outre, les finalités actuellement recensées pourraient être amendées afin de modifier la nature d'un fichier ou d'un ensemble de fichier si le législateur considère que ces finalités ne sont plus pertinentes.

Tout en reprenant ce dispositif en estimant qu'il avait davantage sa place au sein de la présente proposition de loi que dans un texte comportant diverses dispositions de simplification du droit, votre commission a toutefois souhaité apporter deux modifications à la rédaction adoptée par les députés : d'une part, les traitements intéressant la sûreté de l'Etat et la défense sont intégrés au sein de l'ensemble des fichiers de police et leurs finalités entrent ainsi dans le champ d'intervention du législateur (pour le reste leur régime juridique ne serait pas modifié et les actes réglementaires de création de ces fichiers pourraient continuer à être dispensés de publication) ; **d'autre part la sixième finalité** *(« Centraliser les informations destinées à informer le gouvernement et le représentant de l'Etat afin de prévenir les atteintes à la sécurité publique ou à procéder aux enquêtes administratives liées à la sécurité publique »*) **est scindée en deux afin de clairement distinguer ce qui relève de la prévention des atteintes à la sécurité publique et ce qui concerne les enquêtes administratives**.

Par ailleurs, cet amendement détermine un régime spécifique concernant les mineurs pour les traitements relevant du 7° du I, c'est-à-dire pour les fichiers de renseignement mis en œuvre par le ministère de l'intérieur. La durée de conservation des données personnelles les concernant devrait ainsi être inférieure à celle prévue pour les majeurs, afin de renforcer leur « droit à l'oubli ».

Serait également prévue **la publication de l'ensemble des actes réglementaires créant des traitements de données intéressant la sécurité publique**. Pourraient donc dorénavant seuls être dispensés de publication les actes concernant les traitements intéressant la sûreté de l'État ou de la défense alors que la législation actuelle autorise le Gouvernement à ne pas publier les actes réglementaires créant des fichiers de police dans leur ensemble. Cette disposition entérine la pratique actuelle puisque le II de l'article 26 de la loi CNIL, qui permet cette dispense de publication pour tous les types de fichiers de police, a connu une application très restrictive, seuls les fichiers de renseignement en ayant bénéficié[1].

---

[1] *Décret n°2007-914 du 17 mai 2007pris pour l'application du I de l'article 30 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

En outre, les actes réglementaires non publiés créant des traitements intéressant la défense ou la sécurité nationale **seraient transmis à la délégation parlementaire au renseignement et à la CNIL**.

Enfin, **votre commission a retenu le mécanisme d'expérimentation introduit dans la proposition de loi de simplification et d'amélioration de la qualité du droit pour les traitements dont la mise en œuvre nécessite une phase expérimentale**. Ce point représente une avancée très importante car il permet à la CNIL d'intervenir en amont de l'élaboration d'un fichier de police et donc éventuellement d'infléchir le projet avant qu'il ne soit complètement « verrouillé ». Dans la situation actuelle en effet, les services de l'Etat sont conduits à présenter les traitements informatisés dans leur état final à la CNIL, ce qui présente le double inconvénient de ne pas permettre à celle-ci de suggérer des modifications en cours d'élaboration et d'obliger ceux-là à remettre en cause toute l'architecture de leur projet pour faire droit aux demandes tardives de la CNIL.

Votre commission a adopté l'article 4 **ainsi modifié**.

Article 4 bis (nouveau)
(art. 8, 27, 31, 44 et 49 de la loi « informatique et libertés »)
Coordinations

Cet article, issu d'un amendement du rapporteur, effectue les coordinations nécessaires au sein de la loi du 6 janvier 1978 rendues nécessaires par la nouvelle rédaction de l'article 26 de cette loi.

Votre commission a adopté l'article 4 **bis ainsi rédigé.**

Article 4 ter (nouveau)
(art. 13 de la loi « informatique et libertés »)
Création au sein de la CNIL d'une formation spécialisée chargée des fichiers de police

Afin de contribuer à l'amélioration du dialogue technique entre la CNIL et les services chargés de la mise en œuvre des fichiers, il est proposé, par cet article issu d'un amendement du rapporteur, de créer **une formation spécialisée au sein de la CNIL, consacrée aux fichiers de police**. Elle aurait pour missions l'instruction des demandes d'avis sur les les projets d'actes réglementaires créant les traitements ; le suivi des procédures de mise en œuvre expérimentale des traitements ; enfin l'organisation, en accord avec les responsables des traitements concernés, des modalités d'exercice du droit d'accès indirect.

Cette formation serait élue par la CNIL et serait composée de trois membres, dont deux membres ou ancien membres du Conseil d'État, de la Cour des comptes ou de la Cour de cassation.

Votre commission a adopté l'article 4 **ter ainsi rédigé.**

Article 4 quater (nouveau)
(art. 16 de la loi « informatique et libertés »)
Extension des compétences du bureau de la CNIL

Cet article, issu d'un amendement du rapporteur reprenant, comme l'ensemble des articles additionnels après l'article 4, de la proposition de loi de simplification et d'amélioration de la qualité du droit précitée, permet de confier au bureau de la CNIL la possibilité d'émettre des avis au nom de celle-ci dans le cadre de la démarche d'expérimentation mentionnée au V de l'article 26 de la loi n° 78-17 du 6 janvier 1978 dans sa nouvelle rédaction. Comme indiqué ci-dessus, il s'agit de favoriser le dialogue technique en amont entre la CNIL et les services expérimentant des traitements préalablement à leur création par un acte réglementaire.

Votre commission a adopté l'article 4 quater **ainsi rédigé.**

Article 4 quinquies (nouveau)
(art. 29 de la loi « informatique et libertés »)
Durée de conservation des données et modalités de traçabilité

Cet article, issu d'un amendement du rapporteur, propose de modifier la rédaction de l'article 29 de la loi « Informatique et Libertés » afin de rendre obligatoire dans les actes qui créent des fichiers de police l'inscription de la durée de conservation des données et les modalités de traçabilité des consultations du traitement.

Votre commission a adopté l'article 4 quinquies **ainsi rédigé.**

Article 4 sexies (nouveau)
(art. 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires)
Information systématique de la délégation parlementaire au renseignement sur les traitements dispensés de la publication des actes réglementaires les créant

Par coordination avec la nouvelle rédaction de l'article 26 de la loi « informatique et libertés », cet article, issu d'un amendement du rapporteur, prévoit la transmission à la délégation parlementaire au renseignement de tout décret en Conseil d'État créant un traitement dont il a été prévu une dispense de publication au Journal Officiel.

Votre commission a adopté l'article 4 **sexies ainsi rédigé.**

Article 4 septies (nouveau)
(art. 21 de la loi n° 2003-239 du 18 mars 2003)
Amélioration du contrôle des fichiers d'antécédents judiciaires par le procureur de la République

Cet article, issu d'un amendement du rapporteur, vise à renforcer l'efficacité du contrôle des fichiers d'antécédents judiciaires par le procureur de la République.

Le 1° permet de faire figurer dans la loi le délai de traitement des demandes de mise à jour des fichiers d'antécédents judiciaires en fonction des suites judiciaires dans la loi, tout en le ramenant à un mois (au lieu de trois actuellement).

Le 2° maintient la faculté accordée au procureur de la République de maintenir dans les fichiers d'antécédents judiciaires les données personnelles d'une personne ayant bénéficié d'une décision de relaxe ou d'acquittement, mais il prévoit, en contrepartie, qu'une telle décision doit être notifiée par le procureur à la personne concernée.

Le 3° prévoit que, pour les autres types de classement sans suite que le classement motivé par une insuffisance de charges (pour lequel les données personnelles au sein du STIC ou de JUDEX peuvent être effacées), ils feront l'objet d'une mention dans ces fichiers, ce qui constituera un progrès par rapport à la situation actuelle. En effet, toute personne qui consultera les données personnelles d'un individu inscrit dans un de ces fichiers sera avisée que cet individu a bénéficié d'une mesure de classement sans suite.

Enfin, la deuxième disposition introduite par le 3° prévoit que toutes les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République seront systématiquement transmises aux responsables des autres traitements automatisés pour lesquels ces mêmes décisions sont susceptibles d'avoir une incidence sur la durée de conservation des données.

Votre commission a adopté l'article 4 **septies ainsi rédigé.**

Article 4 octies (nouveau)
(art. 397-5 du code de procédure pénale)
Utilisation par le ministère public des fichiers d'antécédents judiciaires dans le cadre des procédures de comparution immédiate

Cet article, issu d'un amendement du rapporteur, vise à mieux préciser les conditions d'utilisation des données figurant dans des fichiers d'antécédents judiciaires lors de procédures de comparution immédiate, afin d'établir une forme d' « égalité des armes » entre l'accusation et la défense.

Comme l'indique le rapport d'information de M. Jacques-Alain Bénisti et Mme Delphine Batho sur les fichiers de police précité, l'utilisation des fichiers de police par le ministère public au cours du procès pénal n'est pas sans conséquences sur l'équilibre entre défense et accusation.

À la différence du FNAEG, dont les éléments sont versés au dossier et peuvent faire l'objet d'une demande d'expertise contradictoire par la défense, les fichiers d'antécédents judiciaires sont souvent utilisés par l'accusation de manière orale, sans que la défense puisse y avoir accès. La mention des affaires dans laquelle une personne a été mise en cause

précédemment peut jouer un rôle non négligeable dans l'opinion que se forme le juge, tout particulièrement en cas de comparution immédiate.

Afin de remédier à cette situation, il est proposé de compléter l'article 395 du code de procédure pénale en prévoyant que si le procureur de la République envisage de faire mention d'éléments concernant le prévenu et figurant dans un fichier d'antécédents judiciaires, il doit les verser au dossier auquel l'avocat a accès au titre du troisième alinéa de l'article 393 du même code.

Votre commission a adopté l'article 4 **octies ainsi rédigé.**

Article 5
(art. 31 de la loi « informatique et libertés »)
Obligation pour la CNIL d'indiquer au public la durée de conservation des données

L'article 5 modifie l'article 31 de la loi « informatique et libertés » afin que la liste des traitements de données que la CNIL met à la disposition du public précise, pour chacun de ces traitements, **la durée de conservation des données.**

La délivrance de cette information se justifie d'autant plus que le responsable de traitement doit, lors de sa déclaration à la CNIL, indiquer à cette dernière « *la durée de conservation des informations traitées* » (article 30, I, 5° de la loi « informatique et libertés ») et que, si un correspondant a été désigné, celui-ci tenir un registre de tous les traitements avec pour chacun d'entre eux la durée de conservation des données (article 48 du décret précité de 2005).

Votre commission a adopté l'article 5 **sans modification**.

Article 5 bis (nouveau)
(art. 31 de la loi « informatique et libertés »)
Publicité des avis de la CNIL

A l'initiative de M. Alex Türk, votre commission a adopté un article 5 *bis* afin d'apporter une précision importante en matière de **publicité des avis de la CNIL**. Elle a prévu que chaque fois qu'une loi renvoie à des textes règlementaires d'application pris « *après avis de la CNIL* », sans autre forme de précision, les avis de la CNIL sont par principe publics.

La question se pose surtout en matière de **fichiers de police** : en effet, en vertu de l'article 26 de la loi « informatique et libertés », ces fichiers font l'objet d'un **avis public** de la CNIL, mais sont souvent créés sans faire référence à cet article.

A titre d'exemple, l'article 5 *bis* du projet de loi « récidive » crée un fichier des expertises psychiatriques, médico-psychologiques, psychologiques et pluridisciplinaires. Il précise que les caractéristiques essentielles de ce fichier seront définies par décret en Conseil d'Etat après avis de la CNIL.

Toutefois, il n'indique que cet avis sera rendu public conformément à l'article 26 de la loi « informatique et libertés ».

L'amendement, de portée générale, apporte donc une opportune clarification. Ainsi ne pourra-t-on plus interpréter le silence de la loi en matière d'application de l'article 26 précité comme remettant en cause la publicité de l'avis de cette Commission.

Votre commission a adopté l'article 5 *bis* **ainsi rédigé.**

Article 6
(art. 32 de la loi « informatique et libertés »)
Obligations d'information du responsable de traitement

L'article 6 de la proposition de loi réécrit une grande partie de l'article 32 de la loi « informatique et libertés » afin **d'étendre les obligations d'information du responsable du traitement**.

En premier lieu, cet article prévoit que l'information visée à l'article 32, c'est-à-dire **l'information sur les caractéristiques principales du traitement de données personnelles**, doit être délivrée, avant ledit traitement, de manière **spécifique, claire et accessible**.

Par « *information spécifique* », il faut entendre une information distincte des conditions générales de vente ou d'utilisation. En effet, si de plus en plus de sites marchands cherchent à délivrer, à côté des conditions générales de vente, une information spécifique, généralement sous une rubrique « vie privée » ou « protection des données personnelles », ils sont encore largement minoritaires et, le plus souvent, les responsables de traitement font aujourd'hui figurer ces informations parmi les dispositions générales (livraison du produit, facturation, conditions de remboursement…).

Par « *information claire* », il faut entendre une information qui soit intelligible, c'est-à-dire rédigée en des termes simples, non techniques et que toute personne normalement attentive doit pouvoir aisément comprendre. D'après les auteurs de la proposition de loi, entendus par votre rapporteur, cette exigence de clarté peut, par exemple, être satisfaite par de courtes vidéos pédagogiques, notamment quand le site Internet s'adresse aux jeunes générations, davantage enclines à regarder une vidéo qu'à lire un texte.

Par « *information accessible* », il faut entendre une information à laquelle une personne normalement attentive peut avoir accès sans effort particulier. Alors que la clarté renvoie à une notion intellectuelle, l'accessibilité a trait, quant à elle, à une notion de présentation. Ainsi l'information devra-t-elle être repérée sans difficultés et figurer en caractères suffisamment grands.

En second lieu, l'article 6 de la proposition de loi **étend la liste des mentions** que le responsable de traitement doit **obligatoirement** porter à la connaissance de la personne objet du traitement. Cette extension n'est pas contraire à la directive précitée du 24 octobre 1995 puisque son article 10 dispose qu' *« en cas de collecte de données auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant* ***au moins*** *les informations énumérées ci-dessous ».*

Deux nouvelles mentions deviennent obligatoires : la **durée** de conservation des données collectées et les modalités d'exercice des **droits d'accès, de rectification et de suppression** par voie électronique.

Tout d'abord, la durée de conservation des données collectées constitue, pour les personnes qui font l'objet du traitement, une information **tout aussi essentielle** que l'identité du responsable de traitement ou la finalité de ce dernier. La proposition de loi fait donc le choix d'ajouter cette mention. Rappelons que le rapport d'information précité sur « *la vie privée à l'heure du numérique »* préconise de faire du citoyen « *l'acteur de sa propre protection* » ou le « *gendarme de ses propres données* ». Or, il ne peut exercer cette vigilance que s'il est informé **en toute transparence** de la durée de conservation des données qu'il s'apprête à livrer au responsable de traitement. Comme indiqué précédemment (voir commentaire de l'article 5), la délivrance de cette information se justifie d'autant plus que le responsable de traitement doit, lors de sa déclaration à la CNIL, indiquer à cette dernière « *la durée de conservation des informations traitées* » et que, si un correspondant a été désigné, celui-ci doit tenir un registre de tous les traitements avec pour chacun d'entre eux la durée de conservation des données.

La seconde mention que la proposition de loi rend obligatoire concerne la possibilité d'exercer les droits d'accès, de rectification et de suppression par **voie électronique, après identification**. L'objectif est de faciliter l'exercice de ces droits alors que les responsables de traitement prévoient aujourd'hui généralement la seule transmission par **courrier postal**, de nature à décourager les personnes concernées.

En troisième lieu, l'article 6 de la proposition de loi crée une obligation pour le responsable du traitement disposant d'un site Internet d'y créer une rubrique spécifique, claire, accessible et permanente reprenant les mentions obligatoires prévues au I de l'article 32, complétées comme indiqué précédemment. Il s'agit d'une **obligation distincte** de celle évoquée plus haut, qui ne concerne que l'information donnée **au moment** du recueil des données. C'est pourquoi l'information doit être délivrée, non seulement de manière « *spécifique, claire, accessible* » mais également de manière **permanente**, c'est-à-dire **indépendamment de tout traitement**. Concrètement, si le responsable de traitement dispose d'un site Internet, il devra indiquer dans une rubrique dédiée toutes les caractéristiques des traitements qu'il est susceptible

d'effectuer : finalité, durée de conservation, cession des informations à des tiers... Notons que lorsqu'il recueille effectivement des données personnelles, il pourra renvoyer à cette rubrique permanente, située, par exemple, à côté des « mentions légales ».

Enfin, l'article 6 de la proposition de loi apporte **deux modifications importantes au régime juridique des « cookies ».**

D'une part, il renforce **l'obligation d'information** incombant au responsable du traitement. Tel qu'il est actuellement rédigé, l'article 32 de la loi « *informatique et libertés* » dispose que l'information doit être « *claire et complète* ». La rédaction proposée est « *spécifique, claire, accessible et permanente* ». Elle ne reprend pas l'adjectif « *complet* » mais on peut le considérer comme inutile car le II de l'article 32 détaille le contenu de l'information à délivrer à l'internaute. Elle prévoit en revanche de **nouvelles exigences** dans les conditions définies plus haut à propos des responsables de traitement (information spécifique, accessible et permanente). En outre, les responsables de traitement ne devront pas seulement informer les utilisateurs de la **finalité** des cookies – ce que prévoit aujourd'hui l'article 32 précité - mais également de la **nature** des informations stockées ainsi que des personnes ou catégories de personnes habilitées à avoir accès à ces informations. La grande majorité des personnes entendues par votre rapporteur ont salué l'ensemble des dispositions tendant à renforcer l'obligation d'information en matière de « cookies ».

D'autre part, l'article 6 du texte proposé impose le **consentement** de l'utilisateur avant tout stockage de « cookies » sur son ordinateur.

Pour prendre la mesure de la portée de cette disposition, rappelons que les « cookies » sont de petits fichiers d'une centaine d'octets que le navigateur utilisé par l'internaute (Internet Explorer, Opéra…) installe sur le disque dur de ce dernier à la demande du site consulté. Créés en 1994 par des ingénieurs de Netscape, les « cookies » sont également appelés « mouchards électroniques » ou « témoins de connexion ». Leur objet est de permettre au site qui les a envoyés de « reconnaître » l'internaute en stockant un certain nombre d'informations : adresse IP, système d'exploitation et navigateur utilisés, pages consultées, nombre de visites du site…. En cela, les « cookies » permettent de **faciliter la navigation**, en mémorisant un certain nombre d'informations que l'internaute n'aura pas à ressaisir ultérieurement (par exemple, un cookie permettra à un internaute faisant ses achats en ligne de conserver en mémoire les produits placés dans le panier virtuel et de les présenter sur la facture finale). Toutefois, les « cookies » permettent également au fournisseur de contenu ou à la régie publicitaire de conserver en mémoire un **grand nombre d'informations relatives aux habitudes de navigation de l'internaute,** leur offrant ainsi la possibilité de lui proposer des publicités conformes à ses préférences (telles qu'elles auront été déduites des informations collectées).

On peut donc distinguer deux formes de « cookies » : les « **cookies » techniques**, dits « de session » strictement nécessaires à la navigation, comme dans le cas précité du « panier virtuel » et les « **cookies » comportementaux** qui comprennent des informations sur les habitudes de navigation de l'internaute.

Bien que le terme « cookies » n'apparaisse pas dans la loi « informatique et libertés », son article 32, en son paragraphe II, vise tous les outils qui ont pour effet d'inscrire ou d'accéder à des informations stockées sur l'ordinateur d'un utilisateur : il est admis que cette définition renvoie explicitement aux « cookies ». Ce même article dispose que l'internaute doit être informé de « *manière claire et complète* » de la finalité des « cookies » ainsi que des **moyens pour s'y opposer**. Seuls échappent à cette obligation d'information les « cookies » techniques. Les moyens actuels pour s'y opposer sont les suivants : paramétrer son navigateur Internet de manière appropriée soit pour refuser *a priori* tous les « cookies » comportementaux soit pour les effacer *a posteriori* du disque dur.

La proposition de loi opère **une évolution profonde** en passant d'une logique **d'opposition dite « d'opt-out »** à une **logique de consentement dite d' « opt-in ».** Il est en effet très différent d'avoir un droit de refus des « cookies » ou d'avoir un droit au consentement. Dans le premier cas, le silence de l'utilisateur vaut acceptation ; dans le second, il vaut refus.

Votre commission **a adopté** deux amendements tendant principalement à :

- remplacer la formule « *avant tout traitement de données* » par « *dès la collecte de données* » afin que l'information obligatoire du responsable de traitement soit bien comprise comme ne devant être délivrée qu'en cas de traitement effectif de données personnelles, et non, par exemple, dans le cas d'une simple demande de renseignement général (alinéa 2) ;

- assouplir l'obligation d'information concernant la durée de conservation des données en prévoyant l'information sur les seuls « critères déterminant la durée de conservation des données ». Un responsable de traitement ne serait ainsi pas tenu de communiquer une durée sous forme d'un chiffre précis (5 ans, 10 ans…) mais pourrait, par exemple, faire référence à d'autres notions telles que la durée du contrat, les délais de prescription, les délais légaux de conservation des données en fonction des usages : ainsi la SACEM a-t-elle l'obligation de conserver certaines données 101 ans… ;

- modifier les alinéas 10 et 11 afin de clarifier que la personne objet du traitement doit être informée des coordonnées du service auprès duquel elle peut exercer ses droits d'accès, de rectification et de suppression, même si le responsable de traitement ne dispose pas d'un site Internet ; dans ce cas, le responsable de traitement devra, en outre, indiquer les modalités d'exercice de ces droits par voie électronique après identification. A cet égard, votre rapporteur s'est longuement interrogé sur l'opportunité de remplacer le terme « identification », qui figure dans la proposition de loi, par celui

d' « authentification ». En effet, ce dernier terme suppose une preuve d'identité plus forte que la simple identification par un identifiant (ou « log-in ») et un mot de passe. Dans un premier temps, votre rapporteur avait jugé préférable de prévoir une **obligation d'authentification**, dans le souci d'éviter des usurpations d'identité numérique qui peuvent se produire, par exemple, en cas de conflits familiaux. Toutefois, il a été convaincu au fil des auditions, d'une part, que l'authentification pourrait être comprise comme interdisant la possibilité, ouverte aujourd'hui par l'article 92 du décret précité de 2005, d'exercer ces droits d'accès, de rectification et de suppression par **voie postale** en joignant à la demande une photocopie de la pièce d'identité, d'autre part, que le terme « identification » était suffisamment large pour que le décret d'application de la loi « informatique et liberté » soit modifié pour prévoir une identification plus forte, quand, par exemple, la carte nationale d'identité électronique sera mise en place ;

- clarifier, à l'alinéa 14, que l'adjectif « spécifique » renvoie à une rubrique dédiée, comme le souligne d'ailleurs l'exposé des motifs de la proposition de lois ;

- préciser que l'information sur les « cookies » devra être **globale** (alinéa 16) afin d'éviter une fastidieuse information au cas par cas ;

- préciser que l'utilisateur **doit être en mesure d'exprimer son choix**, quel qu'il soit, en matière de « cookies », **avant toute introduction** sur son disque dur de tels « mouchards électroniques ». Pour votre rapporteur, ce choix passe notamment par le **paramétrage approprié du navigateur Internet**.

Ces deux derniers points méritent que l'on s'y arrête.

Lors de leur audition, les auteurs de la proposition de loi ont expliqué que le basculement refus-consentement évoqué plus haut n'était qu'une transposition fidèle de la directive 2009/136/CE du 18 décembre 2009 modifiant la directive 2002/58/CE « Vie privée et Communications Electroniques » du 12 juillet 2002. Tel qu'il est désormais rédigé, l'article 5-3 de cette dernière directive prévoit que *« les États membres garantissent que le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur* ***ait donné son accord*** *après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement ».*

Précisons que les Etats-membres ont jusqu'au 25 mai 2011 pour transposer cette directive.

De nombreuses personnes entendues par votre rapporteur ont fait valoir que la transposition proposée était **contraire à l'esprit, voire à la lettre même de la nouvelle directive,** qui doit être interprétée à la lumière du considérant 66 qui révèle l'intention du législateur communautaire.

Les arguments suivants ont été avancés :

- le considérant 66 vise certes « l'accord de l'utilisateur », mais également, à deux reprises, « **le droit de refus** » ;

- ni le nouvel article 5-3 de la directive « Vie privée et Communications Electroniques » ni le considérant 66 ne prévoient que cet accord doit être **préalable** à l'introduction de « cookies » dans l'ordinateur de l'internaute, le terme « préalable » ayant disparu au cours des discussions à Bruxelles ;

- une déclaration commune signée le 19 novembre 2009 par 13 Etats membres (l'Autriche, la Belgique, l'Estonie, la Finlande, l'Allemagne, l'Irlande, la Lettonie, Malte, la Pologne, la Roumanie, la Slovaquie, l'Espagne et le Royaume-Uni) a interprété le nouvel article 5-3 de la directive comme ne remettant pas en cause *« le droit de refus actuel en matière de cookies* ». Mme Nathalie Kosciusko-Morizet, secrétaire d'Etat chargée de la Prospective et du Développement de l'Economie Numérique, a, quant à elle, fait savoir à votre rapporteur que *« la France n'interprétait pas l'article 5 de la nouvelle directive comme la création d'une nouvelle obligation, mais bien comme la réaffirmation du droit de l'internaute à refuser les cookies »,* et que *« cette interprétation a semblé assez évidente à la France pour quelle ne se joigne pas à la déclaration commune ».*

Cette question **juridique** – le législateur communautaire a-t-il entendu passer d'une logique d'opposition à une logique de consentement ? – est d'autant plus importante qu'elle est au cœur **d'enjeux économiques considérables.**

Les représentants des professionnels de la publicité en ligne entendus par votre rapporteur ont ainsi souligné que l'introduction en droit français du consentement préalable en matière de « cookies » serait doublement préjudiciable :

- elle serait « *catastrophique pour le commerce électronique* » et provoquerait « *un effondrement des revenus publicitaires* », qui constituent des « *sources vitales de revenus pour nombre d'éditeurs de sites* ». Elle marquerait « *la fin de la publicité ciblée* », « *un coup fatal à la presse en ligne, aux sites de contenus, au e-commerce* » et conduirait la France à perdre des activités et des emplois au profit d'Etats dans lesquels la législation est moins contraignante ;

- elle affecterait aussi les internautes eux-mêmes dans leur pratique d'Internet. Adopter le principe de l'Opt-in serait une entrave à la navigation fluide et rapide des internautes, *« ces derniers étant obligés de réitérer continuellement leur souhait d'accepter ou de refuser les cookies pour chaque site, voire chaque page web, consulté ».* En pratique, ils se verraient contraints d'interrompre leur navigation pour cliquer sur des fenêtres (ou « pop-up ») d'acceptation sur leur écran. Face aux demandes permanentes envahissant leur écran et à l'accès ralenti aux services en ligne, *« ces internautes finiraient très vite par exprimer leur mécontentement »,* voire, *« pour nombre d'entre eux, à abandonner purement et simplement le média Internet ».*

Face à ces remarques, votre rapporteur souligne, en premier lieu, qu'il est essentiel, comme le fait la proposition de loi, d'améliorer **l'information des internautes sur les « cookies » comportementaux.** Une meilleure connaissance du fonctionnement et des finalités de ces témoins de connexion ne pourra que conforter l'objectif, poursuivi par les auteurs de la proposition de loi, de rendre les individus acteurs de leur propre protection. Une information spécifique, claire, accessible, permanente garantit un choix éclairé en fonction du bilan avantages/inconvénients ressenti en matière de « cookies ».

En second lieu, votre rapporteur considère qu'un accord ou un consentement sont nécessairement **préalables**, même si la directive n'a *in fine* pas retenu cette précision.

Enfin, il admet que, tel qu'il figure dans la proposition de loi, le principe de l'Opt-in risquerait de contrarier de manière excessive le développement du **commerce en ligne** ainsi que la **navigation** des internautes, ce qui ne pouvait pas être l'intention du législateur communautaire.

En conséquence, votre rapporteur interprète la nouvelle norme communautaire comme :

- la consécration juridique des dernières évolutions techniques des navigateurs, évolutions qui consistent à offrir aux internautes de nombreuses possibilités de **paramétrage** en matière de « cookies » ;

- l'obligation pour les responsables de traitement, c'est-à-dire les annonceurs en ligne, et, à travers eux, les sites Internet qui les accueille, **d'informer très clairement** les internautes de ces possibilités de réglage et de les expliciter.

En conséquence, votre rapporteur a acquis la conviction que la directive n'a pas tranché le débat « opt in »/« opt out »[1] mais qu'elle a en revanche mis l'accent sur la nécessité de permettre à l'utilisateur d'exprimer un **choix préalable et éclairé en matière de « cookies ».**

Tel est le sens de la modification adoptée par votre commission.

Cette lecture du nouvel article 5-3 de la directive paraît conforme au considérant 66 qui prévoit que les méthodes retenues pour informer l'utilisateur et permettre son accord *« devraient être les plus conviviales possibles »* et que cet accord peut s'exprimer techniquement *« par le paramétrage du navigateur »* (Internet Explorer, Opéra…). Pour votre rapporteur, le navigateur paraît bien l'outil approprié pour permettre à l'utilisateur d'exprimer **un choix *a priori*** en matière de « cookies », sans remettre en cause la fluidité de la navigation sur Internet.

Il appartiendra à l'avenir aux représentants des utilisateurs, des sites Internet et des éditeurs de navigateurs de **déterminer ensemble les modalités**

---

[1] *C'est-à-dire, comme indiqué précédemment, que la directive n'a pas tranché la question de savoir si la non-intervention de l'utilisateur vaut refus ou acceptation.*

précises de ce paramétrage : un réglage par défaut est-il proposé à l'internaute au moment de l'installation ou de la mise à jour du navigateur ? Si oui, lequel ? Est-il facile de le modifier ? Est-on obligé de faire un choix global en matière de « cookies » (acceptation ou refus en bloc) ou peut-on gérer des préférences en fonction des caractéristiques des « cookies » qui sont généralement différentes d'un site à l'autre ?

On pourrait imaginer que les navigateurs qui proposent à l'utilisateur un paramétrage par défaut protecteur des données ou, à tout le moins, offrent des possibilités de contrôle fin en matière de « cookies », reçoivent, à l'avenir, un **label « protection des données »**.

Rappelons, en effet, que le rapport d'information des auteurs de la proposition de loi plaide pour la création de labels identifiant et valorisant des logiciels, applications et systèmes offrant des **garanties renforcées** en matière de protection des données personnelles. Le rapport regrette l'absence d'information relative au niveau de protection offert par les différents produits ou procédures proposés sur le marché en matière de droit à la vie privée.

Cette lacune contraste avec l'information délivrée aux consommateurs dans de nombreux domaines tels que la restauration, l'automobile ou l'environnement. On sait ainsi qu'un hôtel 3 étoiles offre de bonnes prestations, qu'un véhicule 5 étoiles est très résistant aux chocs et qu'un congélateur de classe A + consomme peu d'énergie.

Ces informations sur la qualité des produits semblent donner **entière satisfaction aux consommateurs** et leur fournissent des **repères très utiles** pour orienter leurs achats. Ce besoin d'information est peut-être encore plus fort dans le domaine du numérique compte tenu de l'abondance des produits existants, de leur technicité et de leur caractère relativement récent. C'est pourquoi, conclut le rapport sur ce point, il est *« probable qu'à prix et service égaux, un utilisateur privilégierait s'il a le choix un produit labellisé, et que même à prix plus élevé ou service moindre, il pourrait refuser une technologie intrusive au profit d'une technologie dont le label lui assure un niveau de protection supérieur. »*

Votre commission a adopté l'article 6 **ainsi modifié**.

Article 7
(art. 34 de la loi « informatique et libertés »)
Notification des failles de sécurité

Cet article tend à renforcer les obligations des responsables de traitements en matière de sécurité des données personnelles.

Une protection efficace des données personnelles contre les pertes accidentelles, les violations, les altérations ou les divulgations indues constitue un enjeu important, puisqu'elle contribue à maintenir la confiance des utilisateurs et des consommateurs de services électroniques mais aussi celle des clients des banques ou des usagers de l'administration.

Nombre de « failles de sécurité » se résument à la perte accidentelle d'un support matériel sur lequel des données personnelles sont inscrites : ainsi la perte par la première banque britannique d'un cédérom contenant des informations sur plusieurs centaines de milliers de clients ou bien la vente sur le site d'enchères eBay d'un ordinateur contenant les données bancaires d'un million de personnes.

Toutefois, il peut s'agir également des conséquences d'intrusions dans les systèmes informatiques par les réseaux. Dans ce dernier cas, la difficulté de réaliser systématiquement des attaques-tests pour tester la fiabilité des systèmes et l'évolution permanente des techniques utilisées par les pirates informatiques rend la protection plus aléatoire.

L'article 34 de la loi 6 février 1978 modifiée impose déjà aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

En dépit de ces dispositions, **le niveau général de protection des données personnelles en France n'est pas satisfaisant**, comme l'a rappelé le rapport d'information de M. Yves Détraigne et Mme Escoffier précité. Si aucune perte massive de données ou de violation majeure d'un traitement n'a eu pour le moment de fort retentissement médiatique, un tel événement est probable tant la protection des données n'est pas encore une préoccupation majeure des différents acteurs concernés. Ainsi, des précautions relativement efficaces telles que le cryptage des données ne sont encore que rarement mises en œuvre.

S'appuyant sur ce constat, l'article 7 tend à **instaurer une obligation d'information sur les failles de sécurité**, telle qu'elle existe par exemple dans la majorité des Etats américains, afin **d'inciter les responsables de traitement des données personnelles à mettre en œuvre les mesures de protection adéquates.** En effet, les conséquences pour la crédibilité d'une entreprise ou d'un organisme d'une telle information sont potentiellement importantes et peuvent donc l'amener à renforcer ses procédures de sécurité.

Or, dans le cadre de la réforme du paquet « télécom », la commission européenne a présenté, le 13 novembre 2007, trois propositions de texte dont une proposition de directive modifiant la directive 2002/58/CE. Le (3) de l'article 2 de cette proposition tend à obliger les responsables de traitements, « *en cas de violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles* », à avertir l'autorité administrative compétente et l'abonné concerné.

Compte tenu du champ de la directive « vie privée et communications électroniques », cette obligation de notification ne concernerait que les fournisseurs de services de communications électroniques accessibles au public, tels que les opérateurs mobiles ou les FAI. Toutefois, les considérants

de la directive préconisent l'extension de cette procédure à l'ensemble des secteurs, en soulignant que « *l'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs* ».

Les auteurs de la proposition de loi ont ainsi estimé que cette obligation pouvait utilement être étendue à l'ensemble des responsables de traitements de données personnelles. Cette extension conduit par ailleurs à écarter l'hypothèse d'une compétence de l'Autorité de régulation des communications électroniques et des postes (ARCEP) en la matière, au profit de la compétence de la CNIL.

La présente proposition tend ainsi d'une part à préciser la nature des atteintes qui peuvent être portées à un traitement de données personnelles et d'autre part à prévoir que, si une telle atteinte a lieu, le responsable du traitement avertit la CNIL qui peut elle-même, dans le cas où cette atteinte est de nature à affecter les données à caractère personnel d'une ou plusieurs personnes physiques, exiger du responsable de traitement qu'il avertisse ces personnes.

La position de votre commission

Tout en validant l'essentiel de cet article, votre commission a souhaité renforcer le rôle du correspondant informatique et libertés (que l'article 3 de la proposition de loi tend à rendre obligatoire lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel qui relève du régime d'autorisation ou pour lequel plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre). Elle a ainsi proposé un amendement tendant à prévoir que, **en cas de violation d'un traitement de données à caractère personnel, le responsable de traitement a l'obligation d'avertir le correspondant informatique et liberté**, qui avertira lui-même la CNIL. Par ailleurs, dans le cas où cette violation aurait affecté des données personnelles d'une ou plusieurs personnes physiques, le responsable de traitement devrait en informer ces personnes.

Par cohérence avec le premier paragraphe du texte proposé et afin de ne viser que les failles de sécurité proprement dites, le vocable d' « atteinte » de la proposition de loi serait remplacé par celui de « violation », ce qui permet de ne pas viser les autres atteintes telles que, par exemple, la conservation d'une donnée au-delà de la durée maximale autorisée, qui sont déjà couvertes par la loi.

Le terme de « notification » serait par ailleurs remplacé par celui plus général d' « information » afin que la violation de données puisse être portée à la connaissance des personnes concernées par tout moyen que précisera le décret en conseil d'Etat d'application (email, courrier, publication dans la presse, etc.), au lieu du seul envoi personnalisé avec accusé de réception, comme le terme de « notification » tendrait à l'imposer.

Enfin, votre commission a adopté un amendement prévoyant que l'ensemble de ces obligations d'information ne s'appliquent pas aux fichiers de police. En effet, il ne paraît pas envisageable, par exemple, d'informer des personnes inscrites dans un fichier de renseignement que des données les concernant ont été perdues.

Votre commission a adopté l'article 7 **ainsi rédigé.**

Article 8
(art. 38 de la loi « informatique et libertés »)
Droit d'opposition à un traitement

L'article 8 de la proposition de loi **facilite l'exercice du droit d'opposition**. Il substitue au terme « opposition », mal compris, celui, plus explicite, de « suppression » et dispose que ce droit de suppression s'exerce « sans frais ». En outre, il réécrit l'article 38 de la loi « informatique et libertés » relatif au droit d'opposition pour bien distinguer le droit d'opposition commerciale, qui s'exerce avant tout traitement ou, en cas de collecte indirecte, avant toute communication des données, et le **droit de suppression** des données qui s'exerce, par définition, après.

Insistons sur le fait que le droit d'opposition prévu au premier alinéa de l'actuel article 38 de la loi « informatique et libertés » est **au cœur du droit à l'oubli numérique :** il permet à chaque individu, pour des motifs légitimes (*cf infra*), de demander à retirer d'Internet des données personnelles, qu'elles aient été livrées par la personne elle-même ou par des tiers.

En effet, la CNIL, par deux délibérations en date du 22 novembre 2005, a considéré que les sites Internet, y compris ceux réalisés par des particuliers, constituent des **traitements automatisés de données** : *« La diffusion ou la collecte d'une donnée à caractère personnel à partir d'un site web constitue un traitement automatisé de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée, notamment celles relatives aux formalités préalables ».*

Ce point a également été **confirmé** par la jurisprudence :

- à propos d'un site référençant des notaires (CA Bourges, 11 avril 2007, Ligue européenne de défense des victimes de notaires c/ Ministère public) ;

- à propos d'un site « antisectes » (TGI Villefranche sur Saône, 18 février 2003, Ministère public c/ X confirmé par CA Lyon, 25 février 2004) ;

- à propos du site de notation des professeurs (CA Paris, 25 juin 2008, note2be c/ SNES) ;

- à propos d'un forum de discussion, (TGI Paris, réf., 14 avril 2008, X c/ Google France).

Le droit d'opposition permet ainsi à un individu d'effacer, s'il le souhaite, son **passé numérique.**

Pour votre commission, le droit d'opposition couvre toutes les hypothèses, y compris la suppression **des liens persistants des moteurs de recherche.** En effet, votre rapporteur a pu constater que même quand les pages Internet ont disparu, les moteurs de recherche continuent à donner en quelques mots l'information contenue dans ces pages. Il importe donc que les moteurs de recherche améliorent leur système de désindexation automatique des pages Internet supprimées et qu'à défaut ils fassent droit rapidement aux demandes d'opposition qui leur sont adressées.

Signalons également que la suppression des données peut passer par leur **effacement** ou leur **anonymisation.** Dans ce dernier cas, l'anonymisation doit être **irréversible**. En avril 2008, le G29[1], dans son rapport sur les moteurs de recherche, soulignait justement que *« lorsque l'anonymisation est préférée à la suppression des données, les méthodes utilisées devraient être étudiées soigneusement et exécutées jusqu'au bout. Cela peut impliquer la suppression de portions de l'historique de recherche, afin d'éviter la possibilité d'identification indirecte de l'utilisateur qui a effectué les recherches en question. »*

La position de votre commission

Outre un amendement rédactionnel, votre commission a adopté **deux amendements.**

Le premier modifie l'alinéa 2 de l'article 8 afin de remplacer la formule « avant tout traitement de données » par « dès la collecte de données » afin de clarifier que la possibilité d'exercer son droit d'opposition commerciale se fait dès la collecte de données, et non avant celle-ci ;

Le second – plus important - réécrit l'alinéa 3 de l'article 8 afin de **clarifier l'exercice du droit de suppression.**

Actuellement, ce droit ne peut être exercé qu'à trois conditions cumulatives : que le demandeur invoque des « motifs légitimes », que le traitement ne réponde pas à une obligation légale et que l'exercice de ce droit

[1] *Le G29 est un groupe de travail européen, créé par l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation, rassemblant les représentants de vingt-sept autorités indépendantes de protection des données nationales.*

n'ait pas été écarté par une disposition expresse de l'acte autorisant le traitement.

Votre rapporteur a vainement cherché à préciser la notion de **« motifs légitimes ».** Transposée littéralement en 2004 de la directive de 1995, elle n'a pas été explicitée au cours des débats parlementaires et n'a fait l'objet, semble-t-il, que d'une **jurisprudence très limitée**. Tout au plus trouve-t-on un arrêt de la Cour d'appel de Besançon qui a déclaré légitime l'opposition formulée par une personne à la diffusion sur un site internet de données que la juridiction a reconnu comme « outrageantes ». Elle a ainsi ordonné le retrait de ces données, sous astreinte de deux cents euros par jour de retard[1]. On peut donc penser que les motifs d'exercice du droit à l'oubli sont légitimes quand le responsable de traitement a porté atteinte à **un droit fondamental de l'individu** tel que la présomption d'innocence, le droit à la vie privée, à l'honneur, la considération… Votre rapporteur n'ayant pu trouver une rédaction de nature à ne créer aucune difficulté d'interprétation, votre commission a jugé plus prudent de ne pas revenir sur la notion actuelle de « motifs légitimes » mais de mieux encadrer son expression.

Votre commission a ainsi souhaité préciser que le droit à la suppression des données ne pourrait être exercé dans quatre **nouveaux cas de figure :**

- lorsque les données sont nécessaires à la finalité du traitement : il s'agit d'éviter que les données soient effacées dans le cas, par exemple, où un bien est toujours sous garantie ou n'a pas été entièrement réglé par le consommateur ;

- lorsque le traitement est nécessaire pour la sauvegarde, la constatation, l'exercice ou la défense d'un droit ;

- lorsque le droit de suppression porte atteinte à une liberté publique garantie par la loi : il s'agit essentiellement de protéger la liberté de la presse ;

- lorsque les données constituent un fait historique : le droit de suppression ne peut avoir pour objet ou pour effet de réécrire ou de falsifier l'histoire.

Votre commission a adopté l'article 8 **ainsi modifié**.

[1] *CA Besançon, 31 janv. 2007 : D. 2007, p. 2771, obs. Lepage*

Article 9
(art. 39 de la loi « informatique et libertés »)
Obligation pour le responsable de traitement d'indiquer l'origine de la donnée

L'article 9, outre des coordinations avec l'article 32 de la loi « informatique et libertés », précise l'obligation pour le responsable du traitement interrogé au titre du droit d'accès **d'indiquer l'origine de la donnée**. Cette indication permet en effet à la personne objet du traitement de remonter jusqu'au responsable du traitement détenteur du fichier d'origine et d'exercer éventuellement auprès de lui ses droits d'accès, de rectification ou d'opposition. Or seule est actuellement prévue la communication des **informations disponibles** quant à l'origine des données personnelles, disponibilité qui, en pratique, est rare, les opérateurs n'ayant, semble-t-il, pas mis en place les outils adéquats.

Au cours des auditions, votre rapporteur a été sensible au fait qu'il était extrêmement difficile pour les responsables de traitement de connaître **l'origine précise** des données qu'ils détiennent. En effet, une fois acquises, les données sont souvent traitées à nouveau en fonction de critères complexes.

Votre commission a donc souhaité revenir à la rédaction actuelle « information **disponible** quant à l'origine des données » tout en clarifiant un point : même si l'origine des données n'est pas connue, le responsable de traitement ne peut échapper à son obligation de communiquer le **contenu précis des données** qu'il détient lorsqu'il est interrogé au titre du droit d'accès. Votre commission a donc adopté un amendement en ce sens.

Elle a adopté l'article 9 **ainsi modifié**.

Article 9 bis (nouveau)
(art. 44 de la loi « informatique et libertés »)
Contrôles inopinés de la CNIL

A l'initiative du Gouvernement[1], votre commission a adopté un article 9 *bis* afin de donner à la CNIL la possibilité de demander au juge des libertés et de la détention l'autorisation préalable d'effectuer une **visite inopinée** *« lorsque l'urgence, la gravité des faits justifiant le contrôle ou le risque de destruction ou de dissimulation de documents l'exigent ».*

En effet, tel qu'il est actuellement rédigé, l'article 44 de la loi « informatique et libertés » dispose que le responsable des lieux **peut s'opposer à une visite de la Commission**. Dans ce cas, la visite ne peut se dérouler qu'avec l'autorisation d'un président du tribunal de grande instance territorialement compétent ou du juge délégué par lui. Ce magistrat est saisi à la requête du Président de la Commission.

---

[1] *Notre collègue M. Alex Türk a présenté un amendement similaire qui a été retiré au profit de celui du Gouvernement qui prévoyait un régime juridique plus complet.*

Le Conseil d'Etat a d'ailleurs récemment **conforté ce principe** en estimant, sur le fondement de l'article 8 de la Convention européenne des droits de l'homme relatif à l'inviolabilité du domicile, que les responsables des locaux dans lesquels se déroule un contrôle de la CNIL doivent même être *« informés de leur droit à s'opposer à ces visites »* (arrêt du 6 novembre 2009 du Conseil d'Etat, Société Inter Confort, req. N° 304300).

Or, ce droit d'opposition est de nature à **restreindre considérablement la portée et l'efficacité des contrôles de la CNIL** puisque l'organisme contrôlé pourra bénéficier du temps nécessaire à l'obtention d'une ordonnance judiciaire pour effacer - ou dissimuler - des données informatiques qui seraient contraires à la loi.

En permettant au juge des libertés et de la détention, gardien des libertés individuelles, d'autoriser la CNIL à effectuer un **contrôle inopiné**, l'amendement renforce l'efficacité de la CNIL dans sa mission de contrôle **sans porter atteinte aux droits du responsable des lieux visités**. En effet, conformément à l'article 44 précité, la visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée et celui-ci peut décider l'arrêt ou la suspension de la visite à tout moment.

Votre commission a adopté l'article 9 *bis* **ainsi rédigé.**

Article 10
(art. 45 de la loi « informatique et libertés »)
Publicité des audiences de la formation restreinte de la CNIL

L'article 10 modifie l'article 45 de la loi « informatique et libertés » afin de rendre systématiquement **publiques** les audiences de la formation restreinte de la CNIL alors que les audiences ne sont aujourd'hui publiques qu'à la demande des parties.

La proposition de loi entend tirer les conséquences d'une ordonnance du Conseil d'État du 19 février 2008 qui considère que la Commission, *« eu égard à sa nature, à sa composition et à ses attributions »*, **peut être qualifiée de tribunal** au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[1]. Or, cet article dispose que *« toute personne a droit à ce que sa cause soit entendue (...) **publiquement** »*.

Toutefois, votre commission estime que la CNIL ne peut être regardée comme un tribunal **à l'égal des juridictions « classiques »** et n'a donc pas à se conformer à toutes les exigences du procès équitable. Dans un cas proche, le Conseil d'Etat, dans un arrêt du 4 avril 1999 à propos du pouvoir de sanction reconnu au Conseil du marché à terme, n'en a pas jugé autrement[2]. La haute juridiction indique dans cet arrêt que la publicité des audiences de ce Conseil n'est pas obligatoire dès lors que les personnes

[1] *CE référé, 19-02-2008, n° 311974, SOCIETE PROFIL FRANCE*
[2] *CE, 04-04-1999, n° 182421 Groupement d'Intérêt Économique (G.I.E.) ODDO-FUTURES*

sanctionnées peuvent saisir le Conseil d'Etat d'un recours de pleine juridiction examiné, lui, en séance publique conformément à l'article 6-1 précité.

Le même raisonnement pourrait être tenu pour la CNIL dont les sanctions sont susceptibles de recours devant le Conseil d'Etat aux termes de l'article 46 de la loi « informatique et libertés ».

En conséquence, votre commission a **supprimé** l'article 10.

Article 11
(art. 46 de la loi « informatique et libertés »)
Publicité des sanctions de la CNIL

Cet article rend **plus aisée** la publicité des sanctions les plus graves prononcées par la CNIL, publicité aujourd'hui conditionnée à la *« mauvaise foi du responsable du traitement »*. L'article supprime cette condition.

Aux termes de l'actuel 46 de la loi « informatique et libertés », la CNIL peut rendre publics les avertissements qu'elle prononce en vertu de l'article 45 de la même loi. Pour les autres sanctions, à savoir les mises en demeure, les sanctions pécuniaires et les injonctions de cesser un traitement, elle ne peut ordonner leur insertion dans des publication, journaux et supports qu'elle désigne, qu'en **cas de mauvaise foi** du responsable de traitement, mauvaise foi qu'il n'est pas toujours facile de démontrer comme l'a indiqué M. Alex Türk à votre rapporteur lors de son audition.

En conséquence, l'article supprime opportunément cette condition.

Votre commission a adopté l'article 11 **sans modification**.

Article 12
(art. 47 de la loi « informatique et libertés »)
Sanctions pécuniaires susceptibles d'être prononcées par la CNIL

Cet article tend à **élever le montant des sanctions pécuniaires susceptibles d'être prononcées par la CNIL** en cas de manquement aux obligations prévues par la loi « informatique et libertés » du 6 janvier 1978.

L'article 45 de cette loi dispose que la CNIL peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la loi « informatique et libertés ». Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui est adressée, la CNIL peut prononcer à son encontre, après une procédure contradictoire :

- une sanction pécuniaire, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;

- une injonction de cesser le traitement, lorsque celui-ci a fait l'objet d'une déclaration, ou un retrait de l'autorisation, lorsque le traitement a été préalablement autorisé par la CNIL.

En application des dispositions prévues à l'article 47 de cette même loi, le montant de la sanction pécuniaire doit être proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, ce montant ne peut excéder 150.000 euros. En cas de manquement réitéré dans un délai de cinq ans, ce montant peut être porté à 300.000 euros ou, s'agissant d'une entreprise, à 5% du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300.000 euros.

Dans leur rapport d'information précité, nos collègues Anne-Marie Escoffier et Yves Détraigne avaient souligné que ce plafonnement légal des sanctions susceptibles d'être prononcées par la CNIL s'accompagnait **d'une pratique empreinte d'une certaine timidité**. Ils avaient relevé qu'en 2008, la CNIL avait prononcé onze sanctions pour un montant total de 137.100 euros. Par comparaison, l'agence espagnole de protection des données a prononcé, cette même année, 630 sanctions pour un total de 22,6 millions d'euros.

Dans le but de **dissuader davantage les manquements aux obligations posées par la loi « informatique et libertés » du 6 janvier 1978**, l'article 12 de la proposition de loi tend à doubler le montant des sanctions pécuniaires susceptibles d'être prononcées par la CNIL :

- un premier manquement pourrait être sanctionné de 300.000 euros ;

- en cas de manquement réitéré dans un délai de cinq ans, ce montant pourrait atteindre 600.000 euros, ou, s'agissant d'une entreprise, 5% du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 600.000 euros.

Votre commission **approuve cette démarche** qui constituera un signal fort adressé aux responsables de traitements et incitera la CNIL à sanctionner plus sévèrement les manquements caractérisés aux dispositions portant sur la protection des données personnelles.

Votre commission a adopté l'article 12 **sans modification**.

Article 13
(art. 11, 50, 51, 52, 52-1 [nouveau] et 52-2 [nouveau]
de la loi « informatique et libertés »)
Dispositions relatives aux actions juridictionnelles

Cet article tend à renforcer les possibilités d'actions juridictionnelles des individus et de la CNIL en cas de violation des dispositions de la loi « informatique et libertés » par un responsable de traitement.

A l'heure actuelle, les infractions aux dispositions de la loi « informatique et libertés » sont réprimées par les articles 226-16 à 226-24 du code pénal (voir annexe).

En outre, l'article 51 de la loi du 6 janvier 1978 définit un **délit d'entrave à l'action de la CNIL**, puni d'un an d'emprisonnement et de 15.000 euros d'amende.

Enfin, l'article 52 de la loi du 6 janvier 1978 organise les modalités d'intervention de la CNIL dans les procédures pénales relatives aux infractions précitées :

- le procureur de la République est tenu d'aviser le président de la CNIL des poursuites engagées sur le fondement des dispositions précitées et, le cas échéant, des suites qui leur sont données. Il l'informe également de la date et de l'objet de l'audience de jugement ;

- en outre, la juridiction d'instruction ou de jugement peut appeler le président de la CNIL (ou son représentant) à déposer ses observations ou à les développer oralement à l'audience.

L'article 13 de la proposition de loi tend à compléter et à renforcer ce dispositif.

Tout d'abord, il rappelle que, conformément aux dispositions de l'article 40 du code de procédure pénale, la CNIL est tenue d'informer sans délai le procureur de la République des infractions dont elle a connaissance[1].

En outre, s'agissant des recours portés devant les juridictions civiles, cet article insère dans la loi « informatique et libertés » **un nouvel article 52-1** ouvrant à toute personne lésée par un manquement aux dispositions de cette loi la possibilité de saisir, outre l'une des juridictions territorialement compétentes en vertu du code de procédure civile, la juridiction du lieu où il demeurait au moment de la conclusion du contrat ou de la survenance du fait dommageable.

A l'heure actuelle, l'article 42 du code de procédure civile dispose que, sauf disposition contraire, la juridiction territorialement compétente est celle où demeure le défendeur. Néanmoins, l'article 46 de ce même code permet au demandeur de saisir à son choix, outre la juridiction du lieu où demeure le défendeur :

- en matière contractuelle, la juridiction du lieu de la livraison effective de la chose ou du lieu de l'exécution de la prestation de service ;

- en matière délictuelle, la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi ;

- en matière mixte, la juridiction du lieu où est situé l'immeuble ;

- enfin, en matière d'aliments ou de contribution aux charges du mariage, la juridiction du lieu où demeure le créancier.

---

[1] *Le second alinéa de l'article 40 du code de procédure pénale dispose que « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».*

En matière délictuelle, la détermination de la juridiction du lieu du fait dommageable a été rendue **plus complexe par l'essor d'Internet**. En effet, en matière de diffamation, de contrefaçon ou de publicité illicite par Internet, par exemple, le dommage est potentiellement réalisé en tous lieux comportant un point d'accès au réseau. Ce constat a conduit la jurisprudence à estimer que, dans ce cas, le dommage est subi **en tous lieux** où les exemplaires contrefaits[1] ou les images télévisées interdites[2] ont été diffusées. Ces solutions, qui limitent considérablement la portée des règles de compétence territoriale, permettent de faciliter la répression de ces faits.

La rédaction retenue par la proposition de loi pour le nouvel article 52-1 s'inspire de l'article L. 141-5 du code de la consommation, introduit par le Sénat à l'occasion de l'examen de la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures. Cet article dispose que « *le consommateur peut saisir à son choix, outre l'une des juridictions territorialement compétentes en vertu du code de procédure civile, la juridiction du lieu où il demeurait au moment de la conclusion du contrat ou de la survenance du fait dommageable* ».

Votre commission approuve ces dispositions qui permettront de faciliter l'accès au juge civil des individus qui s'estiment lésés par un manquement aux dispositions de la loi « informatique et libertés ».

Enfin, l'article 13 de la proposition de loi renforce les dispositions relatives aux observations de la CNIL devant les juridictions civiles, pénales ou administratives. Un **nouvel article 52-2**, inséré dans la loi « informatique et libertés », disposerait que :

- les juridictions civiles, pénales ou administratives peuvent, d'office ou à la demande des parties, inviter la CNIL à déposer des observations écrites ou à les développer oralement à l'audience ;

- la CNIL peut elle-même déposer des observations écrites devant ces juridictions. En outre, elle serait obligatoirement entendue par ces juridictions lorsqu'elle en fait la demande.

Votre commission est favorable à ces dispositions, inspirées de celles qui ont été retenues pour la HALDE[3] et qui permettront de faciliter l'intervention de la CNIL devant l'ensemble des juridictions appelées à connaître d'affaires mettant en jeu la protection des données à caractère personnel. Comme le faisait observer Mme Marie-Anne Frison-Roche dans une étude réalisée en 2006 pour l'office parlementaire d'évaluation de la

---

[1] Voir par exemple, CA Paris, 14ème chambre, 1er mars 2000 ; TGI Nanterre, 8 décembre 1999.
[2] Cass., 2ème chambre civile, 25 octobre 1995.
[3] L'article 13 de la loi n°2004-1486 du 30 décembre 2004 portant création de la haute autorité de lutte contre les discriminations et pour l'égalité dispose que : « les juridictions civiles, pénales ou administratives peuvent, lorsqu'elles sont saisies de faits relatifs à des discriminations, d'office ou à la demande des parties, inviter la haute autorité ou son représentant à présenter des observations. La haute autorité peut elle-même demander à être entendue par ces juridictions ; dans ce cas, cette audition est de droit ».

législation[1], « *les juridictions ne sont généralement pas spécialisées, ce qui accroît la difficulté de la tâche des magistrats. C'est pourquoi il est essentiel de prévoir que les autorités administratives indépendantes peuvent, sans exception, fournir des avis à des juridictions, ou interpréter le silence des textes dans ce sens. Le fait qu'il s'agisse* ***d'avis techniques gratuits pour le service public de la justice*** *n'est pas leur moindre qualité* ».

L'attention de votre commission a toutefois été attirée sur les dispositions prévoyant que les observations écrites de la CNIL sont recevables quelle que soit la procédure applicable devant la juridiction saisie. Il lui est en effet apparu que de telles dispositions pourraient ne pas être pleinement compatibles avec **les exigences du procès équitable**. Tel serait par exemple le cas lorsque ces observations sont produites après la clôture du délai de l'instruction.

Suivant la proposition de son rapporteur, elle a adopté un **amendement** tendant à supprimer ces dispositions du texte de l'article 13.

Le II de l'article 13 de la proposition de loi procède aux coordinations rendues nécessaires par les modifications précitées. A cet effet, il modifie les dispositions de l'article 11 de la loi du 6 janvier 1978, qui porte sur les missions de la CNIL, afin de prendre en compte l'élargissement des possibilités ouvertes à la CNIL de présenter ses observations devant les juridictions.

Votre commission a adopté l'article 13 **ainsi modifié**.

Article 13 bis (nouveau)
(art. 72 de la loi « informatique et libertés »)
Application outre-mer de la loi « informatique et libertés »

A l'initiative de votre rapporteur, votre commission a adopté un article additionnel tendant à modifier l'article 72 de la loi « informatique et libertés » afin de prévoir l'application de cette dernière à tout le territoire de la République, y compris outre-mer.

Dans sa rédaction actuelle, l'article 72 énumère les collectivités d'outre-mer qui se trouvent dans le champ de la loi. Il est apparu préférable à votre commission de prévoir une **formule générale** : « La présente loi est applicable sur l'ensemble du territoire de la République française. »

L'énumération n'apparaît pas, en effet, comme la formule la plus adaptée et la plus pérenne. A titre d'exemple, il n'est aujourd'hui plus nécessaire de prévoir expressément, comme le fait l'article 72 précité, l'application de la loi « informatique et libertés » à Mayotte dans la mesure où l'article L. 6113-1 du code général des collectivités territoriales définit un

---

[1] *Voir cette étude dans le rapport de notre collègue Patrice Gélard, « les autorités administratives indépendances : évaluation d'un objet juridique non identifié », tome II : annexes, Office parlementaire d'évaluation de la législation, rapport n° 404 (2005-2006).*

régime d'application **de plein droit** dans ce domaine dès lors qu'il ne figure pas parmi les compétences propres de cette collectivité.

Votre commission a adopté l'article 13 *bis* **ainsi rédigé**.

Article 14

Entrée en vigueur de la loi

L'article 14 prévoit l'entrée en vigueur de la loi six mois après sa publication afin de laisser le temps aux entreprises et administrations de s'adapter aux nouvelles dispositions.

Votre commission a adopté l'article 14 **sans modification**.

EXAMEN EN COMMISSION

MERCREDI 24 FÉVRIER 2010

_____

Puis la commission a examiné le rapport de M. Christian Cointat et établi le texte qu'elle propose pour la proposition de loi n° 93 (2009-2010), présentée par M. Yves Détraigne et Mme Anne-Marie Escoffier, visant à mieux garantir le droit à la vie privée à l'heure du numérique.

M. Christian Cointat, rapporteur, a rappelé que la proposition de loi de M. Yves Détraigne et Mme Anne-Marie Escoffier faisait suite au rapport d'information des mêmes auteurs, publié au nom de la commission des lois le 27 mai 2009, et traduisait plusieurs recommandations formulées dans ce rapport.

Après avoir relevé que les sujets abordés par ce texte sont sensibles et complexes, il a insisté sur la nécessité pour le législateur de trouver un équilibre entre l'accompagnement du développement des nouvelles technologies, facteur de progrès indiscutables, et un encadrement juridique destiné à combattre ses dérives, en particulier au regard de la protection des données personnelles et, plus généralement, de la vie privée, protection réclamée par les citoyens. A cet égard, il a regretté que de nombreux représentants d'entreprises et d'administrations aient, au cours de leur audition, plaidé pour le statu quo dans ce domaine.

Il a souhaité que la proposition de loi soit perçue à l'étranger comme un nouveau signal fort de la France en faveur d'un renforcement de la protection des données personnelles, à l'heure où des initiatives sont lancées pour faire évoluer le cadre juridique communautaire – et à terme international – de cette protection, trente ans après la loi « informatique et libertés » du 6 janvier 1978, texte précurseur en la matière.

Tout en souscrivant largement aux objectifs de la proposition de loi, il a souhaité la modifier afin qu'elle soit mieux comprise par les entreprises et par l'administration. Ainsi :

- sur l'article premier, il a indiqué que celui-ci complétait l'article L. 312-9 du code de l'éducation afin que l'initiation des élèves à l'usage d'Internet intègre autant les questions liées au téléchargement illégal que celles, tout aussi essentielles, de la protection des données personnelles et, plus généralement, de la vie privée. Son amendement n° 1 tend à en aménager la rédaction afin, en particulier, de prévoir que les enseignants ne doivent pas être « préalablement formés » sur la question de la protection des données mais « expérimentés en la matière ». En effet, la sensibilisation aux enjeux de la protection de la vie privée relève moins d'une discipline académique que d'une expérience et d'une appétence particulière de certains enseignants pour ce type de problématique. En conséquence, il s'est déclaré prêt à retirer son amendement au profit de celui déposé par Mme Catherine Morin-Desailly, rapporteur pour avis au nom de la commission de culture, de l'éducation et de la communication, tendant à inscrire la sensibilisation des élèves aux enjeux de la protection de la vie privée dans le cadre de l'éducation civique et non dans celui des cours consacrés aux

nouvelles technologies. Ce rattachement est tout à fait cohérent avec le rapport d'information sur la vie privée à l'heure des mémoires numériques qui estime que cette sensibilisation peut être dispensée à l'occasion des cours d'éducation civique, dès lors qu'il s'agit de transmettre des valeurs plus que des connaissances techniques ;

- il a rappelé que l'article 2 visait à clarifier le statut de l'adresse IP. En effet, cette adresse constitue, selon le rapport d'information précité, un moyen indiscutable d'identification, fût-elle indirecte, d'un internaute, au même titre qu'une adresse postale ou un numéro de téléphone. Il a souhaité modifier la rédaction de cet article afin de faire clairement apparaître que l'adresse IP ne permet pas à elle seule d'identifier un internaute et ne constitue que l'élément d'un « faisceau d'indices » permettant d'identifier une personne physique ;

- il a expliqué que l'article 3 rendait obligatoires les correspondants « informatique et libertés » (CIL) lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre. Il a approuvé le principe posé par cet article, considérant que ce correspondant ne devait pas être perçu comme « un espion » qui entrave l'action de la structure dans laquelle il est désigné, mais comme une aide, une garantie et un conseil qui permet, d'une part, la diffusion de la culture « informatique et libertés » dans les structures dans lesquelles il a été désigné, d'autre part, et symétriquement, la diffusion de la culture « administration » ou « entreprises » au sein de la Commission nationale de l'informatique et des libertés (CNIL). Il a souhaité apporter quelques aménagements à l'article 3 jugeant fondées certaines craintes dont celle que la mutualisation des CIL serait dorénavant exclue. En conséquence, il a souhaité, d'une part, préciser que la désignation obligatoire du CIL pourrait intervenir dans un cadre mutualisé, d'autre part, maintenir la possibilité de mutualisation lorsque la création du CIL n'est pas obligatoire.

En outre, il a contesté que la mise en place de CIL soit coûteuse pour les structures dans lesquelles ils seront obligatoires, entreprises comme administrations pouvant respecter cette nouvelle obligation à moyens constants.

Enfin, s'agissant du seuil de 50 salariés ayant accès à un traitement de données personnelles, il a indiqué que celui-ci constituait une incitation pour les entreprises et administrations à limiter les accès aux fichiers tout en se déclarant ouvert à des amendements visant à relever ce seuil ;

- il a rappelé que l'article 4 réservait au législateur la compétence exclusive pour autoriser les catégories de fichiers nationaux de police et pour définir les principales caractéristiques de ces catégories (services responsables, finalités et durée de conservation des informations traitées), alors que les fichiers de police peuvent actuellement être autorisés par arrêté ou, s'ils comportent des données sensibles, par décret en Conseil d'Etat. Il a souhaité s'écarter de la rédaction proposée par la proposition de loi, pour deux raisons principales :

- d'une part, la rédaction de l'article 4 pourrait être dépourvue de caractère normatif, le législateur ordinaire n'étant pas susceptible de définir pour l'avenir sa propre compétence ;

- d'autre part, l'Assemblée nationale a adopté, le 2 décembre 2009, un article 29 bis lors de la première lecture de la proposition de loi de simplification et d'amélioration de la qualité du droit, présentée par M. Jean-Luc Warsmann. Cet article modifie l'article 26 de la loi « informatique et libertés » dans un sens qui préserve un équilibre entre la garantie des droits et libertés et la souplesse nécessaire pour permettre au Gouvernement de mettre en œuvre des fichiers opérationnels dans des délais raisonnables. Le dispositif prévoit que tout fichier créé par arrêté ou par décret doit répondre à l'une des finalités qu'il énumère. A défaut, seul le législateur serait compétent.

Dans un souci de compromis, face aux objections du Gouvernement, le rapporteur s'est déclaré prêt à reprendre, sous réserve de quelques adaptations, ce dispositif qui présente l'avantage de mieux encadrer les fichiers de police au regard du droit actuel ;

- il a rappelé que l'article 6 apportait deux modifications importantes au régime juridique des « cookies ». D'une part, il renforce l'obligation d'information incombant au responsable du traitement. Tel qu'il est actuellement rédigé, l'article 32 de la loi « informatique et libertés » dispose que l'information doit être « claire et complète ». La rédaction proposée demande une information « spécifique, claire, accessible et permanente ». D'autre part, il impose le consentement de l'utilisateur avant tout stockage de « cookies » sur son ordinateur. Il a indiqué avoir cherché à assouplir ce dernier principe qui, appliqué de manière trop rigide, obligerait les internautes à réitérer trop fréquemment leur choix d'accepter ou de refuser les cookies pour chaque site, voire chaque page web, consultés. Les utilisateurs se verraient ainsi contraints en pratique d'interrompre leur navigation pour cliquer sur des fenêtres ou « pop-up » sur leur écran, ce qui, d'une part, constituerait une entrave à la navigation fluide et rapide des internautes, d'autre part, mettrait en grandes difficultés les professionnels du commerce en ligne. En conséquence, il a souhaité, d'une part, prévoir une information globale, et non au cas par cas, en matière de « cookies », d'autre part, que cette information renvoie l'utilisateur aux possibilités de paramétrage du navigateur Internet afin qu'il puisse exprimer un choix préalable, quel qu'il soit, en matière de « cookies », ce qui semble conforme aux choix récents du législateur communautaire ;

- il a rappelé que l'article 8 concernait le droit à l'oubli : il permet à chaque individu, pour des motifs légitimes, de demander à retirer d'Internet des données personnelles, qu'elles aient été livrées par la personne elle-même ou par des tiers. Il a expliqué que, n'ayant pu trouver une rédaction de nature à ne créer aucune difficulté d'interprétation, il avait jugé plus prudent de ne pas revenir sur la notion de « motifs légitimes », qui figure dans la proposition de loi tout en précisant, à l'inverse, que le droit à la suppression des données ne pourrait être exercé dans quatre nouveaux cas de figure :

- lorsque les données sont nécessaires à la finalité du traitement : il s'agit d'éviter que les données soient effacées dans le cas, par exemple, où un bien est toujours sous garantie ou n'a pas été entièrement payé par le consommateur ;

- lorsque le traitement est nécessaire à la sauvegarde, la constatation, l'exercice ou la défense d'un droit ;

- lorsque le droit de suppression porte atteinte à une liberté publique garantie par la loi : il s'agit essentiellement de protéger la liberté de la presse ;

- lorsque les données constituent un fait historique : le droit de suppression ne peut avoir pour objet ou pour effet de réécrire ou de falsifier l'histoire ;

- il a rappelé que l'article 10 rendait systématiquement publiques les audiences de la formation restreinte de la CNIL alors que les audiences ne sont aujourd'hui publiques qu'à la demande des parties. Toutefois, il a estimé que la CNIL ne pouvait être regardée comme une juridiction et qu'elle n'avait donc pas à se conformer à toutes les exigences du procès équitable. En conséquence, il s'est prononcé en faveur de la suppression de cet article.

Mme Anne-Marie Escoffier a remercié le rapporteur pour le travail accompli en tenant informés les auteurs de la proposition de loi de l'avancement de ses travaux. Elle a souligné que, face aux nouvelles menaces qui pèsent sur la protection des données, la première réponse réside dans la responsabilisation d'individus éclairés sur les enjeux pour leur propre protection.

Saluant à son tour la qualité du travail du rapporteur, M. Yves Détraigne a souligné que, si la proposition de loi pouvait apparaître comme technique, voire ésotérique, elle n'en était pas moins au cœur d'enjeux fondamentaux. Il a indiqué avoir reçu comme Mme Anne-Marie Escoffier de très nombreuses sollicitations (demandes d'entretiens, de participation à des colloques, conférences…) à la suite de la publication du rapport d'information et de la proposition de loi, car ces questions suscitent de nombreuses attentes mais aussi certaines inquiétudes. En conséquence, il a plaidé pour un dispositif équilibré qui tienne compte des différents intérêts en présence.

Mme Catherine Troendle s'est déclarée défavorable à l'obligation de désignation des CIL, jugeant préférable d'en rester au système actuel basé sur le volontariat.

M. Alain Anziani a demandé quelles conséquences juridiques s'attachaient à la qualification de l'adresse IP en donnée personnelle. Il a par ailleurs souligné que la question du droit à l'oubli ne se posait pas que sur Internet, prenant l'exemple d'une photographie qui pouvait être diffusée sur un support papier trente ans après sa réalisation. Enfin, il s'est interrogé sur l'opportunité de légiférer en matière de « cookies », les navigateurs actuels permettant tous aux utilisateurs de les refuser a priori ou de les effacer a posteriori. En revanche il est important que les navigateurs offrent un réglage fin permettant aux internautes de gérer des préférences en fonction des

caractéristiques des « cookies » qui sont généralement différentes d'un site à l'autre.

M. Pierre-Yves Collombat, rapporteur, s'est interrogé sur les moyens de lutte contre les courriels non sollicités.

Mme Virginie Klès a mis en garde contre une pratique consistant à transférer des courriels comportant « des chaines » d'adresses mails.

M. Christian Cointat, rapporteur, a indiqué :

- que l'obligation de désignation des CIL constitue une des mesures les plus importantes de la proposition de loi. Or, le principe d'indépendance du CIL n'est pas incompatible avec le statut de la fonction publique, pas plus que ne le sont, dans les ministères, les corps d'inspection, de contrôle ou de comptables publics. Enfin, il est essentiel de resserrer les liens entre la CNIL et le réseau des CIL ;

- que la clarification du statut juridique de l'adresse IP permet d'apporter à celle-ci la protection de la loi « informatique et libertés » ;

- que l'amendement qu'il propose consacre la pratique actuelle en matière de possibilités de paramétrage des navigateurs ;

- que la captation des courriels, responsables du phénomène des « spams », peut notamment résulter de la pratique des chaines décrite par Mme Virginie Klès.

Il a souligné que le droit à l'oubli devait couvrir toutes les hypothèses, y compris la suppression des liens persistants des moteurs de recherche. En effet, même quand les pages Internet ont disparu, les moteurs de recherche continuent à donner en quelques mots l'information contenue dans ces pages. Il importe donc que les moteurs de recherche améliorent leur système de désindexation automatique des pages Internet supprimées et qu'à défaut ils fassent droit rapidement aux demandes d'opposition qui leur sont adressées.

M. Jean-Jacques Hyest, président, s'est étonné que le Gouvernement semble parfois accueillir avec circonspection les initiatives parlementaires. De même, certains représentants d'entreprises qualifient ces initiatives de « sympathiques » mais vouées à ne pas être appliquées.

La commission a ensuite examiné les amendements, déposés par le rapporteur, Mme Catherine Morin-Desailly, au nom de la commission de la culture, de l'éducation et de la communication, M. Charles Gautier et les membres du groupe socialiste, apparentés et rattachés, M. Alex Türk et le Gouvernement.

A l'article premier (sensibilisation des jeunes aux enjeux de la protection de la vie privée sur Internet), le rapporteur a retiré son amendement n° 1 au bénéfice de l'amendement n° 36 de Mme Catherine Morin-Desailly, rapporteur pour avis au nom de la commission de culture, de l'éducation et de la communication, tendant à inscrire la sensibilisation des élèves aux enjeux de la

protection de la vie privée dans le cadre de l'éducation civique et non dans celui des cours sur les nouvelles technologies.

Mme Catherine Morin-Desailly, rapporteur pour avis de la commission de la culture, de l'éducation et de la communication, a souligné la nécessité de former les élèves au développement d'une attitude critique et réfléchie vis-à-vis de l'information disponible et à l'acquisition d'un comportement responsable dans l'utilisation des outils interactifs, lors de leur utilisation d'Internet, que cela soit pour la recherche d'informations ou pour échanger avec leurs amis. Cet objectif fait partie intégrante de l'acquisition de la maîtrise des nouvelles technologies demandée à chaque élève au titre du socle commun de connaissances et de compétences défini par la loi du 23 avril 2005.

M. Jean-Jacques Hyest, président, a douté du caractère législatif de nombreuses dispositions figurant dans le code de l'éducation.

Mme Nicole Borvo Cohen-Seat a regretté que la culture générale des élèves ne passe presque plus que par l'éducation civique.

La commission a adopté l'amendement n° 36.

La commission a ensuite examiné l'amendement n° 3 du rapporteur, tendant à insérer un article additionnel après l'article 2. Le rapporteur a expliqué que cet amendement avait deux objets :

- d'une part, il donne un caractère contradictoire au rapport public annuel de la CNIL ; il prévoit le recueil des observations des ministres, personnes et organismes concernés avant la publication du rapport annuel de la CNIL : cette dernière ferait connaître les observations provisoires pour lesquelles elle estime nécessaire de susciter les remarques des personnes susvisées, remarques qui auraient vocation à figurer en annexe du rapport annuel. Cette procédure contradictoire permettrait de mettre en place un dialogue formalisé qui ne pourra qu'améliorer les relations entre la CNIL et les responsables de traitement concernés ;

- d'autre part, il assure une représentation pluraliste lors de la désignation, par les présidents des assemblées parlementaires, des membres de ces assemblées appelés à siéger dans cette commission.

M. Alex Türk s'est déclaré défavorable au premier objet de l'amendement, estimant que la procédure contradictoire qu'elle imposait, d'une part, rendrait très complexe l'établissement du rapport annuel de la CNIL, d'autre part, n'était pas conforme à la nature de la CNIL, qui n'est pas une juridiction, à la différence de la Cour des comptes.

Rejoignant cette analyse, M. Jean-Pierre Michel a souligné en outre que l'adoption de cet amendement conduirait à étendre cette procédure à toutes les autorités administratives indépendantes, ce qui ne lui a pas paru souhaitable.

En conséquence, le rapporteur a retiré son amendement n° 3 et la commission a adopté l'amendement n° 35 de M. Charles Gautier, tendant à assurer la représentation pluraliste de la CNIL.

La commission a ensuite examiné l'amendement n° 4 rectifié du rapporteur, tendant à insérer un article additionnel après l'article 2. M. Christian Cointat, rapporteur, a expliqué que cet amendement visait à permettre la mise en œuvre plus rapide des traitements soumis à déclaration préalable. Dans sa rédaction actuelle, l'article 23 de la loi « informatique et libertés » subordonne la mise en œuvre d'un traitement soumis à déclaration à la transmission par la CNIL d'un récépissé. Or, ce récépissé retarde la mise en œuvre du traitement. En conséquence, l'amendement prévoit que « le demandeur peut mettre en œuvre le traitement dès réception de la preuve de l'accomplissement de la formalité préalable ».

M. Alex Türk s'est déclaré favorable à cet amendement, même s'il a relevé que les responsables de traitements continueraient sans doute, en pratique, à réclamer ledit récépissé « par sécurité ».

La commission a adopté l'amendement n° 4 rectifié.

A l'appui de ses amendements n°s 28, 29, 30 et 31 tendant à confier à la CNIL le contrôle et l'évolution de l'ensemble des systèmes de vidéosurveillance, M. Charles Gautier a fait valoir qu'ils formalisaient une recommandation de son rapport d'information élaboré conjointement avec M. Jean-Patrick Courtois, consacré à la vidéosurveillance et adopté à l'unanimité par la commission des lois en décembre 2008. Cette recommandation rejoint celle formulée dans le rapport d'information consacré à la vie privée à l'heure du numérique des auteurs de la présente proposition de loi, adopté par la commission des lois en mai 2009.

M. Christian Cointat, rapporteur, a souligné, d'une part, que de nombreuses dispositions concernant la vidéosurveillance avaient été adoptées lors de l'examen par l'Assemblée nationale en première lecture du projet de loi sur la sécurité intérieure, dite « LOPPSI », d'autre part, que le dispositif proposé était incomplet : il ne précise pas, notamment, de quelle manière et selon quelles procédures s'exercerait le contrôle de l'installation des systèmes, confié à la CNIL, ni la nature de l'évaluation qui serait réalisée. Il a indiqué que, si l'amendement, après avoir été précisé et complété, était redéposé à l'occasion de l'examen du projet de loi dit « « LOPPSI », il y serait, à titre personnel, favorable.

M. Charles Gautier a retiré ses amendements n°s 28, 29, 30 et 31.

La commission a ensuite examiné l'amendement n° 5 du rapporteur portant sur les correspondants « informatique et libertés » (CIL).

M. Alex Türk a indiqué que les correspondants étaient en augmentation constante : au 1er janvier 2010, ils étaient 1466, représentant quelque 5951 organismes. Ils sont toutefois faiblement implantés dans les collectivités territoriales et les ministères, cette situation semblant résulter d'une certaine hostilité des autorités publiques à l'égard de personnes reconnues comme indépendantes dans l'exercice de leurs fonctions, indépendance qui s'accorderait mal avec le principe d'obéissance hiérarchique de la fonction publique.

Il a souligné que :

- les CIL sont obligatoires en Allemagne depuis près de quarante ans, sans que cela soulève d'objection particulière ;

- la désignation d'un CIL permet la dispense de déclaration préalable auprès de la CNIL ;

- le CIL a l'obligation de dresser un inventaire de tous les traitements effectués dans la structure dans laquelle il se trouve, ce qui est une mission très utile au regard de la protection des données ;

- aucune entreprise ayant désigné un CIL depuis sa création en 2005 ne l'a ensuite supprimé, ce qui tend à prouver que le système donne satisfaction ;

- la CNIL entretient des liens privilégiés de conseil et de formation avec les CIL ;

- la désignation obligatoire des CIL marquait l'aboutissement du processus engagé en 2003-2004, à l'occasion de l'examen de la loi transposant la directive de 1995 sur la protection des données. Il a indiqué qu'alors qu'il était rapporteur pour la commission des lois du Sénat de ce texte, M. Dominique Perben, alors garde des sceaux, avait indiqué en séance que les CIL avaient vocation à devenir un jour obligatoires.

M. Jean-Pierre Vial a noté qu'une réglementation excessive conduirait à complexifier le droit et a jugé que le CIL risquait de se transformer en inspecteur. Il a souligné l'impact de l'amendement proposé tant pour les entreprises, compte tenu du nombre encore limité des CIL, que pour la CNIL elle-même, qui aurait à gérer un réseau considérable de correspondants. En outre, il a indiqué que l'adoption de l'amendement conduirait à doter le CIL d'un statut très précis. En conséquence, il s'est déclaré très réservé quant à l'opportunité d'adopter l'amendement du rapporteur, et a souhaité, à tout le moins, relever sensiblement le seuil déclenchant l'obligation de désigner un CIL.

Mme Catherine Troendle a réaffirmé son opposition à la désignation obligatoire des CIL, mettant en avant le risque de passage progressif d'une mission de conseil à un rôle de contrôleur. Elle a souligné, en outre, que le CIL représentait une charge de travail supplémentaire pour les entreprises.

M. Jean-Jacques Hyest, président, a souligné que l'obligation de désignation d'un CIL dans les collectivités territoriales permettrait, dans l'intérêt de ces derniers, d'examiner attentivement l'ensemble des traitements utilisés et de se prémunir contre toute poursuite. Il s'est réjoui que le rapporteur propose de rétablir le texte actuel de la loi « informatique et libertés » qui prévoit un avis simple de la CNIL, et non un avis conforme comme le proposait la proposition de loi, en cas de démission d'office du correspondant. Ce rétablissement répond ainsi aux critiques craignant de voir le CIL perçu comme un espion ou un nouveau salarié protégé.

A son tour, M. Jean-Pierre Michel a jugé nécessaire la désignation obligatoire d'un CIL dans les collectivités territoriales, soulignant qu'en tant que

membre de la CNIL pendant dix ans, il avait pu constater de nombreuses irrégularités, faites le plus souvent de bonne foi, dans les fichiers détenus par ces dernières. Il a estimé satisfaisant le seuil de 50 salariés ou agents inscrit dans la proposition de loi.

M. Christian Cointat a réaffirmé que le dispositif proposé devait être perçu comme une garantie compte tenu des enjeux.

M. Yves Détraigne a insisté sur l'intérêt de désigner un CIL, qui permet de diffuser la culture « informatique et libertés » au sein des entreprises et des administrations et de leur apporter une plus grande sécurité juridique dans ce domaine.

La commission a adopté l'amendement n° 5 du rapporteur.

La commission a ensuite examiné l'amendement n° 18 du rapporteur, tendant à réécrire l'article 4 de la proposition de loi (autorisation de création des fichiers de police).

M. Bernard Frimat a exprimé la crainte que la présente proposition de loi ne soit jamais inscrite à l'ordre du jour de l'Assemblée nationale, et que les dispositions de l'amendement concernant les fichiers de police, reprises de la proposition de simplification et d'amélioration de la qualité du droit de M. Jean-Luc Warsmann, ne puissent donc pas être adoptées dans ce cadre.

Il a toutefois estimé que les dispositions en cause ne relevaient en aucun cas de la simplification du droit, et souhaité que la proposition de loi de M. Jean-Luc Warsmann précitée puisse être transmise au Conseil Constitutionnel afin que celui-ci puisse se prononcer sur sa constitutionnalité.

M. Jean-Jacques Hyest, président, a regretté que plusieurs textes importants adoptés par le Sénat ne soient pas encore inscrits à l'ordre du jour de l'Assemblée nationale, dont la proposition de loi relative à l'exécution des décisions de justice et aux conditions d'exercice de certaines professions réglementées de M. Laurent Béteille.

Répondant à M. François Pillet, qui l'interrogeait sur les modifications apportées par l'amendement n°18 au régime des fichiers concernant la sûreté de l'Etat ou la défense, M. Christian Cointat, rapporteur, a indiqué que ces fichiers pourraient toujours, comme dans le droit en vigueur, bénéficier d'une dispense de publication par décret en Conseil d'Etat. Par ailleurs, il a estimé que la modification de l'article 4 qu'il proposait rendent plus probable son inscription à l'ordre du jour de l'Assemblée nationale.

La commission a adopté l'amendement n° 18 du rapporteur.

A l'appui de son amendement n° 7 à l'article 6 (obligations d'information du responsable de traitement), M. Christian Cointat, rapporteur, a expliqué qu'il visait à assouplir le principe de consentement préalable en matière de « cookies » en renvoyant l'utilisateur aux possibilités de paramétrage du navigateur Internet afin qu'il puisse exprimer un choix préalable, quel qu'il soit, ce qui semble conforme aux choix récents du législateur communautaire.

M. Alex Türk a souligné que la proposition de loi opérait une évolution profonde en passant de la logique actuelle d'opposition dite « d'opt-out » à une logique de consentement dite d' « opt-in ». Il est en effet très différent d'avoir un droit de refus des « cookies » ou d'avoir un droit au consentement. Dans le premier cas, le silence de l'utilisateur vaut acceptation ; dans le second, il vaut refus. En conséquence, il a souligné que l' « opt-out » était moins protecteur que l' « opt-in », illustrant son propos de la polémique actuelle autour de « Street View », l'application que la société Google a mise en place sur la base d'un « opt-out ». En revanche, il a reconnu que l' « opt-in » pouvait constituer une entrave au développement d'Internet et des outils innovants et conviviaux.

M. Christian Cointat, rapporteur, a indiqué que son amendement n'avait pas tranché le débat « opt-in »/« opt-out » mais laissait aux acteurs le soin de débattre de ces questions.

A l'article 7 (notification des failles de sécurité), M. Alex Türk a indiqué qu'il convenait de rappeler que le responsable de l'entreprise avait la charge de rétablir la situation en cas de faille de sécurité.

Sur l'article 13 (dispositions relatives aux actions juridictionnelles), la commission a examiné les amendements n°16, tendant à supprimer un alinéa inutile, et l'amendement n°43 du Gouvernement tendant à supprimer l'article.

M. François Zocchetto s'est déclaré favorable à la suppression de l'article, jugeant inopportune l'intervention de la CNIL devant les juridictions, fût-ce en tant qu'expert.

M. Pierre Fauchon s'est interrogé sur l'opportunité de légiférer sur cette question, considérant qu'il était possible pour les magistrats de solliciter toute expertise jugée utile.

M. Jean-Jacques Hyest, président, s'est étonné que l'exposé des motifs de l'amendement de suppression du Gouvernement mette en avant l'objectif de stabilité de la norme, objectif quelque peu démenti par la multiplication d'initiatives gouvernementales dans certaines branches du droit, notamment du droit pénal.

M. Christian Cointat a indiqué que les dispositions de l'article 13, en facilitant l'intervention de la CNIL devant les juridictions, avaient pour but de permettre à ces dernières de disposer d'un avis technique dans une matière souvent complexe et à laquelle les magistrats sont peu familiarisés. Il a également souligné que ces dispositions s'inspiraient de celles retenues pour la HALDE et de celles qui sont insérées dans le projet de loi relatif au Défenseur des droits.

La commission a adopté l'amendement n° 16 et rejeté l'amendement n° 43.

La commission des lois a ensuite adopté la proposition de loi ainsi rédigée.

Le sort de l'ensemble des amendements examinés par la commission est retracé dans le tableau suivant :

Article premier Sensibilisation des jeunes aux enjeux de la protection de la vie privée sur Internet			
Auteur	N°	Objet	Sort de l'amendement
M. Christian Cointat, rapporteur	1	Modifications rédactionnelles	Retiré
Mme Morin-Desailly, rapporteur pour avis	36	Insertion des dispositions de l'article 1er modifiées dans la partie du code de l'éducation consacrée à l'éducation civique	Adopté
Article 2 Qualification juridique de l'adresse IP			
M. Christian Cointat, rapporteur	2	Rédactionnel	Adopté
Gouvernement	38	Suppression de l'article	Tombé
Articles additionnels après l'article 2			
M. Christian Cointat, rapporteur	3	Caractère contradictoire du rapport public annuel de la CNIL et composition pluraliste de la commission	Retiré
M. Charles Gautier et les membres du groupe socialiste apparentés et rattachés	35	Composition pluraliste de la commission	Adopté
M. Christian Cointat, rapporteur	4 rect.	Mise en œuvre plus rapide des traitements soumis à déclaration préalable	Adopté
M. Charles Gautier et les membres du groupe socialiste apparentés et rattachés	34	Publicité des avis de la CNIL	Rejeté
	28	Contrôle et évaluation de la vidéosurveillance par la CNIL	Retiré

Division additionnelle après l'article 13			
M. Charles Gautier et les membres du groupe socialiste apparentés et rattachés	29	Rédactionnel	Retiré
Article additionnel après l'article 13			
M. Charles Gautier et les membres du groupe socialiste apparentés et rattachés	30	Suppression des dispositions sur la vidéosurveillance dans la loi du 21 janvier 1995	Retiré
	31	Coordination avec le n°28	Retiré
Article 3 Renforcement du correspondant « informatique et libertés »			
M. Christian Cointat, rapporteur	5	Obligation de création des correspondants « informatique et libertés »	Adopté
Gouvernement	39	Suppression de l'article	Tombé
Article 4 Autorisation de création des fichiers de police			
M. Christian Cointat, rapporteur	18	Nouveau régime des fichiers de police	Adopté
Gouvernement	40	Suppression de l'article	Tombé
M. Charles Gautier et les membres du groupe socialiste apparentés et rattachés	32	Autorisation par la loi des fichiers ou catégories de fichiers de police	Tombé
	33	Mention figurant dans les lois autorisant des fichiers de police	Tombé

Articles additionnels après l'article 4			
M. Christian Cointat, rapporteur	25	Coordination	Adopté
	21	Création d'une formation spécialisée « fichiers de police » au sein de la CNIL	Adopté
	19	Intervention du bureau de la CNIL dans la nouvelle procédure expérimentale pour les fichiers de police	Adopté
	20 rect	Inscription des durées maximales de conservation des données et des modalités de traçabilité des consultations dans les actes réglementaires	Adopté
	22	Transmission à la délégation au renseignement des actes réglementaires de création de fichiers « sûreté/défense »	Adopté
	23	Renforcement du contrôle judiciaire des fichiers de police	Adopté
	24 rect	Droits de la défense dans les comparutions immédiates	Adopté
Article additionnel après l'article 5			
M. Alex Türk	26	Publicité des avis de la CNIL	Adopté
Article 6 Obligations d'information du responsable de traitement			
M. Christian Cointat, rapporteur	6	Assouplissement de l'obligation d'information sur la durée de conservation des données	Adopté
	7	Assouplissement du principe de consentement préalable en matière de cookies	Adopté
Article 7 Notification des failles de sécurité			
M. Christian Cointat, rapporteur	8	Champ d'application de l'obligation de notifier les failles de sécurité	Adopté
	9	Information sur les failles de sécurité	Adopté
	10 rect	Exclusion des fichiers de police de l'obligation d'information sur les failles de sécurité	Adopté
Gouvernement	41	Suppression de l'article	Tombé

Article 8 Droit d'opposition à un traitement			
M. Christian Cointat, rapporteur	11	Clarification	Adopté
	12	Clarification de l'exercice du droit de suppression des données	Adopté
	13	Rédactionnel	Adopté
Gouvernement	42	Suppression de l'article	Tombé
Article 9 Obligation pour le responsable de traitement d'indiquer l'origine de la donnée			
M. Christian Cointat, rapporteur	14	Clarification	Adopté
Article additionnel après l'article 9			
Gouvernement	37	Possibilité d'effectuer des visites inopinées	Adopté
M. Alex Türk	27	Possibilité d'effectuer des visites inopinées	Retiré
Article 10 Publicité des audiences de la formation restreinte de la CNIL			
M. Christian Cointat, rapporteur	15	Suppression de l'article	Adopté
Article 13 Dispositions relatives aux actions juridictionnelles			
M. Christian Cointat, rapporteur	16	Suppression des dispositions prévoyant que les observations écrites de la CNIL sont recevables quelle que soit la procédure applicable	Adopté
Gouvernement	43	Suppression de l'article	Tombé
Article additionnel après l'article 13			
M. Christian Cointat, rapporteur	17	Clarification sur l'application outre-mer de la loi « informatique et libertés »	Adopté

ANNEXE 1
LISTE DES PERSONNES ENTENDUES PAR LE RAPPORTEUR

I. Institutionnels :

Sénateurs

Mme Anne-Marie Escoffier et M. Yves Détraigne, auteurs de la proposition de loi, sénateurs

Mme Catherine Morin-Desailly, rapporteur pour avis de la commission de la culture, sénatrice

Mme Nathalie Goulet, sénateur

Ministère de la Justice

M. Emmanuel Meyer, conseiller

Ministère de l'Intérieur

M. Pierre Boussaroque, sous-directeur des Libertés publiques

Ministère de l'Education nationale

M. Benoît Labrousse, conseiller technique « Nouvelles technologies, éditeurs et multimédias »

Mme Ann-Gaëlle Werner, chargée des Relations avec le Parlement

Ministère de la Défense - Gendarmerie nationale

M. le Lieutenant-colonel Franck Marescal, chef de la division criminalistique « ingéniérie et numérique », Institut de Recherches Criminelles de la Gendarmerie Nationale

M. Le Lieutenant-colonel Alain Permingeat, chef de la division de lutte contre la cybercriminalité, Services Techniques de Recherches Judiciaires et de Documentation

Secrétariat État chargé de la Prospective et du développement économie numérique

M. Fabrice Mattatia, conseiller technique

S.G.A.E.

Mme Suzanne von Coester, conseillère juridique

M. Michael Chaussard, adjoint à la conseillère juridique

Mme Nathalie Gimonet, adjointe au secteur « industries, télécommunications, énergie, compétitivité »

Commission nationale informatique et libertés (CNIL)

M. Alex Türk, président

Mme Sophie Vuillet-Tavernier, directrice des Affaires juridiques, internationales et de l'expertise

Forum des droits sur Internet

Mme Isabelle Falque-Pierrotin, présidente
M. Stéphane Grégoire, juriste

II. Entreprises :

Conseil supérieur du notariat

Me Bernard Reynis, notaire à Paris et ancien président du Conseil supérieur du notariat
M. Xavier Leclerc, responsable du service correspondant à la Protection des données de l'Association pour le Développement du Service Notarial (ADSN)

MEDEF

M. Marc Lolivier, délégué général de la FEVAD (Fédération du e-commerce et de la vente à distance)
M. Nicolas Stoop, chargé de mission à la Direction des Affaires juridiques
Mme Miriana Clerc, chargée de mission à la Direction des Affaires publiques

Google

M. Olivier Esper, chargé des Relations avec les institutions
M. Yoram Elkaim, directeur juridique
M. Alexandra Laferrière, chargée des Relations institutionnelles

Microsoft France

M. Jean Gonié, responsable des Affaires institutionnelles
M. Marc Mossé, directeur des Affaires publiques et juridiques

Price minister

M. Benoît Tabaka, directeur des Affaires juridiques et réglementaires

Syndicat National de Communication Directe

Mme Fabienne Granovsky, responsable déontologie
Mme Nathalie Phan Place, Secrétaire générale

Fédération Française des Telecoms

M. Julien Villalongue, rapporteur de la commission « Sécurité »
Mme Natalie Jouen-Arzur, directrice générale adjointe
Mme Patricia Le Large, membre de la commission « Sécurité »
Mme Florence Chinaud, membre de la commission « Sécurité »

Union Française du Marketing Direct

M. Marc Lolivier, délégué général UFMD et FEVAD

M. Etienne Drouard, avocat Cabinet Morgan Lewis pour l'UFMD

M. Arnaud Caplier, responsable du groupe de travail « Publicité ciblée en ligne » à L'UFMD et membre conseil d'administration du SNCD

III. Associations :

Association Française des Correspondants aux Données personnelles

M. Paul-Olivier Gibert, président

M. Jean-Pierre Rémy

Association Consommation, Logement et Cadre de Vie et UFC-Que chosir ?

Mme Reine-Claude Mader, présidente CLCV

Mme Gaëlle Patetta, directeur juridique UFC

Mme Catalina Chatellier, juriste UFC

IV. Personnes qualifiées :

Me Olivier Proust, avocat

Mme Nathalie Mallet-Poujol, professeur à l'Université Montpellier, chercheur au CNRS

ANNEXE 2

LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS (extraits)

(Version consolidée au 14 mai 2009)

Chapitre Ier : Principes et définitions

Article 1

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Article 5

I. - Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.

II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Chapitre II : Conditions de licéité des traitements de données à caractère personnel

Section 1 : Dispositions générales

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au

regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Article 7

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Section 2 : Dispositions propres à certaines catégories de données

Article 8

I.-Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

II.-Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;

2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;

3° Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;

- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;

4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;

5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;

8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.

III.-Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

IV.-De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

Article 9

Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

Chapitre III : La Commission nationale de l'informatique et des libertés

Article 11

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :

1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.

A ce titre :

a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;

b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;

c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou

envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ;

e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;

f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;

g) Elle peut, dans les conditions définies au chapitre VII, prononcer à l'égard d'un responsable de traitement l'une des mesures prévues à l'article 45 ;

h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;

3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :

a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ;

b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;

c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission, le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ;

4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;

A ce titre :

a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés. A la demande du président de l'une

des commissions permanentes prévue à l'article 43 de la Constitution, l'avis de la commission sur tout projet de loi est rendu public ;

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.

Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Article 13

I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres :

1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ;

2° Deux membres du Conseil économique et social, élus par cette assemblée ;

3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ;

4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;

5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ;

6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;

7° Deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat.

La commission élit en son sein un président et deux vice-présidents, dont un vice-président délégué. Ils composent le bureau.

La formation restreinte de la commission est composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat.

En cas de partage égal des voix, celle du président est prépondérante.

II. - Le mandat des membres de la commission mentionnés aux 3°, 4°, 5°, 6° et 7° du I est de cinq ans ; il est renouvelable une fois. Les membres mentionnés aux 1° et 2° siègent pour la durée du mandat à l'origine de leur désignation ; leurs mandats de membre de la Commission nationale de l'informatique et des libertés ne peuvent excéder une durée de dix ans.

Le membre de la commission qui cesse d'exercer ses fonctions en cours de mandat est remplacé, dans les mêmes conditions, pour la durée de son mandat restant à courir.

Sauf démission, il ne peut être mis fin aux fonctions d'un membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit.

La commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11.

Article 17

La formation restreinte de la commission prononce les mesures prévues au I et au 1° du II de l'article 45.

Chapitre IV : Formalités préalables à la mise en œuvre des traitements

Article 22

I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :

1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

2° Les traitements mentionnés au 3° du II de l'article 8.

III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.

La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.

Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.

En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31.

Section 1 : Déclaration.

Article 23

I. - La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique.

La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé ; il n'est exonéré d'aucune de ses responsabilités.

II. - Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Article 24

I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.

Ces normes précisent :

1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;

2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;

3° La ou les catégories de personnes concernées ;

4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;

5° La durée de conservation des données à caractère personnel.

Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique.

II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.

Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23.

Section 2 : Autorisation

Article 25

I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :

1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;

2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;

3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;

4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

5° Les traitements automatisés ayant pour objet :

- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;

- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;

6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;

7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;

8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes

destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Article 26

I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement.

II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.

III. - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.

IV. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Article 27

I. - Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;

2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

II. - Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ;

2° Ceux des traitements mentionnés au I :

- qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;

- qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;

- et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;

3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;

4° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.

III. - Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.

Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes

Section 1 : Obligations incombant aux responsables de traitements.

Article 32

I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

3° Du caractère obligatoire ou facultatif des réponses ;

4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

5° Des destinataires ou catégories de destinataires des données ;

6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;

7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

II.- Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;

- des moyens dont elle dispose pour s'y opposer.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

III.- Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

IV.- Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

V.- Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

VI.-Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour

préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Section 2 : Droits des personnes à l'égard des traitements de données à caractère personnel

Article 38

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

Article 39

I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit

d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

II.- Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.

Article 40

Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.

Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 41

Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.

La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.

Chapitre VI : Le contrôle de la mise en œuvre des traitements

Article 44

I.-Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.

II.- En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du président du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

Ce magistrat est saisi à la requête du président de la commission. Il statue par une ordonnance motivée, conformément aux dispositions prévues aux articles 493 à 498 du code de procédure civile. La procédure est sans représentation obligatoire.

La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Celui-ci peut se rendre dans les locaux durant l'intervention. A tout moment, il peut décider l'arrêt ou la suspension de la visite.

III.- Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé.

Il est dressé contradictoirement procès-verbal des vérifications et visites menées en application du présent article.

IV.- Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.

Chapitre VII : Sanctions prononcées par la Commission nationale de l'informatique et des libertés

Article 45

I. - La Commission nationale de l'informatique et des libertés peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.

Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :

1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;

2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

II. - En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :

1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ;

2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;

3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

Article 46

Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la commission mais ne prend pas part à ses délibérations. La commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information.

La commission peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner

l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.

Les décisions prises par la commission au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.

Article 47

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder 150 000 Euros. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros.

Lorsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

Chapitre VIII : Dispositions pénales

Article 50

Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Article 51

Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :

1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;

2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

ANNEXE 3
Dispositions pénales

ARTICLES 226-16 A 226-24 DU CODE PENAL

Article 226-16 Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article 226-16-1-A Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-16-1 Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-17 Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-18 Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-18-1 Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-19 Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Article 226-19-1 En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement :

1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 226-20 Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Article 226-21 Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-22 Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 226-22-1 Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-22-2 Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données.

Article 226-23 Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 226-24 Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

TABLEAU COMPARATIF

___

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique	**Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique**
	TITRE I^ER	TITRE I^ER
	DISPOSITIONS PORTANT MODIFICATION DU CODE DE L'EDUCATION	DISPOSITIONS PORTANT MODIFICATION DU CODE DE L'EDUCATION
	Article 1^er	Article 1^er
Code de l'éducation	~~Le second alinéa de~~ l'article ~~L. 312-9~~ du code de l'éducation est ~~remplacé par trois alinéas~~ ainsi ~~rédigés~~ :	L'article L. 312-15 du code de l'éducation est complété par un alinéa ainsi rédigé :
Art. L. 312-15. — Outre les enseignements concourant aux objectifs définis à l'article L. 131-1-1, l'enseignement d'éducation civique comporte, à tous les stades de la scolarité, une formation aux valeurs de la République, à la connaissance et au respect des droits de l'enfant consacrés par la loi ou par un engagement international et à la compréhension des situations concrètes qui y portent atteinte. Dans ce cadre est donnée une information sur le rôle des organisations non gouvernementales oeuvrant pour la protection de l'enfant. Lors de la présentation de la liste des fournitures scolaires, les élèves reçoivent une information sur la nécessité d'éviter l'achat de produits fabriqués par des enfants dans des conditions contraires aux conventions internationalement reconnues. L'enseignement d'éducation civique comporte également, à l'école primaire et au collège, une formation consacrée à la connaissance et au respect des problèmes des personnes handicapées et à leur intégration dans la société. Les établissements scolaires s'associent avec les centres accueillant des personnes handicapées afin de favoriser les échanges et les rencontres avec les		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
élèves.		
	~~« Dans ce cadre, ils reçoivent de la part d'enseignants préalablement formés sur le sujet une information sur les risques liés aux usages des services de communication au public en ligne :~~	« Dans le cadre de l'enseignement d'éducation civique, les élèves sont formés afin de développer une attitude critique et réfléchie vis-à-vis de l'information disponible et d'acquérir un comportement responsable dans l'utilisation des outils interactifs, lors de leur usage des services de communication au public en ligne. Ils sont informés des moyens de maîtriser leur image publique, des dangers de l'exposition de soi et d'autrui, des droits d'opposition, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que des missions de la Commission nationale de l'informatique et des libertés. »
	~~« – Au regard du droit de la propriété intellectuelle ; ils sont informés des dangers du téléchargement et de la mise à disposition illicite d'oeuvres ou d'objets protégés par un droit d'auteur ou un droit voisin pour la création artistique, ainsi que sur les sanctions encourues en cas de manquement au délit de contrefaçon. Cette information porte également sur l'existence d'une offre légale d'oeuvres ou d'objets protégés par un droit d'auteur ou un droit voisin sur les services de communication au public en ligne ;~~	**Alinéa supprimé.**
	~~« – Au regard de la protection des données personnelles et, plus généralement, du droit à la vie privée ; ils sont informés des dangers de l'exposition de soi et d'autrui lorsqu'ils utilisent des services de communication au public en ligne, des droits d'opposition commerciale, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que des missions de la Commission nationale de l'informatique et des libertés. »~~	**Alinéa supprimé.**

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	TITRE II	TITRE II
	DISPOSITIONS PORTANT MODIFICATION DE LA LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS	DISPOSITIONS PORTANT MODIFICATION DE LA LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS
	Article 2	Article 2
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Le deuxième alinéa de l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est complété par une phrase ainsi rédigée :	*(Alinéa sans modification).*
Art. 2. — La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouil-	~~« Constitue en particulier une donnée à caractère personnel toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication. »~~	« Tout numéro identifiant le titulaire d'un accès à des services de communication au public en ligne est visé par le présent alinéa. »

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
lage, l'effacement ou la destruction. Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés. La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.		
		Article 2 bis (nouveau)
Art. 13. — I. — La Commission nationale de l'informatique et des libertés est composée de dix-sept membres : 1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ;.		Au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 précitée, après les mots : « par le Sénat » sont insérés les mots : « , de manière à assurer une représentation pluraliste ».
		Article 2 ter (nouveau)
		I. — Le troisième alinéa du I de l'article 23 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :
Art. 23. — I. — La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi. Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique. La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en oeuvre le traitement dès réception de ce récépissé ; il n'est exonéré d'aucune de ses responsabilités. II. — Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 ne		« Le demandeur peut mettre en œuvre le traitement dès réception de la preuve du dépôt de la déclaration ; il n'est exonéré d'aucune de ses responsabilités. »

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.		
		II. — L'article 70 de la même loi est ainsi modifié :
Art. 70. — Si la Commission des Communautés européennes a constaté qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données.		1° Au premier alinéa, les mots : « délivre le récépissé avec mention » sont remplacés par les mots : « informe le demandeur » ;
Lorsqu'elle estime qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des Communautés européennes. Lorsqu'elle est saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et peut enjoindre au responsable du traitement de suspendre le transfert des données. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au		2° Au second alinéa, les mots : « délivre le récépissé et » sont supprimés.

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
transfert de données à caractère personnel à destination de cet Etat.		
	Article 3	Article 3
	I. — Après le chapitre IV de la loi n° 78-17 du 6 janvier 1978 précitée, il est inséré un chapitre IV *bis* ainsi rédigé :	I. — *(Alinéa sans modification).*
	« Chapitre IV *bis*	*(Alinéa sans modification).*
	« Le correspondant « informatique et libertés »	*(Alinéa sans modification).*
	« *Art. 31-1.* — Lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel ~~et que~~ plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en oeuvre, ladite autorité ou ledit organisme désigne un correspondant « informatique et libertés ».	« *Art. 31-1.* — Lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel qui relève du régime d'autorisation en application des articles 25, 26 ou 27 ou pour lequel plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre, ladite autorité ou ledit organisme désigne, en son sein ou dans un cadre mutualisé, un correspondant « informatique et libertés ». Toute autorité publique ou organisme privé qui ne remplit pas les conditions précédentes peut toutefois désigner un tel correspondant, y compris dans un cadre mutualisé.
	~~« La désignation est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.~~	**Alinéa supprimé.**
	« Le correspondant est chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi et d'informer l'ensemble des personnes travaillant pour le compte de l'autorité ou de l'organisme ~~de la nécessité de protéger les~~ données à caractère personnel.	« Le correspondant est chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi et d'informer et de conseiller l'ensemble des personnes travaillant pour le compte de l'autorité ou de l'organisme sur l'ensemble des questions de protection des données à caractère personnel.
	« Le correspondant bénéficie des qualifications requises pour exercer ces missions. Il tient une liste des traitements effectués, immédiatement accessible à toute personne en faisant la demande. Il ne peut faire l'objet d'aucune sanction de la part de l'employeur du	« Le correspondant bénéficie des qualifications requises pour exercer ces missions. Il tient une liste des traitements effectués, régulièrement mise à jour et immédiatement accessible à toute personne en faisant la demande. Il ne peut faire l'objet d'aucune sanction de la

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	fait de l'accomplissement de ses missions. Il ~~peut saisir~~ la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.	part de l'employeur du fait de l'accomplissement de ses missions. Il saisit la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. Il établit un rapport annuel d'activité et le transmet à la Commission. « La désignation du correspondant est notifiée à la Commission qui peut la refuser s'il ne remplit pas les conditions de compétence visées aux deux alinéas précédents. Cette désignation est portée à la connaissance des instances représentatives du personnel.
Art. 23 et 24. — Cf. annexe.	« En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande de la Commission ~~nationale de l'informatique et des libertés ou après son avis conforme.~~ »	« En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission. »
Art. 22. —	II. — Le III de l'article 22 est ainsi rédigé :	II. — *(Sans modification).*
III. — Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé. La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel. Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire	« III. — Les traitements pour lesquels le responsable a désigné un correspondant « informatique et libertés », dont le statut et les missions sont définis à l'article 31 *bis*, sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de l'Union européenne est envisagé. »	

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.		
. . . . .		
Art. 31 bis. — *Cf. supra.*		
	Article 4	Article 4
	~~I.~~ — L'article 26 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	L'article 26 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :
Art. 26. — I. — Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat et :	« *Art. 26.* — I. — ~~Sont autorisées par la loi les catégories de traitements nationaux de données à caractère personnel mis en oeuvre pour le compte de l'État et :~~	« *Art. 26.* — I. — Les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État, la défense, la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté, ne peuvent être autorisés qu'à la condition de répondre à une ou plusieurs des finalités suivantes :
1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;	~~« 1° Qui intéressent la sécurité publique ;~~	« 1° Permettre aux services de renseignement d'exercer leurs missions ;
2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.	~~« 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.~~	« 2° Permettre aux services de police judiciaire d'opérer des rapprochements entre des infractions susceptibles d'être liées entre elles, à partir des caractéristiques de ces infractions, afin de faciliter l'identification de leurs auteurs ;
	~~« Les catégories de traitements~~	« 3° Faciliter par l'utilisation

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	~~de données à caractère personnel sont constituées par les traitements qui répondent à une même finalité, portent sur les mêmes catégories de données et ont les mêmes catégories de destinataires.~~	d'éléments biométriques ou biologiques se rapportant aux personnes, d'une part la recherche et l'identification des auteurs de crimes et de délits, d'autre part la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie ;
L'avis de la commission est publié avec l'arrêté autorisant le traitement.	~~« L'avis de la Commission nationale de l'informatique et des libertés mentionné au *a* du 4° de l'article 11 sur tout projet de loi autorisant la création d'une telle catégorie de traitements de données est transmis au Parlement simultanément au dépôt du projet de loi.~~	« 4° Répertorier les personnes et les objets signalés par les services habilités à alimenter le traitement, dans le cadre de leurs missions de police administrative ou judiciaire, afin de faciliter les recherches des services enquêteurs et de porter à la connaissance des services intéressés la conduite à tenir s'ils se trouvent en présence de la personne ou de l'objet ;
II. — Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.	~~« II. — La loi autorisant une catégorie de traitements de données mentionné au I prévoit :~~	« 5° Faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs ;
III. — Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.	~~« - les services responsables ;~~	« 6° Faciliter la diffusion et le partage des informations détenues par différents services de police judiciaire, sur les enquêtes en cours ou les individus qui en font l'objet, en vue d'une meilleure coordination de leurs investigations ;
IV. — Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.	~~« - leurs finalités ;~~	« 7° Centraliser les informations destinées à informer le Gouvernement et le représentant de l'État afin de prévenir les atteintes à la sécurité publique ;
	~~« - la durée de conservation des informations traitées. »~~	« 8° Procéder à des enquêtes administratives liées à la sécurité publique ;
		« 9° Faciliter la gestion administrative ou opérationnelle des services de police et de gendarmerie ainsi que des services chargés de l'exécution des dé-

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		cisions des juridictions pénales en leur permettant de consigner les événements intervenus, de suivre l'activité des services et de leurs agents, de suivre les relations avec les usagers du service, d'assurer une meilleure allocation des moyens aux missions et d'évaluer les résultats obtenus ; « 10° Organiser le contrôle de l'accès à certains lieux nécessitant une surveillance particulière ; « 11° Recenser et gérer les données relatives aux personnes ou aux biens faisant l'objet d'une même catégorie de décision administrative ou judiciaire ; « 12° Faciliter l'accomplissement des tâches liées à la rédaction, à la gestion et à la conservation des procédures administratives et judiciaires et assurer l'alimentation automatique de certains fichiers de police ; « 13° Recevoir, établir, conserver et transmettre les actes, données et informations nécessaires à l'exercice des attributions du ministère public et des juridictions pénales, et à l'exécution de leurs décisions. « II. — Les traitements mentionnés au I sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. « Ceux des traitements mentionnés au I qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. « L'avis de la Commission nationale de l'informatique et des libertés est publié avec l'arrêté ou le décret autorisant le traitement. « III *(nouveau)*. — Dans les traitements mentionnés au 7° du I du présent article, la durée de conservation

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		des données concernant les mineurs est inférieure à celle applicable aux majeurs, sauf à ce que leur enregistrement ait été exclusivement dicté par l'intérêt du mineur. Cette durée est modulée afin de tenir compte de la situation particulière des mineurs et, le cas échéant, en fonction de la nature et de la gravité des atteintes à la sécurité publique commises par eux. « IV *(nouveau)*. — Les traitements de données à caractère personnel intéressant la sûreté de l'État et la défense peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la Commission nationale de l'informatique et des libertés. « Les actes réglementaires qui autorisent ces traitements sont portés à la connaissance de la délégation parlementaire au renseignement et de la Commission nationale de l'informatique et des libertés. « V *(nouveau)*. — Lorsque la mise au point technique d'un traitement mentionné au I nécessite une exploitation en situation réelle de fonctionnement, un tel traitement peut être mis en œuvre à titre expérimental pour une durée de dix-huit mois, après déclaration auprès de la Commission nationale de l'informatique et des libertés. « Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les modalités selon lesquelles la commission est informée de l'évolution technique d'un tel projet de traitement et fait part de ses recommandations au seul responsable de ce projet. « VI *(nouveau)*. — Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte ré-

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		glementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la Commission nationale de l'informatique et des libertés un engagement de conformité de celui-ci à la description figurant dans l'autorisation. »
		Article 4 *bis (nouveau)*
		La loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifiée :
Art. 8. —		1° Au IV de l'article 8, la référence : « II » est remplacée par les références : « deuxième alinéa du II » ;
IV. — De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.		
Art. 27. —		2° Au III de l'article 27, la référence : « IV » est remplacée par la référence : « VI » ;
III. — Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.		
Art. 31. — I.. — La commission met à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26..		3° Au premier alinéa du I de l'article 31, la référence : « III » est remplacée par la référence : « IV » ;
Art. 44. —		4° Au IV de l'article 44, la référence : « III » est remplacée par la référence : « IV » ;
IV. — Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.		
Art. 49. — La commission peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de la Communauté européenne, procéder à des vérifications dans les mêmes conditions, selon les mêmes procédures et sous les		5° Au premier alinéa de l'article 49, les références : « au I ou au II » sont remplacées par les références : « aux I, II ou III ».

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
mêmes sanctions que celles prévues à l'article 45, sauf s'il s'agit d'un traitement mentionné au I ou au II de l'article 26.		
La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans d'autres Etats membres de la Communauté européenne.		
		Article 4 ter (nouveau)
Art. 13. — I. — La Commission nationale de l'informatique et des libertés est composée de dix-sept membres :		Le I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 précitée est complété par un alinéa ainsi rédigé :
1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ;		
2° Deux membres du Conseil économique et social, élus par cette assemblée ;		
3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ;		
4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;		
5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ;		
6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;		
7° Deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
par le Président du Sénat. La commission élit en son sein un président et deux vice-présidents, dont un vice-président délégué. Ils composent le bureau. La formation restreinte de la commission est composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat. En cas de partage égal des voix, celle du président est prépondérante..		
		« La commission élit en son sein trois de ses membres, dont deux parmi les membres mentionnés au 3°, au 4° ou au 5°. Ils composent une formation spécialisée de la commission chargée d'instruire les demandes d'avis formulées conformément aux I, II et VI de l'article 26. Cette formation est également chargée du suivi de la mise en œuvre expérimentale de traitements de données prévue au V de l'article 26. Elle organise, en accord avec les responsables de traitements, les modalités d'exercice du droit d'accès indirect, défini aux articles 41 et 42. »
		Article 4 quater (nouveau)
Art. 16. — Le bureau peut être chargé par la commission d'exercer les attributions de celle-ci mentionnées : - au dernier alinéa de l'article 19 ; - à l'article 25, en cas d'urgence ; - au second alinéa de l'article 70. Le bureau peut aussi être chargé de prendre, en cas d'urgence, les décisions mentionnées au premier alinéa du I de l'article 45.		Après le troisième alinéa de l'article 16 de la loi n° 78-17 du 6 janvier 1978 précitée, il est inséré un alinéa ainsi rédigé : « – au V de l'article 26 ; ».

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		Article 4 quinquies (nouveau)
Art. 29. — Les actes autorisant la création d'un traitement en application des articles 25, 26 et 27 précisent :		L'article 29 de la loi n° 78-17 du 6 janvier 1978 précitée est complété par un alinéa ainsi rédigé :
1° La dénomination et la finalité du traitement ;		
2° Le service auprès duquel s'exerce le droit d'accès défini au chapitre VII ;		
3° Les catégories de données à caractère personnel enregistrées ;		
4° Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;		
5° Le cas échéant, les dérogations à l'obligation d'information prévues au V de l'article 32.		
		« Les actes autorisant la création des traitements de l'article 26 comportent en outre la durée de conservation des données enregistrées et les modalités de traçabilité des consultations du traitement. »
		Article 4 sexies (nouveau)
Ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires		Le deuxième alinéa du III de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires est complété par une phrase ainsi rédigée :
Art. 6 nonies. —		
III. — Sans préjudice des compétences des commissions permanentes, la délégation parlementaire au renseignement a pour mission de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget.		
Les ministres mentionnés au premier alinéa du présent III adressent à la délégation des informations et des éléments d'appréciation relatifs au budget, à l'activité générale et à l'organisa-		« Sont transmis à la délégation les actes réglementaires autorisant des traitements de données à caractère personnel intéressant la sûreté de l'État et la défense. »

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
tion des services de renseignement placés sous leur autorité. Ces informations et ces éléments d'appréciation ne peuvent porter ni sur les activités opérationnelles de ces services, les instructions données par les pouvoirs publics à cet égard et le financement de ces activités, ni sur les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement. La délégation peut entendre le Premier ministre, les ministres et le secrétaire général de la défense nationale. S'agissant des agents exerçant ou ayant exercé des fonctions au sein des services mentionnés au premier alinéa du présent III, seuls les directeurs en fonction de ces services peuvent être entendus.		
. . . . .		
Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure		*Article 4 septies (nouveau)*
Art. 21. —		Le III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure est ainsi modifié :
III. — Le traitement des informations nominatives est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention sauf si le procureur de la République ordonne l'effacement des données personnelles.		1° Après la deuxième phrase, il est inséré une phrase ainsi rédigée : « Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. » ; 2° Après la troisième phrase, il est inséré une phrase ainsi rédigée : « Lorsque le procureur de la République prescrit le maintien des données à caractère personnel d'une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. » ; 3° Sont ajoutés une phrase et un alinéa ainsi rédigés :
. . . . .		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		« Les autres décisions de classement sans suite font l'objet d'une mention.
		« Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont transmises aux responsables de tous les traitements automatisés pour lesquels ces décisions ont des conséquences sur la durée de conservation des données à caractère personnel. »
		Article 4 octies (nouveau)
Code de procédure pénale		Après le second alinéa de l'article 395 du code de procédure pénale, il est inséré un alinéa ainsi rédigé :
Art. 395. — Si le maximum de l'emprisonnement prévu par la loi est au moins égal à deux ans, le procureur de la République, lorsqu'il lui apparaît que les charges réunies sont suffisantes et que l'affaire est en l'état d'être jugée, peut, s'il estime que les éléments de l'espèce justifient une comparution immédiate, traduire le prévenu sur-le-champ devant le tribunal. En cas de délit flagrant, si le maximum de l'emprisonnement prévu par la loi est au moins égal à six mois, le procureur de la République, s'il estime que les éléments de l'espèce justifient une comparution immédiate, peut traduire le prévenu sur-le-champ devant le tribunal.		« Si le procureur de la République envisage de faire mention d'éléments concernant le prévenu et figurant dans un traitement automatisé d'informations nominatives prévu par l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, ces informations doivent figurer dans le dossier mentionné à l'article 393 du présent code. »
Le prévenu est retenu jusqu'à sa comparution qui doit avoir lieu le jour même ; il est conduit sous escorte de-		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
vant le tribunal.		
	Article 5	Article 5
Art. 31. — I. — La commission met à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26.	Après le 2° de l'article 31 de la loi n° 78-17 du 6 janvier 1978 précitée, il est inséré un 2° *bis* ainsi rédigé :	*(Sans modification).*
Cette liste précise pour chacun de ces traitements :		
1° L'acte décidant la création du traitement ou la date de la déclaration de ce traitement ;		
2° La dénomination et la finalité du traitement ;		
	« 2° *bis* La durée de conservation des données à caractère personnel ; ».	
3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celles de son représentant ;		
4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ;		
5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ;		
6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.		
		Article 5 bis (nouveau)
II. — La commission tient à la disposition du public ses avis, décisions ou recommandations.		Le II de l'article 31 de la loi du 6 janvier 1978 précitée est complété par une phrase ainsi rédigée :

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		« A l'exception des cas prévus aux articles 26 et 27, lorsqu'une loi prévoit qu'un décret, ou un arrêté, est pris après avis de la Commission nationale de l'informatique et des libertés, cet avis est publié avec le décret ou l'arrêté correspondant. »
III. — La Commission nationale de l'informatique et des libertés publie la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.		
	Article 6	Article 6
	I. — Les I et II de l'article 32 de la loi n° 78-17 du 6 janvier 1978 précitée sont remplacés par quatre paragraphes ainsi rédigés :	I. — *(Alinéa sans modification).*
Art. 32. — I. — La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :	« I. — ~~Avant tout traitement~~ de données à caractère personnel, le responsable du traitement ou son représentant :	« I. — Dès la collecte de données à caractère personnel, le responsable du traitement ou son représentant :
	« - Informe, ~~de manière~~ spécifique, claire et accessible, la personne concernée, sauf si elle a déjà été informée au préalable :	« - Informe, sous une forme spécifique et de manière claire et accessible, la personne concernée, sauf si elle en a déjà été informée au préalable :
1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;	« 1° De l'identité et de l'adresse du responsable du traitement et, le cas échéant, de celle de son représentant ;	« 1° *(Sans modification).*
2° De la finalité poursuivie par le traitement auquel les données sont destinées ;	« 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;	« 2° *(Sans modification).*
	« ~~2° *bis* De~~ la durée de conservation des données à caractère personnel ;	« 3° Des critères déterminant la durée de conservation des données à caractère personnel ;
3° Du caractère obligatoire ou facultatif des réponses ;	« ~~3°~~ Du caractère obligatoire ou facultatif des réponses ;	« 4° *(Sans modification).*
4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;	« ~~4°~~ Des conséquences éventuelles d'un défaut de réponse ~~de la personne concernée ;~~	« 5° Des conséquences éventuelles d'un défaut de réponse ;

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
5° Des destinataires ou catégories de destinataires des données ;	« ~~5°~~ Des destinataires ou catégories de destinataires des données ;	« 6° *(Sans modification).*
6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;	« ~~6°~~ Des coordonnées du service auprès duquel ~~la personne concernée peut exercer ses~~ droits ~~de suppression~~, d'accès ~~et~~ de rectification ; ~~si le responsable du traitement dispose d'un service de communication au public en ligne, il doit permettre à la personne concernée d'exercer ses droits par voie électronique après identification, et l'informe de cette possibilité ;~~	« 7° Des coordonnées du service auprès duquel les droits d'accès, de rectification et de suppression peuvent s'exercer ;
7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.		« 8° *(nouveau)* Le cas échéant, des modalités d'exercice de ces droits par voie électronique après identification ;
	« ~~7°~~ Le cas échéant~~, dans les conditions définies par décret en Conseil d'État,~~ des transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union européenne ;	« 9° *(nouveau)* Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union européenne ;
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.	« - Met en mesure la personne concernée d'exercer son droit d'opposition, tel que visé au premier alinéa de l'article 38 ;	*(Alinéa sans modification).*
	« - ~~Recueille le~~ consentement de la personne concernée, sauf dans les cas visés à l'article 7.	« - S'assure du consentement de la personne concernée, sauf dans les cas visés à l'article 7.
	« I *bis*. — Si le responsable du traitement dispose d'un service de communication au public en ligne, il l'utilise pour porter à la connaissance du public, ~~de manière~~ spécifique, ~~claire, accessible~~ et permanente, toutes les informations visées aux 1° à ~~7°~~ du I.	« I *bis*. — Si le responsable du traitement dispose d'un service de communication au public en ligne, il l'utilise pour porter à la connaissance du public, dans une rubrique spécifique et permanente ainsi que de manière claire et accessible, toutes les informations visées aux 1° à 9° du I.
II. — Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :	« II. — Le responsable du traitement ou son représentant informe, ~~de manière~~ spécifique, ~~claire, accessible~~ et permanente, tout utilisateur d'un réseau de communication électronique :	« II. — Le responsable du traitement ou son représentant informe, dans une rubrique spécifique et permanente ainsi que de manière claire et accessible, tout utilisateur d'un réseau de communication électronique :
- de la finalité de toute action tendant à accéder, par voie de transmis-	« - De la finalité ~~de toute action~~ tendant à accéder, par voie de transmis-	« - De la finalité des actions tendant à accéder, par voie de transmission

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
sion électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;	sion électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement ;	électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement ;
- des moyens dont elle dispose pour s'y opposer.	« - De la nature des informations stockées ;	*(Alinéa sans modification).*
	« - Des personnes ou catégories de personnes habilitées à avoir accès à ces informations ;	*(Alinéa sans modification).*
	« ~~II *bis*. — Après avoir délivré l'information prévue au II, le responsable du traitement ou son représentant recueille le consentement de l'utilisateur.~~	« - Des moyens dont l'utilisateur dispose pour exprimer ou refuser son consentement.
Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :	« Les dispositions du II ~~et de l'alinéa précédent~~ ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :	« Les dispositions du présent II ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :
- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;	« - Soit a pour finalité exclusive de permettre la communication par voie électronique ;	*(Alinéa sans modification).*
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur..	« - Soit est strictement nécessaire à la fourniture d'un service de communication au public en ligne à la demande expresse de l'utilisateur. »	*(Alinéa sans modification).*
Art. 7. — Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :	II. — Le premier alinéa du III du même article est ainsi rédigé :	II. — *(Sans modification).*
1° Le respect d'une obligation légale incombant au responsable du traitement ;	« Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant fournit à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, avant la première communication des données. »	
2° La sauvegarde de la vie de la personne concernée ;		
3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;		
4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
à la demande de celle-ci ; 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. *Art. 38. — Cf. infra.*		
	Article 7	Article 7
	L'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	*(Alinéa sans modification).*
Art. 34. — Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.	« *Art. 34.* — Le responsable du traitement met en oeuvre toutes mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre toute violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicites, ~~particulièrement lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.~~	« *Art. 34.* — Le responsable du traitement met en oeuvre toutes mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre toute violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicites.
Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.	« En cas ~~d'atteinte au~~ traitement de données à caractère personnel, le responsable du traitement avertit sans délai la Commission nationale de l'informatique et des libertés ~~qui peut, si cette atteinte est de nature à affecter les données à caractère personnel d'une ou de plusieurs personnes physiques, exiger du responsable du traitement qu'il avertisse également ces personnes.~~ Le contenu, la forme et les modalités de ~~ces notifications~~ sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. »	« En cas <u>de violation du</u> traitement de données à caractère personnel, le responsable de traitement avertit sans délai <u>le correspondant « informatique et libertés », ou, en l'absence de celui-ci,</u> la Commission nationale de l'informatique et des libertés. <u>Le correspondant « informatique et libertés » prend immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données et informe la Commission nationale de l'informatique et des libertés. Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, le responsable du traitement en informe également ces personnes.</u> Le contenu, la forme et les modalités de <u>cette information</u> sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		Un inventaire des atteintes aux traitements de données personnelles est tenu à jour par le correspondant « informatique et libertés ».
		« Les dispositions du présent article ne s'appliquent pas aux traitements de données personnelles désignés à l'article 26.
		« Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés aux 2° et 6° du II de l'article 8. »
	Article 8	Article 8
	I. — L'article 38 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	I. — *(Alinéa sans modification).*
Art. 38. — Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.	« *Art. 38.* — ~~Avant tout traitement~~ de données ~~personnelles~~ ou, en cas de collecte indirecte, avant toute communication de données personnelles, toute personne physique est mise en mesure de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, ~~notamment~~ commerciale, ~~par le responsable actuel du traitement ou celui d'un traitement ultérieur.~~	« *Art. 38.* — Dès la collecte de données à caractère personnel, ou, en cas de collecte indirecte, avant toute communication de données personnelles, toute personne physique est mise en mesure de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection commerciale.
Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.	« Lorsque des données personnelles ont été traitées, toute personne physique identifiée a le droit, pour des motifs légitimes, ~~de demander~~, sans frais, leur suppression auprès du responsable du traitement. Ce droit ne peut être exercé lorsque le traitement répond à une obligation légale ~~ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement. »~~	« Lorsque des données personnelles ont été traitées, toute personne physique justifiant de son identité a le droit, pour des motifs légitimes, d'exiger, sans frais, leur suppression auprès du responsable du traitement.
Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.		« Ce droit ne peut être exercé lorsque :
		« 1° le traitement répond à une obligation légale ;
		« 2° le droit de suppression a été écarté par une disposition expresse de l'acte autorisant le traitement ;
		« 3° les données sont nécessaires à la finalité du traitement ;

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		« 4° le traitement est nécessaire pour la sauvegarde, la constatation, l'exercice ou la défense d'un droit ; « 5° le droit de suppression porte atteinte à une liberté publique garantie par la loi ; « 6° les données constituent un fait historique. »
	II. — Le début du premier alinéa du I de l'article 39 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	II. — *(Alinéa sans modification).*
Art. 39. — I. — Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre	« Toute personne physique ~~identifiée~~ a le droit d'interroger le responsable du traitement... *(le reste sans changement)* ».	« Toute personne physique justifiant de son identité a le droit d'interroger le responsable du traitement... *(le reste sans changement)* ».

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition..		
	III. — Le début du premier alinéa de l'article 40 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	III. — *(Alinéa sans modification).*
Art. 40. — Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord. Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39. Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin	« Toute personne physique ~~identifiée~~ a le droit de demander au responsable ~~d'un~~ traitement que soient... *(le reste sans changement)* ».	« Toute personne physique justifiant de son identité a le droit de demander au responsable du traitement que soient... *(le reste sans changement)* ».

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.		
Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.		
Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.		
	Article 9	Article 9
Art. 39. — I. — Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :	Le I de l'article 39 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :	*(Alinéa sans modification).*
1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;		
2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;	1° ~~Après le troisième alinéa (2°), il est inséré un 2° *bis* ainsi rédigé :~~	1° Les 3° et 4° du I sont remplacés par des alinéas 3° à 6° ainsi rédigés :
	« ~~2° *bis*~~ La durée de conservation des données à caractère personnel ; » ;	« 3° La durée de conservation des données à caractère personnel ;
3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;		« 4° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union européenne ;
		« 5° La communication, sous une forme accessible, des données à carac-

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		tère personnel qui la concernent ; « 6° La communication, sous une forme accessible, de toute information disponible quant à l'origine de celles-ci ; » ;
4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;	2° ~~Au cinquième alinéa (4°), les mots : « toute information disponible quant à » sont supprimés.~~	2° En conséquence, la référence : « 5° » est remplacée par la référence : « 7° ».
5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition..		
		Article 9 bis (nouveau) Les dispositions des I et II de l'article 44 de la loi n° 78-17 du 6 janvier 1978 précitée sont remplacées par quatre alinéas ainsi rédigés :
Art. 44. — I. — Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de		« I. — Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en oeuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.		ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectés au domicile privé.
Le procureur de la République territorialement compétent en est préalablement informé.		« II. — Lorsque l'urgence, la gravité des faits justifiant le contrôle ou le risque de destruction ou de dissimulation de documents l'exigent, la visite est préalablement autorisée par le juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter. Dans les autres cas, le responsable des lieux peut s'opposer à la visite, qui ne peut alors se dérouler qu'avec l'autorisation du juge des libertés et de la détention. Celui-ci statue dans des conditions fixées par décret en Conseil d'État.
II. — En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du président du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.		
Ce magistrat est saisi à la requête du président de la commission. Il statue par une ordonnance motivée, conformément aux dispositions prévues aux articles 493 à 498 du code de procédure civile. La procédure est sans représentation obligatoire.		
La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Celui-ci peut se rendre dans les locaux durant l'intervention.A tout moment, il peut décider l'arrêt ou la suspension de la visite.		« La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant, qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle. Le juge peut, s'il l'estime utile, se rendre dans les locaux pendant l'intervention. A tout moment, il peut décider la suspension ou l'arrêt de la visite.
		« L'ordonnance ayant autorisé la visite est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite et précise qu'une telle demande n'est pas suspensive. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel devant le premier président de la cour d'appel. »

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	Article 10	Article 10
Art. 45. — I. — La Commission nationale de l'informatique et des libertés peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.		
Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :	~~1° Au deuxième alinéa du I, l'article 45 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié : après les mots : « procédure contradictoire » sont insérés les mots : « et à l'issue d'une audience publique » ;~~	**Supprimé.**
1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en oeuvre par l'Etat ;		
2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.		
II. — En cas d'urgence, lorsque la mise en oeuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :	~~2° Le premier alinéa du II est complété par les mots : « et à l'issue d'une audience publique ».~~	
1° Décider l'interruption de la mise en oeuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en oeuvre par l'Etat ;		
2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;		
3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.		
III. — En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.		
	Article 11	Article 11
Art. 46. — Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la commission mais ne prend pas part à ses délibérations. La commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information.		
La commission peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.	À la deuxième phrase du deuxième alinéa de l'article 46 de la loi n° 78-17 du 6 janvier 1978 précitée, les mots : « en cas de mauvaise foi du responsable de traitement, » sont supprimés.	*(Sans modification).*
Les décisions prises par la commission au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
Conseil d'Etat.		
	Article 12	Article 12
Art. 47. — Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.		
Lors du premier manquement, il ne peut excéder 150 000 Euros. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros.	Au deuxième alinéa de l'article 47 de la loi n° 78-17 du 6 janvier 1978 précitée, le montant : « 150 000 € » est remplacé par le montant : « 300 000 € » et le montant : « 300 000 € » est remplacé (deux fois) par « 600 000 € ».	*(Sans modification).*
Lorsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.		
Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.		
	Article 13	Article 13
	I. — Le chapitre VIII de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :	I. — *(Alinéa sans modification).*
	« Chapitre VIII	*(Alinéa sans modification).*
CHAPITRE VIII		
	« Dispositions relatives aux actions juridictionnelles	*(Alinéa sans modification).*
DISPOSITIONS PÉNALES		
	« Section 1	*(Alinéa sans modification).*
	« Dispositions pénales	*(Alinéa sans modification).*
Art. 50. — Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16	« *Art. 50.* — Les infractions aux dispositions de la présente loi sont réprimées par les articles 226-16 à 226-24	« *Art. 50.* — *(Sans modification).*

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
à 226-24 du code pénal.	du code pénal.	
Art. 51. — Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :	« *Art. 51.* — Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :	« *Art. 51.* — *(Sans modification).*
1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;	« 1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;	
2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;	« 2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;	
3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.	« 3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.	
Art. 52. — Le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions aux dispositions de la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.	« *Art. 52.* — I. — La Commission nationale de l'informatique et des libertés informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance.	
La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience.	« II. — Le procureur de la République avise le président de la Commission de toutes les poursuites relatives aux infractions visées aux articles 226-16 à 226-24 du code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.	
	« Section 2	*(Alinéa sans modification).*

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	« Dispositions civiles	*(Alinéa sans modification).*
	« *Art. 52-1.* — Dans les litiges civils nés de l'application de la présente loi, toute personne peut saisir à son choix, outre l'une des juridictions territorialement compétentes en vertu du code de procédure civile, la juridiction du lieu où il demeurait au moment de la conclusion du contrat ou de la survenance du fait dommageable.	« *Art. 52-1.* — *(Sans modification).*
	« Section 3	*(Alinéa sans modification).*
	« Observations de la Commission nationale de l'informatique et des libertés devant les juridictions civiles, pénales ou administratives	*(Alinéa sans modification).*
	« *Art. 52-2.* — Les juridictions civiles, pénales ou administratives peuvent, d'office ou à la demande des parties, inviter la Commission nationale de l'informatique et des libertés à déposer des observations écrites ou à les développer oralement à l'audience.	« *Art. 52-2.* — *(Alinéa sans modification).*
	« La Commission peut elle-même déposer des observations écrites devant ces juridictions ou demander à être entendue par elles ; dans ce cas, cette audition est de droit.	*(Alinéa sans modification).*
	~~« Dans tous les cas, les observations écrites sont recevables quelle que soit la procédure applicable devant la juridiction saisie. »~~	**Alinéa supprimé.**
Art. 11. — La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ; 2° Elle veille à ce que les traitements de données à caractère personnel soient mis en oeuvre conformément aux dispositions de la présente loi.	II. — Le 2° de l'article 11 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :	II. — *(Sans modification).*

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
A ce titre :		
a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;		
b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;		
c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;		
d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en oeuvre ou envisagent de mettre en oeuvre des traitements automatisés de données à caractère personnel ;	1° Au *d)*, les mots : « et, le cas échéant, des juridictions, » sont supprimés ;	
	2° Le *e)* est ainsi rédigé :	
e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;	« *e)* Elle saisit le procureur de la République et dépose des observations devant les juridictions dans les conditions prévues respectivement aux articles 52 et 52-2. »	
f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;		
g) Elle peut, dans les conditions définies au chapitre VII, prononcer à l'égard d'un responsable de traitement l'une des mesures prévues à l'article 45 ;		
h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;.		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
. . . . .		
Art. 52 et 52-2. — Cf. supra.		
		Article 13 bis (nouveau)
		L'article 72 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		1° Le premier alinéa est ainsi rédigé :
Art. 72. — La présente loi est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.		« La présente loi est applicable sur l'ensemble du territoire de la République française. » ;
Par dérogation aux dispositions du deuxième alinéa de l'article 54, le comité consultatif dispose d'un délai de deux mois pour transmettre son avis au demandeur lorsque celui-ci réside dans l'une de ces collectivités. En cas d'urgence, ce délai peut être ramené à un mois.		2° Au second alinéa, les mots : « de ces collectivités » sont remplacés par les mots : « des collectivités d'outre-mer relevant de l'article 74 ou du titre XIII de la Constitution ».
	TITRE III	TITRE III
	ENTREE EN VIGUEUR DE LA LOI	ENTREE EN VIGUEUR DE LA LOI
	Article 14	Article 14
	La présente loi entre en vigueur six mois à compter de sa publication.	*(Sans modification).*