

**Amendements proposés par DELIS sur le projet de loi relatif 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.
Sénat 2^{ème} lecture**

L'Assemblée nationale a examiné en deuxième lecture jeudi 29 avril le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifiant la loi " informatique et libertés " du 6 janvier 1978.

L'Intercollectif DELIS (Droits et Libertés face à l'Informatisation de la Société) estime que le projet de loi actuel constitue un abaissement très sérieux du niveau de protection des citoyens face aux traitements de leurs données personnelles. DELIS a proposé au gouvernement et aux parlementaires des amendements pour consolider et améliorer les garanties aujourd'hui offertes par la loi.

DELIS attire tout particulièrement l'attention sur les risques que comporte le projet de loi en multipliant les dérogations aux principes fondateurs de la protection des données, que sont : la notification des traitements à la CNIL, la protection des données dites sensibles, le principe de finalité des traitements.

En particulier :

- Affranchir les fichiers soumis à déclaration de toute formalité préalable, dès lors qu'un correspondant aux données a été nommé par le responsable de l'établissement, vide la future loi de toute possibilité de protection des droits des personnes fichées, puisque la CNIL ignorera l'existence de ces fichiers.

- Permettre à des personnes morales, parce qu'elles seraient victimes d'infractions, de tenir des fichiers relatifs aux infractions, condamnations et mesures de sûreté au prétexte de lutter contre la fraude, voire de la prévenir, ouvre la porte à la constitution de véritables casiers judiciaires privés, précédent très dangereux pour les libertés.

DELIS demande au Parlement de rejeter de telles dérives.

DELIS a fait part de ses inquiétudes au rapporteur du projet de loi ainsi qu'aux groupes politiques de l'Assemblée, et leur a adressé les propositions suivantes, qu'elle soumet aux sénateurs avant la seconde lecture au Sénat :

- Maintenir le principe de déclaration préalable de tous les traitements de données personnelles (art. 22, 23 et 24 nouveaux du projet de loi), a fortiori assurer un régime d'autorisation préalable pour les traitements de données susceptibles par leur nature, leur portée ou leur finalité de porter atteinte aux libertés fondamentales ou à la vie privée (art. 25, 26 et 27 nouveaux du projet de loi).

- Élargir la notion de " données sensibles " (art. 8 nouveau du projet de loi) aux caractéristiques génétiques, aux éléments biométriques des personnes et aux données sociales et psychiques touchant à l'intimité de leur vie privée. Faire bénéficier les traitements de " données sensibles " de conditions de protection maximales (consentement exprès de la personne, régime d'autorisation préalable).

- Cantonner le numéro de Sécurité sociale à ses usages actuels ainsi qu'aux traitements ayant pour seule fin d'éviter les erreurs d'identité.

- Encadrer strictement les interconnexions, rapprochements ou toute autre forme de mise en relation entre fichiers, sous contrôle de la CNIL, en les faisant réaliser, s'ils s'avèrent nécessaires, par un organisme indépendant n'ayant aucun intérêt à ces rapprochements ou connexions.

- Proscrire toute réutilisation des données personnelles pour d'autres finalités que celles qui ont présidé à leur collecte initiale (art. 6 nouveau du projet de loi) et les rendre anonymes pour tout traitement statistique, scientifique ou historique associé.

- Renforcer la composition de la CNIL (art. 11 à 21 nouveaux du projet de loi) en y incluant plus de représentants d'usagers et d'organisations de défense des droits de l'homme, et lui attribuer des moyens supplémentaires pour agir en créant des délégations régionales.

DELIS soumet à cet effet les amendements ci-après, actualisés suite au débat et au vote en deuxième lecture à l'Assemblée nationale, avant la deuxième lecture au Sénat, et appelle les sénateurs à adopter ces amendements afin que la loi conjugue, demain comme hier, informatique et libertés.

DELIS – Droits et libertés face à l'informatisation de la société

(Ligue des Droits de l'Homme, Collectif Informatique, Fichiers et citoyenneté, Collectif pour les droits des citoyens face à l'informatisation de l'action sociale, Collectif des associations et des syndicats contre la connexion des fichiers fiscaux et sociaux).

Email DELIS : contact@delis.sgdg.org

Web DELIS: www.delis.sgdg.org

**Amendements proposés par DELIS sur le projet de loi
relatif 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.**

Texte du projet de loi adopté par l'Assemblée nationale en deuxième lecture	Amendements proposés par DELIS	Motivation
<p>La numérotation des articles cités correspond à celle qui figure dans le projet de loi, dans l'ordre des articles de la future loi informatique et libertés telle qu'elle serait modifiée à l'issue de l'actuel processus parlementaire.</p>		

Principe de la finalité : article 6 nv		
<p>“ Art. 6. - Un traitement ne peut porter que sur des données 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 et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;</p> <p>“ 3° (...)</p>	<p>Toutefois, seul 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, s'il recourt à des techniques d'anonymisation à la source des données identifiantes et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; Dans le cas où un traitement ultérieur de données, prévu à l'alinéa précédent, nécessite de disposer d'éléments d'identification directe ou indirecte des personnes concernées, ces éléments d'identification doivent être détruits après la réalisation dudit traitement.</p>	<p>La finalité est le principe fondamental autour duquel s'organisent les autres principes que sont la pertinence, l'adéquation, le caractère non excessif, l'exactitude des données, la loyauté de la collecte, les destinataires, la durée de conservation. Toute réutilisation des données ne doit pas ruiner ce principe fondamental. La Charte européenne des droits fondamentaux à l'art. 8 réaffirme l'exigence d'un traitement “ à des fins déterminées ”. Seul un traitement ultérieur à des fins historiques, scientifiques ou statistiques peut être admis comme non incompatible avec les finalités initiales s'il offre des garanties suffisantes notamment en matière de respect des droits d'information, de rectification et d'opposition des personnes auprès desquelles les données ont été initialement collectées. En plus de ces garanties, un traitement ultérieur à des fins historiques, scientifiques ou statistiques doit être mis en œuvre avec des méthodes garantissant l'impossibilité d'identifier, directement ou indirectement, les personnes auprès desquelles les données ont été initialement collectées. Des principes d'anonymisation ont déjà été mis en œuvre dans le secteur de la Sécurité sociale, de la santé et pour l'exploitation des données relatives au RMI (FOIN, Anonymat...). Toutefois, si le traitement nécessite de disposer de données directement ou indirectement identifiantes (exemple d'études nécessitant un appariement de données), le principe doit être retenu de détruire les éléments d'identification des personnes dès que l'étude a été réalisée.</p>

Principe de la finalité : article 36 nv		
<p>“ Art. 36. - Les données à caractère personnel ne peuvent être conservées (...) de la loi n°79-18 du 3 janvier 1979 précitée. “ Les traitements dont la finalité se limite (...) loi ” “ Il peut être procédé à un traitement ayant des finalités autres que (...) de ce même article. ”</p>	<p>Suppression du 2^e et du 3^e alinéas</p>	<p>Amendement de cohérence avec le précédent.</p>

Etablir dans la loi les modalités de mise en œuvre des interconnexions : au chapitre II section 1 “ dispositions générales ” art. 6 nv		
<p>“ Art. 6. - Un traitement ne peut porter que sur des données qui satisfont aux conditions suivantes : “ 1°(...) “ 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.</p>	<p>Ajouter un 6° ainsi rédigé : “ 6° Lorsqu'elles sont traitées pour faire l'objet d'une interconnexion, celle-ci doit être réalisée par des tierces parties de confiance, n'ayant aucun intérêt à ladite connexion. Les conditions d'application du présent alinéa sont fixées par décret en Conseil d'État pris après avis de la commission ”</p>	<p>Compte tenu de la très forte valeur informationnelle potentiellement générée par une interconnexion de fichiers, nous voulons, qu'obligation soit faite aux parties ayant intérêt à cette interconnexion, de faire réaliser celle-ci en terrain neutre, ce que nous considérons comme une mesure de protection indispensable à l'égard des personnes concernées. Les données, faisant l'objet de l'interconnexion, ne peuvent, en respect de la loi, être traitées qu'aux fins pour lesquelles elles ont été recueillies. Interdiction est donc faite à ces tiers de les utiliser à toutes autres fins et tout particulièrement à des fins commerciales, de plus obligation leur est faite de ne pas conserver lesdites données au-delà du temps nécessaire à la stricte exécution de leur mission. La mise en œuvre de solutions techniques de ce type est opérationnelle depuis plusieurs années en Australie par la Data Matching Agency (DMA).</p>

Données sensibles : article 8 nv		
<p>“ Art. 8. - I. - Il est interdit, sauf consentement exprès de la personne concernée, 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.</p> <p>II.- (...)</p>	<p>“ Art. 8. - I. - Il est interdit, sauf consentement exprès de la personne concernée, 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 aux caractéristiques génétiques des personnes, à leur éléments biométriques, à leur santé, à leur vie sexuelle ou à l'intimité de leur vie privée dans ses composantes psychiques et sociales.</p>	<p>Il convient d'ajouter à la liste des données sensibles devant bénéficier de conditions de protection maximale (par ex. : interdiction de traitement sauf consentement exprès de la personne, autorisation préalable de la CNIL) :</p> <ul style="list-style-type: none"> - les données génétiques qui constituent le “ sanctuaire ” de l'intimité la plus profonde de la personne humaine. Elles sont collectées fréquemment chez le jeune enfant, alors qu'il s'agit souvent d'une collecte dans le cadre de diagnostics prédictifs, et que l'analyse des données ainsi recueillies n'apporte que des arguments de probabilité et non de certitude sur le risque de survenue d'une maladie. Tant du fait de leur nature que du contexte de leur collecte, les données génétiques doivent figurer au titre des données sensibles et le recueil du consentement exprès de la personne ou de son représentant légal est justifié. - les éléments biométriques permettent la mesure et la reconnaissance d'une personne, donc son identification, et soulèvent des problèmes comparables aux caractéristiques génétiques, sachant qu'elles touchent à l'identité-même de la personne. Leur utilisation aux fins de contrôle doit bénéficier des garanties de protection maximales bénéficiant aux données sensibles. - les données relatives à “ l'intimité de la vie privée dans ses composantes psychiques et sociales ”, car elles font l'objet de plus en plus couramment de traitements dans le cadre de l'informatisation de l'action sociale, alors que les appréciations qui y sont portées sur les comportements des personnes touchent à leur identité et à leur intimité, et qu'elles comportent nécessairement une large part de subjectivité. Voir à ce sujet la délibération CNIL n°98-094 du 13/10/98 qui, à propos de typologies sociales, affirme le “ caractère extrêmement sensible de ces informations qui touchent à l'intimité de la vie privée des personnes ” et rappelle leur “ caractère le plus souvent subjectif ”.

Protection des droits des personnes, consentement : art. 8 nv		
<p>“ Art. 8. – I. – Il est interdit, sauf consentement exprès de la personne concernée (...)</p> <p>“ 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 :</p> <p>“ 1°(...)</p> <p>“ 5° 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.</p>	<p>Rédiger le 5° ainsi :</p> <p>“ 5° Les traitements nécessaires aux fins de l'administration de soins dans les situations d'urgence médicale, ou dans celles où la personne n'est pas en mesure de s'exprimer ou ne dispose pas de sa capacité de jugement et qui est 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.</p>	<p>Les données de santé, patrimoine le plus intime des personnes, sont maintenant traitées en réseau et sont sous la pression de la marchandisation. Pour ces données hautement sensibles, le principe du consentement exprès doit être privilégié, et seules les situations d'urgence médicale justifient d'y déroger, ainsi que celles où le patient n'est pas en mesure de s'exprimer ou ne dispose pas de sa capacité de jugement.</p>

Données sensibles : article 9 nv		
<p>“ Art. 9. Les traitements de données relatives aux infractions , condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :</p> <p>1° (...)</p> <p>2° (...)</p> <p>3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi.</p> <p>“ 3° bis 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 I, II et III du même code aux fins d'assurer la défense de ces droits. ”</p>	<p>Supprimer le 3° et le 3° bis de l'article 9 nv</p>	<p>Ces alinéas confient à des personnes morales un droit de création de casier judiciaire, sans aucune garantie (le fait de renvoyer vaguement à “ la loi ” ne veut rien dire en l'espèce). Cela crée un précédent très dangereux pour les Libertés , car cette disposition crée le principe de la constitution de fichiers de police et de relevés de condamnations entre les mains d'organismes dépourvus de mission de service public tels que sont ceux de la Justice et de la Police. Le fait de prévoir un dispositif et de renvoyer à une autre loi les garanties devant y être associées est révélateur de la précipitation avec laquelle cette question de principe est abordée.</p>

Etablir dans la loi le statut du NIR : Chapitre II Section 2 articles 8 nv à 10 nv (dispositions propres à certaines catégories de données) + art 27 nv		
<p>Après les articles 8, 9 et 10 et avant l'article 11 (chapitre III relatif à la CNIL)</p>	<p><i>Insérer un nouvel article ainsi rédigé :</i> <i>“ Le numéro d’inscription des personnes au répertoire national d’identification des personnes physiques destiné à permettre l’identification des personnes est remplacé par un numéro non signifiant.</i> <i>“ Ce numéro ne peut faire l’objet d’un traitement ou de toute autre utilisation, autres que ceux déjà existants et autorisés, qu’aux seules fin d’éviter les erreurs d’identité.</i> <i>“ Les conditions d’application du présent article sont fixées par décret en Conseil d’État pris après avis de la commission ”</i></p>	<p>La transformation du NIR en un identifiant non signifiant apporterait une garantie importante en matière de respect des droits des personnes. En effet, à partir des informations significatives que comporte le NIR, il est à craindre, avec la CNIL, qu’ <i>“ Une utilisation non contrôlée du NIR serait susceptible d’entraîner [...] l’engagement d’actions selon des critères discriminants et non légitimes ”</i>.</p> <p>Il est grand temps qu’à l’instar d’autres pays, tels les Pays-Bas ou la Grande-Bretagne, la France rende le NIR aléatoire et non signifiant.</p> <p>En plus de cela, il est souhaitable de graver dans le marbre de la loi le principe dégagé par le Conseil Constitutionnel selon lequel l’utilisation du NIR ne doit servir qu’à garantir l’identité des personnes et éviter les homonymies, ce qui exclut la possibilité de l’utiliser pour gérer des fichiers, faire des stats, procéder à des interconnexions (DC du 29/12/1998 sur la constitutionnalité de l’article 107 de la loi de finances pour 1999). Ainsi la dangerosité potentielle du NIR, en tant qu’identifiant unique permettant le rapprochement des fichiers et les interconnexions (cf. projet SAFARI) serait-elle écartée, celui-ci ne servant plus à gérer des fichiers ni à faciliter le rapprochement de fichiers.</p> <p>À noter que dans la directive 95/46/CE, le NIR, comme les données sensibles et les données concernant les infractions et les condamnations, est recensé dans une catégorie particulière de données (Art. 8-7 de la directive).</p>

Accroître les pouvoirs juridiques, les moyens et les ressources d'expertises de la CNIL : art. 11 nv à 21 nv		
<p>“ Art. 13. - I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres : (...)</p> <p>“ 6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;</p> <p>“ Art. 19. - La commission dispose de services dirigés par le président et placés sous son autorité. (...)</p>	<p>“ Art. 13. - I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres : (...)</p> <p>“ 6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou pour leur appartenance à la Commission nationale consultative des droits de l'Homme, nommées par décret ;</p> <p>Rédiger le 1^{er} alinéa de l'art. 19 ainsi :</p> <p>“ Art. 19. - La commission dispose de services, comportant notamment un échelon régional, dirigés par le président et placés sous son autorité.</p> <p>Après l'article 21, ajouter un article ainsi rédigé :</p> <p>“ Art. : un comité consultatif auprès de la CNIL est constitué. Il est saisi pour avis des projets d'informatisation les plus sensibles ou portant sur la totalité ou une très grande partie de la population. La composition et les modalités de fonctionnement de ce comité consultatif sont déterminées par décret en Conseil d'État pris après avis de la commission ”.</p>	<p>Pour affirmer la présence de la société civile, nous proposons qu'un ou plusieurs membres de la Commission Nationale Consultative des Droits de l'Homme (CNCDDH) figurent parmi les personnalités qualifiées.</p> <p>La création de délégations régionales de la CNIL démultiplierait sa capacité d'exercer ses missions de contrôle a priori et a posteriori. Notre proposition entrerait en résonance avec la volonté actuelle affichée par le gouvernement de rapprocher des citoyens les moyens d'instruction et de décision.</p> <p>La création d'un comité consultatif auprès de la CNIL vise à ce que les projets d'informatisation d'une certaine envergure soient plus largement portés à la connaissance du grand public qu'actuellement, et que des points de vue plus variés que ceux s'exprimant à ce jour aident à développer des démarches citoyennes dans le domaine de l'informatique et des libertés. La composition de ce comité pourrait s'inspirer de celle de la Commission consultative des droits de l'Homme placée auprès du Premier ministre.</p>

Régime d'autorisation, principe d'une déclaration préalable : article 22 nv

<p>“ Art. 22. – I. – (...) II. – (...) 1° (...) 2° (...) “ Il bis. - 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 État 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. (...)</p>	<p>Supprimer le II bis de l'article 22 nv À défaut, modifier le II bis comme suit : “ “ Il bis. - Les traitements visés à l'article 24.I, 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 État 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 bénéficie de la protection attachée à la qualité de salarié protégé (...)</p>	<p>La création de correspondants à la protection des données à caractère personnel ne peut constituer à elle seule une garantie suffisante pour déroger à toute formalité préalable à la mise en œuvre des traitements, en particulier concernant le respect des obligations prévues à l'art. 6 nv. Aucun élément de garantie ne peut assurer une totale indépendance du correspondant à l'égard de son propre employeur (l'expérience des médecins du travail en atteste).</p> <p>C'est pourquoi DELIS demande la suppression du II bis. Si l'institution de correspondants devait être maintenue lors de la discussion des amendements en deuxième lecture au Sénat, nous proposons deux amendements visant à améliorer la protection des personnes concernées par ces fichiers :</p> <ul style="list-style-type: none"> - en précisant que les traitements visés par la dispense de déclaration correspondent à ceux bénéficiant de normes simplifiées établies par la CNIL, prévues à l'art. 24.I nv. - en assurant au correspondant un statut de salarié protégé, qui lui confère une plus forte garantie d'indépendance vis-à-vis du responsable du traitement <p>En revanche DELIS estime que la généralisation de correspondants de la CNIL, tels qu'ils existent dans les ministères, et si elle n'est pas liée à une dispense de déclaration des traitements, peut favoriser la sensibilisation de tous les acteurs au respect de la loi. Cela pourrait faire l'objet d'un article complémentaire ajouté au chapitre V section I “ obligations incombant aux responsables des traitements ”</p>
--	--	---

Régime d'autorisation, principe d'une déclaration préalable : article 24 nv

“ Art. 24. - I. - Pour les catégories les plus courantes de traitements de données à caractère (...) 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 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.

Suppression du 1^{er} alinéa du II.

et rédaction du 2^e alinéa du II. comme suit :

“ La commission peut autoriser les responsables de certaines catégories de traitements, parmi ceux mentionnés au I, à procéder à une déclaration unique selon les dispositions du II de l'article 23.

DELIS demande la suppression des dispenses de déclaration et appelle à une meilleure utilisation des moyens de communication comme l'internet pour faciliter l'établissement des déclarations ainsi que la mise à disposition de normes permettant des déclarations simplifiées.

Il s'agit principalement par une déclaration fût-elle simplifiée, de sensibiliser les responsables des traitements sur la particularité que revêt un traitement de données personnelles.

Il convient de noter par ailleurs qu'à défaut de déclaration, tant le dispositif de protection des personnes que le dispositif pénal répressif, sont mis en échec.

Régime d'autorisation : article 25 nv		
Article 25 nv	<p>Ajouter au I de l'article 25 un 9° ainsi rédigé : “ 9°- Tout traitement relatif à la vidéosurveillance. ”</p> <p>Ajouter après le I de l'art. 25 nv un I bis ainsi rédigé : “ Des modalités particulières d'autorisation par la Commission nationale de l'informatique et des libertés, pour la mise en œuvre des traitements visés au 5° du II de l'article 8, sont définies par décret en Conseil d'État, pris après avis public et motivé de la Commission nationale de l'informatique et des libertés.</p>	<p>Les traitements relatifs à la vidéosurveillance (enregistrements sur support numérique supplantant les supports analogiques) sont par nature susceptibles de porter atteinte à la protection de la vie privée des personnes (cf. délibération CNIL du 21 juin 1994 sur ce sujet), il doivent pour cela faire l'objet d'une protection particulière et être soumis à autorisation</p> <p>Les données de santé figurent parmi les données sensibles, bénéficiant d'une protection particulière au titre de l'article 8. Les possibilités de traitements de ces données prévues au 5° du II de l'article 8 (que nous proposons d'amender cf. ci-dessus) nécessitent d'être strictement encadrées. A ce titre nous estimons qu'une simple déclaration de ces traitements ne constitue pas une garantie suffisante, mais qu'une procédure particulière d'autorisation doit être prévue qui nécessite a minima l'accord de la CNIL. Compte-tenu du nombre élevé de dossiers concernés (plusieurs centaines de milliers de praticiens et d'établissements de santé mettront en œuvre de tels traitements), cette procédure d'autorisation pourrait être simplifiée par conformité avec une ou plusieurs normes établies par la CNIL. A la différence de la procédure de déclaration simplifiée, l'autorisation en question suppose un examen préalable, fut-il un processus très simplifié, débouchant sur un accord signifié au responsable du traitement dès lors que la conformité du traitement à une norme établie par la CNIL a été vérifiée. Nous proposons que la définition précise de ce processus particulier d'autorisation par la CNIL soit renvoyée à un décret en Conseil d'État.</p>

Régime d'autorisation : articles 26 nv, 27 nv		
Articles 26 et 27 nv	<p><i>Aux articles 26 et 27 nv prévoir un dispositif unique d'autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL, quelle que soit la nature des traitements visés à ces articles. En conséquence, aux alinéas concernés, substituer au dispositif d'autorisation par arrêté ou par décision de l'organe délibérant celui d'autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL.</i></p>	<p>Le régime d'autorisation doit être organisé, selon la nature des traitements, soit sur le principe d'une autorisation délivrée par la CNIL (art. 25 nv), soit sur le principe d'un décret en Conseil d'État pris après avis motivé et publié de la CNIL (art. 26 et 27 nv).</p> <p>En effet, dans le projet de loi, la partition est établie entre trois autorités : le Conseil d'État, la CNIL et le(s) ministre(s) selon la nature des traitements. Outre la complexité qu'introduit cette triple partition, elle comporte l'inconvénient majeur, aux articles 26 et 27 nv du projet de loi (arrêté du ou des ministres compétents), de placer l'autorité ministérielle concernée en situation d'être juge et partie. Cela ne paraît pas souhaitable. C'est pourquoi, la partition que nous proposons (CNIL d'une part pour les traitements " importants ", Conseil d'État d'autre part pour les traitements par nature " dangereux ") offre à notre sens de meilleures garanties du respect de la loi informatique et libertés.</p>