

Document élaboré par la Commission nationale de l'informatique et des libertés
Paris le 14 décembre 2006

Canevas législatif « informatique et libertés »

Introduction et Exposé des motifs

Introduction : pourquoi un canevas législatif ?

Le présent canevas législatif répond à quatre préoccupations :

- concrétiser l'appel lancé par les chefs d'Etat et de gouvernement, lors du X^{ème} sommet de la Francophonie, tenu à Ouagadougou le 27 novembre 2004, en vue de la création ou de la consolidation des règles destinées à assurer la protection des personnes, de leurs libertés et droits fondamentaux dans l'utilisation des fichiers et traitements de données à caractère personnel. Cet appel était accompagné d'un encouragement à la coopération entre les autorités indépendantes nationales chargées de l'application de ces règles (déclaration finale, point 51). Cet appel a été renforcé lors du XI^{ème} sommet, tenu à Bucarest le 24 septembre 2006 (déclaration finale, point 59), par l'engagement pris par les chefs d'Etat et de gouvernement d'intensifier dans ce domaine les travaux législatifs et réglementaires nécessaires ;
- favoriser un rapprochement des législations (harmonisation) en vue de contribuer à l'effectivité de ce droit dans les échanges transfrontaliers de plus en plus nombreux, en proposant un système de protection considéré comme minimal.
Fondé sur les instruments régionaux et internationaux existant ainsi que sur les expériences nationales, il fournit, entre crochets, des options pour l'adaptation du texte en fonction de l'expérience acquise, de la diversité des systèmes juridiques et institutionnels ainsi qu'en fonction des particularismes culturels ;
- répondre aux demandes nationales visant à disposer d'un texte de référence dans le cadre de la préparation d'une loi fondamentale consacrant le droit des personnes à la protection des données personnelles, rédigé de manière compréhensible ;
- donner écho au texte de réflexion publié par la conférence internationale de Londres (3/11/2006) mettant en lumière les évolutions technologiques et législatives en cours et la nécessité de renforcer la coordination et les moyens des autorités indépendantes chargées de la protection des données personnelles.

Exposé des motifs

Pourquoi reconnaître et instituer le droit à la protection des données personnelles ?

En vue de la modernisation des services publics mais aussi du développement économique, nombreux sont **les projets ou programmes nationaux** qui reposent sur l'utilisation de l'informatique et ses développements technologiques désignés communément sous les termes de **technologies de l'information et de la communication**.

L'utilisation de l'informatique permet, en effet, **des gains de temps et de productivité sans précédant ainsi que plus de rigueur dans la gestion quotidienne**. Elle permet également d'offrir à distance des services nouveaux, sur le plan national comme sur le plan international.

Les progrès technologiques sont rapides, en particulier la puissance des ordinateurs double tous les 18 mois à coût constant grâce à la miniaturisation, et l'extension de la numérisation des réseaux est de nature à faire baisser les coûts de communication.

Il convient cependant, à côté de ces bénéfices attendus de l'usage de ces technologies, de considérer, dans toute démocratie tournée vers le progrès et le développement, avec la même objectivité, **les risques que ces technologies**, si elles ne sont pas encadrées par l'établissement de principes directeurs et droits individuels nouveaux, **font peser sur les libertés des personnes concernées**.

En effet, les informations relatives aux personnes contenues dans un fichier peuvent être conservées pour de longues durées et lorsqu'elles sont informatisées ou numérisées, elles peuvent être aisément rapprochées avec d'autres, être l'objet de détournement de la finalité pour laquelle elles ont été collectées, copiées ou manipulées à l'insu des personnes concernées.

Le fonctionnement des réseaux numériques de communication actuels génèrent des traces des actes posés par toute personne en toute occasion: qui communique avec qui ? Quel site internet de toute nature, administrative, politique, caritative a été consulté ? Où se trouve le téléphone portable connecté ? Les usages des services offerts sur ces réseaux conduisent également les personnes à fournir des traces, par exemple des achats effectués à distance. Toutes ces informations touchent au droit à la vie privée ou aux libertés fondamentales notamment de s'informer, de penser, de communiquer, d'aller et venir.

Des puces électroniques peuvent être intégrées, et le seront demain de plus en plus, aux objets distribués et possédés. Selon les travaux menés dans les laboratoires de recherche et de développement et dans un futur proche, elles dialogueront entre elles. Avec l'accord des personnes concernées ou à leur insu ? Combien de temps ? Voilà des questions que tout un chacun doit se poser aujourd'hui.

Pour répondre à ces défis qui concernent tous les secteurs d'activités, a émergé depuis quelques décennies un régime de protection des personnes qui leur reconnaît un nouveau droit personnel fondamental, celui du droit à la protection des données personnelles.

Compte tenu du **caractère tout à la fois national et international** des technologies en cause, les pays qui ont institué ce droit ont le plus souvent adopté également des règles, en accord avec les règles de l'OMC (article XIV des accords du GATT), destinées à assurer **la poursuite de la protection en cas de transfert de données vers des pays étrangers**. Il en est ainsi par exemple des pays de l'Union européenne et du Canada.

A l'heure actuelle 45 pays au monde ont consacré dans leur législation ce droit, dont une vingtaine au sein de l'Organisation Internationale de la Francophonie.

Dans ce contexte, il convient tout à la fois de **combler le vide juridique et d'harmoniser les législations parcellaires**. Une telle harmonisation doit se concevoir « **par le haut** » puisque le domaine relève des libertés et droits fondamentaux.

Comment assurer le droit à la protection des données personnelles ?

Le présent canevas législatif incorpore les textes adoptés au sein de différentes enceintes régionales ou internationales, les principes directeurs pour la réglementation des fichiers adoptés par l'Assemblée générale de l'ONU en 1990, les lignes directrices de l'OCDE adoptées en 1980, la convention 108 du Conseil de l'Europe adoptée en 1981, la directive européenne 95/46 de 1995 et la charte des droits fondamentaux de l'Union européenne adoptée en 2000.

Toutefois, le canevas proposé adapte ces textes. En effet, s'ils établissent des principes compatibles entre eux, ils sont diversement développés ou contraignants et utilisent parfois des concepts différents. Par ailleurs le domaine dans lequel ces instruments sont le moins développés est celui des missions et pouvoirs de l'autorité indépendante chargée d'en assurer le respect. Pourtant, le principe de sa création est posé dans le texte de l'ONU et développé dans les textes européens ainsi que surtout sur le plan national en Europe et hors d'Europe, par exemple au Canada, en Australie, en Nouvelle Zélande, au Burkina Faso.

C'est pourquoi le présent canevas de législation se fonde sur les instruments régionaux et internationaux les plus récents, ainsi que sur les expériences nationales acquises tout particulièrement en matière de missions et pouvoirs de l'autorité de contrôle ainsi qu'en matière de sanctions.

Quelle législation ?

Le régime juridique vise à protéger les personnes contre les risques d'abus en matière de fichier et de traitement de données personnelles au regard de leurs libertés et droits fondamentaux. Cet objectif fait l'objet d'un préambule sous la forme d'un article préliminaire.

La protection repose de manière classique sur quatre piliers : les principes fondamentaux qui doivent présider à la conception et à la mise en œuvre des traitements de données personnelles et qui sont de nature à prévenir les abus, les droits des personnes, l'autorité indépendante et le régime des sanctions.

Le canevas de législation traite de chacun de ces thèmes dans l'ordre suivant :

Le chapitre I circonscrit le champ d'application et définit les termes utilisés.

Le chapitre II établit l'ensemble des principes fondamentaux ou règles de nature à prévenir les risques d'abus qui doivent être respectés par toute personne utilisant des données personnelles.

Le chapitre III consacre les droits des personnes concernées par les traitements des données personnelles et des utilisations qui en sont faites.

Le chapitre IV institue une autorité publique indépendante chargée de s'assurer que les traitements de données ne portent pas atteinte aux droits et libertés des personnes.

Le chapitre V est dédié au délégué à la protection des données personnelles qui constitue un mode complémentaire de mise en œuvre de la législation déjà adopté par plusieurs Etats.

Le chapitre VI définit le régime des sanctions.

Le chapitre VII porte sur les dispositions transitoires et finales.

Article préliminaire

En préambule est assigné à l'informatique, c'est-à-dire aux **technologies destinées au traitement et à la communication de l'information** quel qu'en soit le procédé, **le double objectif** d'être **au service de chaque personne** et de **respecter l'identité humaine, les libertés et droits fondamentaux** des personnes, en particulier le droit à la vie privée. Ce double objectif qui est de nature à guider l'action de chacun constitue un choix de société humaniste. Il constitue, également, une incitation, pour l'industrie des technologies de l'information et de communication, à fournir des produits matériels et logiciels de nature à contribuer à sa réalisation.

Le droit à la protection des données personnelles est reconnu à toute personne quelle que soit sa nationalité. Il s'agit **d'un droit autonome qui fait partie intégrante des droits de l'homme** et qui est **cardinal à l'heure de la société dite de l'information**.

Dans ce contexte, la caractéristique de l'informatique, la plus novatrice au regard des technologies, qui est de permettre de traiter de manière automatique des informations selon des modèles qui peuvent être très sophistiqués, conduit à poser **une limite à la tentation de la prise de décision automatique vis à vis des personnes concernées**. On songera, par exemple, à certaines études anciennes sur la prise d'une décision de justice de manière automatique, ou à des décisions de rejet de demande de crédit fondé sur le seul résultat d'un calcul de score.

Pour prévenir le risque d'une décision arbitraire fondée sur un modèle statistique, le principe est posé selon lequel aucune décision ne doit pouvoir être opposée à une personne lorsqu'elle est prise sur le seul fondement d'un traitement informatique définissant son profil ou évaluant certains aspects de sa personnalité.

La variété et la complexité des traitements de données personnelles, leur mise en œuvre à l'aide de matériels sophistiqués et sous forme codée, leur impact structurant pour la société et l'évolution très rapide des technologies, impliquent que pour assurer **le respect des règles de ce droit soit instituée une autorité spécialisée et indépendante**.

Chapitre I - Champ d'application et définitions

L'article 1 porte sur le champ d'application. Le caractère horizontal de l'usage de l'informatique conduit à ce que les risques présentés soient de même nature **quel que soit que le secteur d'utilisation**. Dès lors le régime de protection doit s'appliquer dans tous les cas où des données personnelles font l'objet **d'un fichier ou d'un traitement**, c'est-à-dire dans tous les cas où des données sont collectées, détenues et utilisées par d'autres personnes que celle concernée.

Les traitements visés sont **opérés en tout ou partie sur le territoire national**. Compte tenu de la mondialisation, ce critère de rattachement à la loi nationale permet d'assurer la protection des personnes concernées par des traitements opérés à l'étranger à partir d'une collecte de données intervenue sur le territoire national. Ce critère permet à la loi de s'appliquer, à l'inverse, lorsque le traitement porte sur des données collectées à l'étranger et exploitées sur le territoire national.

Si le phénomène déclencheur du besoin de protection a été l'informatisation et la constitution de fichiers numérisés de données personnelles, il n'en demeure pas moins que la coexistence de fichiers manuels peut faire peser des risques de même nature aux personnes concernées, par exemple lorsqu'ils sont tenus à leur insu ou si les données qu'ils contiennent ne sont pas à jour. De plus, réglementer les seuls traitements informatisés présenterait le risque de laisser se développer des situations illégales au moyen de fichiers manuels. C'est pourquoi le régime de protection doit s'appliquer tant aux **traitements de données personnelles informatisés en tout ou en partie** qu'à ceux portant sur **des données conservées dans un fichier manuel**.

Le droit à la protection des données personnelles et la législation qui le consacre ne doit cependant pas faire obstacle, sous peine de contradiction, à l'exercice de deux autres libertés et droits fondamentaux.

Ainsi le régime de protection **ne s'applique** pas aux fichiers et traitements mis en œuvre au titre de la **vie privée** car chacun a le droit, sans limitation, à disposer de données pour son usage personnel.

Le régime de protection ne doit pas non plus s'appliquer aux traitements liés à la liberté d'expression. En effet l'exercice de la liberté d'expression est régi par d'autres lois qui protègent les personnes par des mesures adaptées complétées par des codes de déontologies. Par exemple l'injure est interdite et le droit de réponse est institué en matière de presse écrite et audiovisuelle.

Les articles 2 à 5 définissent les termes utilisés

Une donnée personnelle est toute information qui se rapporte à une personne identifiée ou qui peut être identifiée. Cette définition très large qui couvre les données sous forme de texte, d'image ou de son, répond également aux situations où un simple numéro attribué à une personne ou à un bien qu'elle possède permet de l'identifier, par exemple son numéro de téléphone ou celui de la plaque numérotique de sa voiture. De même, en l'absence de son nom, la réunion de plusieurs données se rapportant à une personne peuvent permettre, à celui qui les détient ou à un tiers à qui elles seraient communiquées, de l'identifier. C'est le cas, par exemple, de la profession, l'adresse, l'âge, le sexe et le nombre des enfants. Plus généralement de telles informations sont relatives à des éléments physiques, physiologiques, psychiques, économiques, culturels ou sociaux.

Un traitement de données personnelles comprend chacune des opérations qui peuvent être opérées sur de telles données et tout ensemble, ou processus, de ces opérations depuis leur collecte, jusqu'à l'élaboration d'un résultat par calcul et la communication de ces données par exemple à des tiers. Ainsi, sont en pratique concernées les opérations destinées à la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, l'élaboration ou la modification, l'extraction, la consultation, l'utilisation, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Un fichier est un ensemble structuré et stable de données personnelles accessibles selon des critères déterminés. Il peut s'agir, par exemple, d'un fichier manuel constitué de dossiers du personnel d'une entreprise accessibles par le nom du salarié ou par la dénomination du service dans lequel il est affecté.

Le responsable du traitement est toute personne ou organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens à mettre en œuvre. Cette définition répond à la préoccupation que la responsabilité soit établie non seulement lorsqu'un traitement est mis en œuvre par un responsable unique, par exemple un département ministériel, mais également lorsqu'un traitement répondant à une finalité commune est établi en commun par plusieurs entités.

Les sous-traitants sont les personnes extérieures au responsable de traitement, choisies par celui-ci mais qui traitent les données selon ses instructions et non pour leur propre compte.

Le consentement de la personne concernée, lorsqu'il est requis s'entend de toute manifestation positive de volonté, libre, spécifique et informée.

Chapitre II - Les principes fondamentaux

Les principes fondamentaux, ou règles de nature à prévenir les risques d'abus, sont ceux qui doivent être mis en œuvre lors de la conception et de l'utilisation des données personnelles. Ils comprennent des principes généraux ainsi que des principes complémentaires relatifs à des données et traitements exigeant un régime de protection renforcée ou particulière.

L'article 6 définit les principes généraux. Ils ont trait aux obligations relatives au caractère loyal de la collecte et des traitements des données, à la finalité légitime poursuivie par ces opérations, à la proportionnalité des données traitées et conservées au regard de la ou des finalités poursuivies, à la mise à jour des données, à leur sécurité et à celle des traitements opérés.

La légitimité de la finalité d'un traitement s'appréciera au regard, par exemple, des obligations légales auxquelles il répond, de la mission de service public confiée au responsable du traitement, de l'accord donné par la personne concernée, par exemple pour répondre à une enquête de consommation.

Les principes ainsi énumérés, ne font pas obstacle à la conservation de données et à leur réutilisation, au-delà de la période nécessaire à la finalité du traitement ou du fichier, à des fins d'archives, de recherches historiques, statistiques ou scientifiques sur le fondement et selon les garanties définies par les législations pertinentes et (ou), si nécessaires, dans les conditions définies par l'Autorité indépendante.

Les obligations de sécurité prévues à l'article 7 incombent au responsable du traitement et sont des obligations de moyen au regard de l'évaluation des risques présentés par le traitement, notamment du fait de son architecture en réseau. Ces obligations concernent également le sous-traitant qui doit être choisi pour ses bonnes pratiques en la matière. Ces obligations doivent empêcher notamment que les données soient déformées, endommagées ou que des tiers, qui n'ont pas à en connaître, en aient communication.

Ces principes généraux ne font pas obstacle à ce que les **autorités légalement habilitées** dans le cadre d'une **mission particulière d'enquête ou de contrôle** puissent demander au responsable du traitement de leur communiquer les données personnelles correspondantes.

Les principes complémentaires prévus aux articles 7 à 9 sont relatifs à trois catégories de traitements particuliers de données personnelles. Il s'agit des traitements de données sensibles, des traitements d'infractions ou condamnations et des transferts de données personnelles vers l'étranger.

Le régime des traitements portant sur des données sensibles (article 8)

Le traitement de données sensibles, telles que, par référence aux principes directeurs de l'ONU et à la convention 108 du Conseil de l'Europe, l'origine raciale, les opinions politiques, les convictions religieuses, l'appartenance syndicale et celles qui se rapportent à la santé ou à la vie sexuelle des personnes, est interdit parce que susceptible de conduire à des discriminations. Toutefois, des traitements de ces données peuvent être mis en œuvre si des garanties particulières sont établies au cas par cas, en fonction de la légitimité des finalités poursuivies, ainsi que des conditions de leur mise en œuvre. Par exemple, les données médicales peuvent être collectées mais sont soumises au secret professionnel. La diversité des situations conduit à confier le soin de définir les garanties à l'autorité indépendante qui tiendra compte dans cet exercice du droit en vigueur par ailleurs.

La loi peut également prévoir des exceptions au bénéfice des associations et autres organismes à but non lucratif, à caractère religieux, philosophique, politique ou syndical en ce qui concerne les traitements qu'ils mettent en œuvre à la seule fin la gestion de leurs membres ou de leurs contacts réguliers.

La liste des données sensibles relève parfois également de la diversité culturelle et doit être adaptée dans ce contexte.

Le régime des traitements portant sur des données relatives aux infractions et condamnations (article 9)

Pour éviter que les données relatives aux infractions et condamnations ne soient opposées aux personnes de manière indue, par exemple lorsque la peine est accomplie ou lorsque la condamnation est amnistiée, le principe est que seuls peuvent procéder à leur traitement les juridictions et autorités publiques gérant un service public agissant dans le cadre de leurs attributions légales, les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi, les autres personnes morales, pour les stricts besoins de la gestion des contentieux relatifs aux infractions dont elles ont été victimes.

Le régime relatif aux transferts de données personnelles vers l'étranger (article 10)

Afin que la protection assurée sur le plan national ne soit pas contournée en cas de transfert de données vers l'étranger, il est nécessaire que celui-ci ne soit autorisé que si la protection assurée dans l'Etat destinataire est suffisante. Ce sera le cas lorsque la législation de cet Etat est d'effet équivalent à la législation nationale. Ce peut être également le cas lorsque le destinataire présente des garanties, notamment du fait des clauses contractuelles ou conventionnelles liant l'émetteur et le destinataire à propos du traitement qui sera opéré chez ce dernier, ou des règles internes à l'entreprise qui y sont respectées.

Une telle approche est, de plus, une condition posée par de nombreux pays déjà dotés d'une législation craignant qu'un transfert vers l'étranger ne donne lieu à des transferts ultérieurs vers d'autres pays étrangers sans que la protection des données ne soit assurée.

Il convient de confier l'exercice très spécifique de l'évaluation du caractère suffisant de la protection assurée à l'Autorité indépendante.

Chapitre III - Les droits des personnes

La facilité avec laquelle il est possible de collecter, de conserver et d'utiliser des données, et dans nombre de situations quotidiennes (établissement d'un bulletin de paie, de feuille d'imposition, de relevé de compte bancaire etc.) conduit à conférer aux personnes un droit de contrôle sur les données qui les concernent.

De manière opérationnelle, **ce droit individuel de contrôle se décompose en plusieurs droits** : droit des personnes d'être informées sur l'usage des données qui les concernent, droit de s'opposer le cas échéant à l'usage des données, droit d'accès et de rectification des données. Le droit d'être informé est en pratique une condition à l'exercice des autres droits dont il convient de connaître le contenu au préalable. C'est pourquoi il est prévu de traiter des droits d'opposition, d'accès et de rectification avant de traiter du droit à l'information.

L'article 11 consacre le droit des personnes à s'opposer, pour des motifs légitimes, à l'utilisation de leurs données. Toutefois, en cas de réutilisation de l'adresse des personnes à des fins de prospection il n'est pas besoin d'invoquer un motif légitime. La prospection visée concerne toutes les formes de prospection quelle qu'en soit la nature, commerciale, caritative ou politique. De nombreux Etats, tels les Etats membres de l'Union européenne et l'Australie, ont renforcé cette protection en exigeant le consentement préalable de la personne lorsque la prospection est adressée par un moyen électronique, par exemple par e mail ou par SMS.

L'article 12 organise le droit d'accès, de rectification et de suppression, c'est-à-dire le droit pour la personne de savoir si elle est concernée par un traitement, de connaître et d'obtenir copie des **informations détenues sur elle** sous une forme intelligible, de faire rectifier ou compléter les données qui sont périmées ou incomplètes, de les faire supprimer le cas échéant.

La complexité de certains traitements conduit également à reconnaître à toute personne **le droit de connaître les raisonnements utilisés dans les traitements informatisés** dont les résultats lui sont opposés.

Il convient dans ce contexte de traiter des cas où une limite à l'exercice du droit d'accès est nécessaire. Il s'agit de l'accès aux données relevant de **la sûreté**, de **la défense nationale** ou de **la sécurité publique**. En effet la révélation de telles données peut être de nature à mettre en péril l'intérêt pour lequel elles sont nécessaires. Le texte propose, à **l'article 12 bis entre crochets**, une méthode mise en œuvre dans plusieurs pays européens et destinée à s'assurer que l'évaluation de la mesure restrictive d'exercice de ce droit fondamental sera effectuée au cas par cas. Elle consiste à prévoir un mode d'exercice de ce droit de manière indirecte, par l'intermédiaire de l'Autorité indépendante qui, consultant le fichier concernant la personne, en effectuera un contrôle et proposera au responsable du traitement soit de communiquer les données à la personne concernée, soit de refuser la communication lorsque celle ci porterait atteinte à l'intérêt en cause. La décision est prise par le responsable de traitement.

L'article 13 consacre le droit d'être informé.

Ce droit est essentiel pour assurer la confiance. Ainsi la personne pourra en toute connaissance de cause communiquer les informations qui lui sont demandées, par exemple par une entreprise ou une administration, et savoir comment exercer ses droits par la suite.

Les informations essentielles dont doit disposer la personne dans ce contexte sont les suivantes : l'identité du responsable du traitement, la finalité poursuivie par le traitement, le caractère obligatoire ou facultatif des informations qui lui sont demandées, les destinataires des données, les modalités d'exercice de ses droits d'opposition, d'accès et de rectification, [*le cas échéant, des transferts de données personnelles envisagés à destination d'un État n'assurant pas un niveau de protection suffisant*].

Le principe de loyauté de la collecte des données implique que ces informations soit portées à la connaissance de la personne sous une forme compréhensible au moment de la collecte des données, sur des formulaires papiers ou électroniques.

La disposition relative à ce droit est rédigée afin que son application soit adaptée à diverses circonstances de collecte des données. La collecte des données peut en effet être effectuée par un autre moyen que celui d'un formulaire, par téléphone par exemple. De même il convient de tenir compte de situations plus complexes comme celles, par exemple, d'un fichier sur les incidents de remboursement de crédits dont le responsable est un organisme central, tel qu'une banque centrale. Dans ce cas l'information sur l'existence d'un tel fichier pourrait être effectuée par l'organisme de crédit au moment de la demande de crédit, et en cas de défaut de paiement, préalablement à l'inscription de la personne dans le fichier des incidents.

Chapitre IV – L'Autorité indépendante

Ce chapitre institue l'autorité indépendante chargée de veiller à l'application des dispositions de la législation.

Le présent canevas législatif propose, compte tenu des évolutions rapides et structurantes des traitements de données personnelles y compris sur le plan international, **un modèle d'autorité généraliste** qui rend compte de son activité devant les pouvoirs publics et qui est **dotée d'une panoplie de pouvoirs d'intervention** lui permettant d'**orienter son action en vue de garantir l'effectivité de la protection**. Ainsi, elle doit pouvoir **donner des conseils lorsque de nouvelles technologies apparaissent, intervenir de manière sélective préalablement** à la mise en œuvre des traitements qui présentent le plus de risques pour les personnes. Elle doit pouvoir également **régler de manière amiable** de nombreuses plaintes qui n'ont pas un caractère grave. En revanche, elle doit pouvoir **prononcer des sanctions lorsque les atteintes aux droits des personnes sont graves et coopérer avec ses homologues étrangers** en étant en mesure de leur transmettre une plainte. Inversement, l'autorité doit être en mesure d'utiliser ses pouvoirs d'investigation et de sanction vis à vis d'acteurs mettant en œuvre, sur son territoire, des traitements de données concernant des personnes ne résidant pas sur son territoire (cas de nombreux spams, par exemple).

Le chapitre consacré à l’Autorité indépendante est divisé **en trois sections** relatives aux modalités de constitution de l’autorité, à ses pouvoirs, missions et moyens (section 1), aux procédures relatives à la mise en œuvre de ses pouvoirs en matière de création de traitement (section 2) et en matière de contrôle sur place des traitements mis en œuvre (section 3). La question des sanctions est traitée au chapitre suivant.

La Section 1 est consacrée à la création de l’Autorité indépendante

Les articles 14 et 15 portent sur l’indépendance et la composition de l’Autorité

Compte tenu de ses pouvoirs vis-à-vis tant d’organismes publics que d’organismes privés, l’Autorité doit être un organisme indépendant. Il peut être, soit un organisme indépendant exerçant une mission de service public, soit une autorité publique.

Il est proposé que cet organisme soit de nature collégiale et pluraliste, et que son président soit élu par le collège. Une telle approche, de même que l’origine, les compétences, le mode de désignation et le statut de ses membres, constituent des éléments de nature à assurer l’indépendance nécessaire de l’organisme, l’impartialité et l’autorité de ses décisions.

Sans que soit précisé, dans ce canevas législatif, le nombre et les modalités de désignation des membres de cet organisme indépendant, questions qui relèvent du choix des autorités qui élaborent une telle législation, **il est recommandé que leur origine reflète la diversité de la société et que leurs compétences concernent les technologies de l’information et les libertés individuelles.**

L’inamovibilité pour la durée du mandat, de même que l’incompatibilité avec une fonction de membre du gouvernement de ses membres constituent également des conditions nécessaires à l’indépendance de l’autorité. S’agissant des incompatibilités, la fonction de direction dans une personne morale, publique ou privée, doit être examinée au regard des conflits d’intérêt.

Il n’est pas nécessaire que l’ensemble des membres de l’Autorité soient permanents. **Cependant, l’indemnisation des membres pour la participation aux travaux de l’Autorité, la disponibilité et le montant suffisant d’un budget alloué sur le budget de la Nation constituent également des éléments de nature à assurer l’indépendance de l’autorité.**

Il peut être prévu que certaines des ressources de l’autorité proviennent soit de certaines de ses activités, par exemple des déclarations de traitements effectuées devant elle, soit de subventions d’organismes internationaux dont l’Etat est membre. La régularité des comptes de l’Autorité indépendante est soumise au contrôle de l’organe compétent en matière de comptabilité publique. Les comptes de l’Autorité indépendante et le bilan de son activité sont présentés au Parlement lors d’une séance publique.

L’article 16 prévoit les missions de l’Autorité. Celles-ci sont étendues et concernent l’information du public sur les droits et obligations, le conseil, le contrôle des traitements de données personnelles, la dénonciation des infractions pénales, le cas échéant le prononcé de sanctions, la veille en matière de nouvelles technologies, la contribution aux négociations internationales ayant une incidence sur des traitements de données personnelles, la coopération avec les autorités homologues instituées dans d’autres Etats, la concertation avec les autres autorités indépendantes en matière de libertés publiques.

L'article 17 précise les pouvoirs de l'Autorité qui concernent la réception des déclarations de traitement de données personnelles et la tenue, à la disposition du public, de la liste des traitements déclarés ou autorisés, le contrôle de ces derniers avant leur mise en œuvre dans les cas prévus par la législation, la réception et l'instruction des plaintes des particuliers, le contrôle sur place des traitements mis en œuvre.

Les personnes intéressées par la création ou la mise en œuvre de traitements doivent faciliter la tâche de l'Autorité en lui communiquant les informations qu'elle demande.

Pour aider les responsables de traitements dans l'accomplissement de leur tâche, il est prévu de conférer à l'Autorité un pouvoir réglementaire de nature à simplifier leur démarche notamment dans les cas où la loi a prévu qu'elle autorise des traitements. De même elle peut prévoir, par voie réglementaire, que certaines catégories de traitements sont exonérées de déclaration.

Afin de faciliter l'exercice des droits des personnes, il est prévu de conférer à l'Autorité un pouvoir réglementaire.

Il est prévu que les décisions administratives prises par l'autorité sont susceptibles d'un recours devant la juridiction compétente.

L'article 18 prévoit les moyens de l'Autorité

L'autorité doit être dotée de services qu'elle organise librement. Elle doit pouvoir établir des bureaux répartis sur l'ensemble du territoire notamment lorsque celui ci est étendu ou dans le cadre d'un Etat fédéral.

Il est prévu que les membres et agents de l'Autorité sont tenus au secret professionnel pour les informations qu'ils ont à connaître dans l'exercice de leurs fonctions. On songera notamment aux circonstances dans lesquelles du fait d'un contrôle sur place ils peuvent avoir à connaître de données couvertes par le secret médical ou par le secret bancaire. En revanche, un tel secret ne peut être opposé aux membres et agents de l'Autorité sous peine de les empêcher d'accomplir leurs missions.

La Section 2 organise le régime juridique des formalités relatives à la création des traitements

Pour répondre aux craintes liées aux usages des données numérisées à l'insu des personnes, **l'article 19 prévoit le principe que tout traitement de données personnelles est déclaré** à l'Autorité qui en tient la liste à la disposition du public selon la mission qui lui est confiée. Cette formalité est cependant limitée à ceux des traitements qui sont informatisés en tout ou en partie.

Lorsque la loi le prévoit, en raison notamment de l'importance en nombre des traitements et des responsables de traitements sur le territoire et de l'expérience acquise, le registre des traitements relevant d'un même responsable de traitement peut être tenu par le délégué à la protection des données personnelles qu'il aura désigné (voir chapitre V).

L'article 20 prévoit la possibilité de dispense de déclaration.

Pour prévenir le développement d'une bureaucratie contraignante, il y a lieu de prévoir que les traitements les plus courants, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés peuvent être dispensés de déclaration.

Cette dispense, selon le degré d'encadrement juridique des traitements en cause, tels ceux dont la finalité est la tenue d'une comptabilité ou celle d'établir la paie du personnel, peut être décidée par la loi ou par l'autorité de contrôle en fonction de l'expérience acquise.

Par ailleurs, afin d'éviter une ingérence dans l'exercice de la liberté d'association, une dispense peut être également prévue pour les associations à but non lucratif à l'égard des traitements portant gestion de leurs membres et de leurs correspondants réguliers.

L'article 21 définit les traitements nécessitant l'autorisation ou l'avis préalable de l'Autorité.

Certains traitements sont de nature à présenter des risques particuliers pour les droits et libertés en raison soit de leur portée, soit des données sur lesquels ils portent, soit de leur modalité ou de leur finalité.

Il convient d'établir la liste des critères dans la législation ainsi que d'en prévoir le régime. De tels traitements peuvent en effet être soumis, selon les cas, soit à l'autorisation préalable de l'Autorité, soit à un acte réglementaire adopté après avis de l'Autorité.

Les traitements qui peuvent présenter des risques sont ceux qui :

- concernent une large partie de la population, tel un fichier central de recensement de population ;
- utilisent des informations qui favorisent potentiellement les interconnexions tel un identifiant national ;
- peuvent discriminer une personne relativement à une autre, à l'instar des données génétiques ou des données biométriques ;
- portent sur des données sensibles dont l'usage est interdit, telles l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, l'appartenance syndicale et celles qui se rapportent à la santé ou à la vie sexuelle des personnes ;
- intéressent la sûreté de l'État, la défense ou 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 ;
- reposent sur l'interconnexion de fichiers ou de traitement correspondant à des intérêts différents ;
- sont susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat. Par exemple en matière d'octroi de crédit les traitements qui reposent sur l'usage de logiciels de modélisation des comportements pour établir un score de capacité de remboursement ou ceux qui concourent à l'établissement d'un fichier commun à plusieurs organismes financiers les incidents de remboursement ;
- comportent un transfert de données vers un pays tiers n'assurant pas une protection suffisante. Dans ce cas la décision de l'Autorité sera fonction des garanties apportées par le déclarant sur les conditions de mise en œuvre du traitement par le destinataire. Ces garanties peuvent tenir, en particulier, aux clauses contractuelles liant le responsable du transfert et le destinataire des données ou les règles internes observées chez le destinataire. Dans certains cas, l'Autorité pourra autoriser de tels transferts sans que le formalisme indiqué ci dessus soit requis.

Selon la répartition des pouvoirs entre l'exécutif et le législatif, certains traitements de données personnelles peuvent être créés par voie législative ou réglementaire. Il est prévu, dans ces cas, que les projets des dispositions concernées sont soumis à l'avis préalable de l'Autorité accompagnés d'un document, exposé des motifs ou étude d'impact, lui permettant d'apprécier le contexte, l'ampleur et la nature des résultats attendus.

Il doit en outre être prévu un délai maximum au terme duquel l'Autorité doit se prononcer. Celui-ci pourrait être de deux mois renouvelable une fois.

L'article 22 prévoit que **les modalités et le contenu de la déclaration d'un traitement** sont fixés par l'Autorité. Le responsable de traitement est tenu de mettre à jour la déclaration de son traitement en fonction des évolutions de celui-ci et de sa suppression éventuelle.

Une déclaration comportera toutes les caractéristiques permettant d'identifier le responsable d'un traitement et d'apprécier, comment les principes fondamentaux sont appliqués au cas d'espèce : outre les données relatives à l'identité du responsable du traitement, seront indiqués la ou les finalités du traitement, les données personnelles collectées et enregistrées, leur origine et leur durée de conservation, les personnes habilitées à accéder aux données ou pouvant en obtenir communication, les transferts de données personnelles à destination d'autres États, les mesures envisagées pour assurer la sécurité du traitement.

Une telle description, qui est utile au déclarant en vue d'évaluer lui-même la mesure dans laquelle il a tenu compte des principes fondamentaux, pourra être établie, adaptée, voire simplifiée par l'Autorité selon différentes catégories de traitements dans le cadre de l'exercice de son pouvoir réglementaire.

La Section 3 détermine les modalités d'exercice des pouvoirs de contrôle sur place de l'Autorité

L'article 23 introduit le **principe de l'habilitation des membres et agents** de l'Autorité participant aux missions de contrôle. Les modalités d'une telle habilitation pourront, par exemple, être prévues par le règlement intérieur de l'Autorité.

Les personnes chargées d'un contrôle doivent pouvoir avoir accès à toutes les informations nécessaires à leur mission. Il en est ainsi de l'accès aux fichiers, traitements, matériels utilisés et documentations les concernant.

Les droits de la défense conduisent à prévoir qu'un procès verbal de la mission est établi et adressé au responsable du traitement pour observations.

Il n'est pas utile de prévoir une information préalable du contrôlé qui pourrait ainsi s'organiser pour dissimuler des informations. Il convient, en revanche, de prévoir le cas où le responsable du traitement s'oppose à la mission de contrôle. Dans ce cas, l'autorité doit pouvoir requérir du juge compétent la force publique.

Chapitre V – Le délégué à la protection des données personnelles

En vue d'une plus grande effectivité du droit, la volonté de diffuser la culture « informatique et libertés » au plus près de la conception et de la mise en œuvre des traitements de données personnelles conduit souvent le législateur à prévoir en complément de l'Autorité indépendante, l'institutionnalisation d'un délégué à la protection des données personnelles dans les organismes publics et privés. Une telle mesure peut être soit obligatoire, soit optionnelle.

Lorsqu'une telle solution est retenue il convient de prévoir au minimum :

- **les missions du délégué (article 23)** : de veiller au respect des obligations de la loi, et en particulier être consulté préalablement à leur mise en œuvre sur l'ensemble des nouveaux traitements, tenir à jour le registre des traitements mis en œuvre par le responsable des traitements, recevoir les demandes et les réclamations des personnes intéressées, informer le responsable des traitements des manquements constatés, saisir l'Autorité indépendante en cas de manquement constatés, lorsque le responsable de traitement ne prend pas les mesures nécessaires pour faire cesser les manquements, ou en cas de doute sur l'application de la loi, établir un bilan annuel de ses activités qu'il présente au responsable des traitements et qu'il tient à la disposition de l'Autorité indépendante ;
- **l'information** par le responsable du traitement auprès **de l'Autorité** de la personne désignée ;
- **la dispense de déclaration des traitements (article 24)** auprès de l'Autorité sauf dans les cas où le traitement relève du régime de l'autorisation ou de l'avis préalable ;
- les conditions relatives aux **compétences professionnelles (article 25)** et au lieu de résidence sur le territoire de l'Etat de la personne désignée comme délégué à la protection des données personnelles, ainsi qu'aux **incompatibilités de fonction** notamment avec celle de responsable de traitement. Il peut être prévu que le délégué soit un salarié du responsable de traitement ou soit une personne externe qui, de ce fait, pourrait être le délégué de plusieurs organismes. Tel pourrait être le cas, par exemple, d'une personne attachée à une fédération professionnelle ;
- les **garanties d'indépendance** et de moyens du délégué vis à vis du responsable du traitement : ne pas recevoir d'ordre, ne pas faire l'objet de sanctions du fait de l'exercice de ses fonctions ;
- l'obligation de confidentialité du délégué sur les informations recueillies à l'occasion notamment de l'instruction d'une plainte ou d'une requête dont il est saisi ;
- **les conditions d'une révocation éventuelle (article 26)** par le responsable du traitement pour des motifs graves. Ce pourrait être en effet le cas par exemple si l'Autorité constatait, à l'occasion d'un contrôle, des manquements importants dans l'application de la loi qui seraient imputables à la négligence du délégué. Pour sa part l'Autorité doit pouvoir demander la révocation du délégué en cas de conflit d'intérêt entre plusieurs de ses activités éventuelles avec celle de délégué à la protection des données personnelles.

Chapitre VI - Sanctions

Le présent canevas prévoit que l'Autorité indépendante est dotée d'un pouvoir de sanction (section1). En effet, il est utile de recourir à une telle solution qui, compte tenu du caractère souvent massif des traitements et des conséquences des manquements pour les nombreuses personnes concernées, présente l'avantage de la rapidité au regard d'une procédure judiciaire. La section 2 concerne les sanctions pénales.

Section 1 : sanctions prononcées par l'autorité indépendante

Selon la nature du manquement et de ses conséquences ainsi que selon son degré de gravité l'Autorité indépendante pourra prononcer trois types de sanction prévus à **l'article 27**, une **sanction pécuniaire, une injonction de cesser le traitement ou un avertissement**.

Ces décisions doivent être prises après une procédure contradictoire.

L'article 28 vise à répondre aux **situations d'urgence** lorsque l'atteinte aux droits et libertés est grave et immédiate en prévoyant la saisine par l'Autorité du **juge des référés**.

L'article 29 prévoit que la décision de l'Autorité peut s'accompagner d'une **injonction de procéder dans un délai déterminé aux modifications nécessaires du traitement**.

L'article 30 porte sur la **procédure contradictoire** qui prévoit l'établissement par l'Autorité d'un rapport soumis pour observations au responsable du traitement qui peut se faire représenter ou assister.

Il prévoit également le **recours devant la juridiction compétente contre les décisions prises par l'Autorité indépendante**.

L'article 31 prévoit le **principe de la proportionnalité de la sanction à la gravité des manquements** commis.

A titre d'illustration, on trouvera à **l'annexe 1** du présent canevas un **exemple de grille instituant la liste des manquements à la loi**.

L'article 32 prévoit les modalités de **publicité des décisions** de l'autorité.

Section 2 : sanctions pénales

L'article 32 prévoit le principe de **sanctions pénales** pour le non respect des dispositions de la loi.

A titre d'illustration on trouvera à **l'annexe 2** au présent canevas **un exemple d'articles pouvant figurer dans le code pénal**.

Le chapitre VI - Dispositions transitoires et finales

Dans un chapitre VI sur les dispositions transitoires et finales il est utile de prévoir le délai au terme duquel les décrets d'application nécessaires à l'entrée en vigueur de la loi seront pris.

Il est également utile de prévoir une période transitoire pour la mise en conformité à la loi des traitements de données personnelles mis en œuvre antérieurement à l'entrée en vigueur de la loi.