



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

La loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : quels changements dans la loi « informatique et libertés » du 6 janvier 1978 ?

Document de synthèse établi par la direction des affaires juridiques de la CNIL

Dernier Etat à transposer la directive européenne 95/46 CE du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, la France a fait le choix, symbolique, de maintenir la loi « informatique et libertés » du 6 janvier 1978 tout en la remaniant profondément. Tant dans sa structure que dans sa philosophie d'ensemble, la nouvelle loi a ainsi subi d'importants changements et a été considérablement enrichie qu'il s'agisse de son champ d'application et des conditions de licéité définies désormais précisément ou encore des nouveaux pouvoirs de sanction accordés à la Commission Nationale de l'Informatique et des Libertés.

Toutefois, autre symbole fort, son article premier – fondement essentiel des principes informatique et libertés- reste inchangé : « L'informatique doit être au service de chaque citoyen. Son développement doit d'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 ».

La nouvelle loi « informatique et libertés » c'est tout d'abord une large simplification des formalités déclaratives, le contrôle préalable de la CNIL étant désormais limité aux seuls traitements présentant des risques particuliers d'atteinte aux droits et libertés ; c'est ensuite un accroissement conséquent des pouvoirs d'intervention de la CNIL, c'est enfin un renforcement des droits des personnes sur leurs données.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

I. UN CHAMP D'APPLICATION MIEUX DÉFINI, LES CONDITIONS DE LICÉITÉ DES TRAITEMENTS PRÉCISEMENT DETERMINÉES

La nouvelle loi, calquée sur ce point sur la structure de la directive, détermine d'abord en son chapitre premier (articles 2 à 5) son champ d'application en définissant à cet effet un certain nombre de notions-clés (donnée à caractère personnel, traitement, fichier, responsable de traitement, destinataires), puis précise, dans un second chapitre, les conditions de licéité des traitements (articles 6 à 10).

1. Le champ d'application de la loi

La loi du 6 janvier 1978 s'applique aux traitements automatisés comme aux fichiers manuels. Elle comporte un champ d'application plus étendu que celui de la directive, puisqu'elle inclut les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État dans le domaine du droit pénal. Sont exclus du champ d'application de la loi les « traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles » (agendas électroniques, répertoires d'adresses, sites internet familiaux en accès restreint...).

Il doit également être relevé que sont soumis à la loi les traitements de données à caractère personnel dont le responsable est soit établi sur le territoire français (c'est-à-dire y exerce une activité dans le cadre d'une installation stable, quelle que soit sa forme juridique, filiale, succursale...) ou 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 État membre de la Communauté européenne.

- la donnée à caractère personnel

Outre la substitution de la notion de « données à caractère personnel » à celle « d'informations nominatives », la nouvelle loi donne une définition plus complète et sans doute plus large de cette notion, inspirée de celle figurant à l'article 2 de la directive, sans toutefois la reprendre intégralement. En particulier le législateur n'a pas repris la référence aux éléments propres à l'identité physique, physiologique, économique, culturelle ou sociale de la personne.

Est ainsi qualifiée de donnée à caractère personnel, « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ou par référence à un numéro d'identification ou à 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 peuvent avoir accès le responsable du traitement ou toute autre personne ».

Cette définition fait ainsi référence aux traitements qui bien que ne comportant pas de noms de personnes, peuvent cependant permettre de les identifier indirectement, que ce soit par la mention de leur numéro de sécurité sociale, l'insertion de leur photographie ou encore par la corrélation ou le rapprochement de données (par exemple, les dates et lieux de naissance, le lieu de résidence...).



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

- le traitement de données à caractère personnel

La notion de traitement, reprise de l'ancien article 5 de la loi de 1978 est cependant plus large dans la mesure où elle ne fait plus référence au traitement « automatisé » mais tout au contraire souligne que constitue un traitement de données toute opération (celles-ci étant énumérées) portant sur de telles données « quel que soit le procédé technique utilisé ».

- le responsable du traitement

S'inspirant de l'article 2 de la directive, l'article 3 de la loi définit le responsable du traitement comme « la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».

La loi de 1978, dans sa rédaction initiale, ne comportait aucune définition du responsable de traitement. Une clarification législative s'imposait donc.

Le rapport sur la transposition en droit français de la directive 95/46, remis en 1998 au Premier ministre par M. Guy Braibant avait d'ailleurs souligné que cette définition était essentielle – et devait figurer en tête de la loi – dans la mesure où elle détermine la personne physique ou morale sur laquelle les obligations prévues par la directive reposent et où le lieu d'établissement de cette personne constitue le premier critère de détermination de la loi nationale applicable.

2. Les conditions de licéité des traitements (articles 6 et 7)

L'article 6 de la nouvelle loi fixe les conditions de licéité de la collecte et du traitement des données à caractère personnel, telles qu'elles découlent de l'article 6 de la directive :

- ❑ loyauté et licéité de la collecte,
- ❑ détermination spécifique de la finalité du traitement et des conditions de réutilisation ultérieure des données à des fins statistiques ou à des fins de recherche scientifique ou historique,
- ❑ respect du principe de proportionnalité des données dans la collecte et le traitement des données (celles-ci doivent être pertinentes, adéquates et non excessives au regard des finalités de la collecte et des traitements),
- ❑ exactitude et mise à jour des données,
- ❑ durée de conservation proportionnée à la finalité.

La loi du 6 janvier 1978 déterminait déjà les règles fondamentales de licéité des traitements en imposant, notamment, le respect des principes de loyauté, d'une durée de conservation limitée, d'une réutilisation possible des données à des fins historiques, statistiques ou scientifiques, et d'exactitude des données. La loi de 1978 ne se référait en revanche au principe de finalité que de manière incidente, dans les dispositions relatives aux obligations de déclaration.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

Reprenant sur ce point les dispositions tant de la Convention 108 du Conseil de l'Europe¹ que de la directive 95/46, l'article 6 nouveau ajoute une exigence supplémentaire, en imposant que les collectes de données respectent le principe de « proportionnalité ». En effet, le traitement ne doit porter que sur des données qui sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ».

La nouvelle loi apporte, en outre, une innovation importante en évoquant la question de l'utilisation future des données collectées. Pour écarter le risque d'un usage injustifié, même décalé dans le temps, des informations recueillies, elle pose d'abord le principe de l'interdiction de tout traitement ultérieur des données « incompatible avec les finalités pour lesquelles elles ont été collectées ». Une exception est néanmoins prévue au profit des traitements réalisés à des fins statistiques ou à des fins scientifiques ou historiques, sous réserve qu'ils respectent les conditions de licéité, les formalités préalables à la mise en œuvre des traitements et les obligations imposées aux responsables de traitements et, enfin, qu'ils ne soient pas utilisés pour prendre des décisions à l'égard des personnes concernées.

Conformément aux termes de la directive de 1995, l'article 7 précise également les conditions de licéité permettant la création d'un traitement de données à caractère personnel, à savoir le consentement de la personne concernée, le respect d'une obligation légale, la sauvegarde de la vie de la personne, l'exécution d'une mission de service public ou d'un contrat ou encore la réalisation de l'intérêt légitime du responsable du traitement « sous réserve de ne pas méconnaître l'intérêt ou les droits fondamentaux de la personne concernée ».

Cette dernière condition suppose de réaliser la balance entre les intérêts des responsables et les droits des personnes concernées. La directive de 1995 ne donne aucun critère à cet égard.

La portée particulièrement générale et peu habituelle en droit français de cette disposition a d'ailleurs conduit le rapporteur du projet de loi à l'Assemblée nationale en première lecture à rappeler qu' « il appartiendrait à la CNIL de veiller au respect de cet équilibre, au travers de son contrôle *a priori* ou *a posteriori* ».

3. Les catégories de données sensibles (articles 8 et 9)

L'article 8 énumère la liste des données dites sensibles dont la collecte et le traitement sont en principe interdits : il s'agit des données relevant de l'article 31 ancien de la loi de 1978 (origines raciales, opinions politiques, philosophiques ou religieuses, appartenance syndicale des personnes, mœurs), complétées désormais de l'origine ethnique et des données relatives à la santé et à la vie sexuelle, conformément à l'article 8 de la directive.

Par dérogation à cette interdiction, certains traitements de données sensibles sont possibles dans la mesure où la finalité du traitement l'exige et moyennant le respect de certaines conditions.

¹ Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

Ces dérogations sont au nombre de dix :

- ❑ les traitements de données sensibles pour lesquels la personne concernée a donné son consentement exprès sauf dans le cas où la loi a prévu que l'interdiction ne peut être levée par le consentement ; cette disposition s'inspire de la rédaction de l'article 8, 2 a) de la directive qui précise que les législations des Etats membres peuvent prévoir que l'interdiction du traitement des données sensibles ne peut être levée par le consentement de la personne.
- ❑ les traitements nécessaires à la sauvegarde de la vie humaine (et pour lesquels la personne n'a pu donner son consentement) (ex : fichiers d'associations humanitaires);
- ❑ les traitements des associations et organismes à caractère religieux, philosophique, politique ou syndical (autorisées à n'enregistrer que les données sensibles correspondant à l'objet de l'association, et ce uniquement pour les membres et les personnes entretenant avec l'organisme des contacts réguliers et sans qu'il y ait de cession de ces données à des tiers, sauf à obtenir le consentement exprès des personnes concernées) ;
- ❑ les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée (ex : hommes politiques, dirigeants syndicaux, chefs de communautés religieuses) ;
- ❑ les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice (ex : fichiers de clients de professions juridiques pouvant comporter des données sensibles liées à la nature de l'affaire) ;
- ❑ les traitements nécessaires aux fins de 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 professionnel de santé ou par une autre personne tenue au secret professionnel (ex : fichiers de dossiers médicaux, fichiers de dépistage ou de surveillance sanitaire) ;
- ❑ les traitements statistiques réalisés par l'INSEE ou par un service statistique ministériel, après avis du Conseil national de l'information statistique (CNIS).
- ❑ les traitements de données de santé à des fins de recherche médicale selon les modalités prévues au chapitre IX de la loi ;
- ❑ les traitements de données sensibles susceptibles de faire l'objet, « à bref délai », d'un procédé d'anonymisation reconnu conforme à la loi par la CNIL (ex : certains traitements statistiques de données de santé) ;
- ❑ les traitements de données sensibles, justifiés par l'intérêt public et autorisés par la CNIL (article 25) ou par décret en Conseil d'Etat pris après avis de la CNIL (article 26).

Par ailleurs, l'article 9 dresse limitativement la liste des personnes pouvant procéder au traitement (automatisé ou non) d'informations relatives aux infractions, condamnations et mesures de sûreté.

Le premier alinéa en réserve le traitement aux juridictions, autorités publiques et personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

Le second alinéa ouvre cette faculté aux auxiliaires de justice agissant pour les stricts besoins de l'exercice de leurs missions légalement définies.

Le troisième alinéa, qui visait les personnes morales victimes d'infractions, a été déclaré contraire à la Constitution par le Conseil constitutionnel dans sa décision n°2004-499 DC du 29 juillet 2004.

Enfin, le quatrième et dernier alinéa prévoit que les sociétés de perception et de répartition des droits d'auteur et des droits des artistes-interprètes et des producteurs de phonogrammes et de vidéogrammes ainsi que les organismes de défense professionnelle peuvent procéder à de tels traitements dans le cadre des atteintes aux droits d'auteur, aux droits voisins et droits des producteurs de bases de données tels que définis aux livres Ier, II et III du Code de la propriété intellectuelle. Cette disposition a pour objet de lutter contre le développement des actes de contrefaçons via l'utilisation sur internet des systèmes d'échanges de fichiers « peer to peer » .



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

II. UN RENFORCEMENT DES DROITS DES PERSONNES SUR LEURS DONNÉES

La nouvelle loi informatique et libertés renforce les droits des personnes sur leurs données, obligeant désormais les responsables de traitements à délivrer une information plus détaillée sur les conditions d'utilisation des données, que celles-ci soient recueillies de manière directe ou indirecte. Le droit d'opposition en matière de prospection commerciale est enfin consacré dans la loi et les conditions d'exercice du droit d'accès et de rectification sont précisées. Toutefois, des dérogations sont introduites pour tenir compte en particulier des spécificités de certains traitements notamment statistiques.

1. Le droit à l'information (articles 32 et 39)

- Les informations devant obligatoirement être délivrées (article 32)

Comme dans l'ancienne loi de 1978 les responsables de traitements doivent apporter aux personnes auprès desquelles ils recueillent directement des données un certain nombre d'informations.

Si l'indication du caractère obligatoire ou facultatif des réponses, des conséquences éventuelles d'un défaut de réponse, des destinataires des données et de l'existence d'un droit d'accès et de rectification était déjà prévue dans la loi de 1978 (en son article 27), la nouvelle loi élargit la liste des informations qui doivent être communiquées : identité du responsable du traitement, finalité poursuivie par le traitement, existence d'un droit d'opposition et d'un droit d'accès, transferts de données envisagés à destination d'un Etat non-membre de l'Union européenne. En cas de recueil des données par questionnaires, ceux-ci doivent comporter la plupart de ces mentions.

En outre, conformément à l'article 11 de la directive européenne 95/46, lorsque les données n'auront pas été recueillies auprès de la personne, celle-ci devra cependant être informée des conditions d'utilisation de ses données et de ses droits, dès l'enregistrement de ses données ou lors de leur première communication. Des dérogations à cette obligation d'information sont cependant prévues lorsque les données sont collectées pour la prévention, la recherche ou la poursuite d'infractions pénales, lorsque les données, recueillies pour un autre objet, sont traitées pour être conservées à des fins historiques, statistiques ou scientifiques ou encore lorsque l'information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

De même, la loi permet de limiter si nécessaire l'information des personnes dans le cas des traitements intéressant la sûreté, la défense ou la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté. Ces exceptions sont prévues par la directive 95/46.

Enfin, l'information délivrée peut se limiter à la seule indication de l'identité du responsable du traitement et des finalités poursuivies dès lors que le traitement porte sur des données sensibles (relevant de l'article 8) et qu'elles sont destinées à être anonymisées dans de brefs délais.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

- L'information « à la demande » (article 39)

En outre, et sans préjudice de l'information qui a déjà pu lui être délivrée sur ce point, toute personne justifiant de son identité pourra obtenir des précisions sur les finalités, les données traitées ainsi que sur l'origine de celles-ci, précision particulièrement utile à connaître en cas de prospection commerciale.

Par ailleurs, et reprenant en cela les dispositions de l'article 3 de la loi du 6 janvier 1978, mais de façon plus restrictive, toute personne pourra interroger le responsable du traitement afin de connaître et de contester la logique qui sous-tend le traitement en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

2. Le droit d'opposition (article 38)

Reprenant presque littéralement les dispositions antérieures de la loi de 1978, le nouvel article 38 permet à toute personne de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, sauf dans les cas où 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.

Toutefois, la loi consacre le droit de s'opposer, sans frais, à l'utilisation de ses données à des fins de prospection, notamment commerciale. Cette disposition, nouvelle, renforce donc la protection des personnes dans le secteur du marketing commercial, activité qui suscite un nombre considérable de plaintes auprès de la CNIL. Il convient néanmoins de préciser que les professionnels du marketing direct, sous l'impulsion de la CNIL, ont fait application de ce principe² avant même la rédaction de la directive 95/46/CE, comme en témoigne l'adoption d'un code de déontologie par l'Union française du marketing direct en 1993 dont l'objectif affiché était notamment de « garantir la mise en œuvre du droit au refus d'être prospecté ».

3. Le droit d'accès (article 39 et suivants)

- Les conditions d'exercice du droit d'accès

Sans modifier substantiellement les conditions dans lesquelles toute personne peut demander et obtenir communication des données la concernant enregistrées dans un fichier, la nouvelle loi les encadre plus précisément sur les points suivants :

le juge des référés pourra être saisi en cas de risque de dissimulation ou de disparition des données ;

si un responsable de traitement estime qu'une demande est manifestement abusive (par exemple en raison de son caractère répétitif), il pourra simplement s'y opposer alors qu'auparavant la CNIL devait lui accorder l'autorisation de ne plus tenir compte de la demande ;

le droit d'accès est exclu lorsque les données sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et aux seules fins de statistiques ou de recherche scientifique ou historique. Cette dérogation doit être prévue dans la demande

² Cette pratique ayant d'ailleurs été consacrée par le Conseil d'Etat.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

d'autorisation ou la déclaration effectuée auprès de la CNIL, sauf dans le cas des traitements d'archives.

Par ailleurs en cas de délivrance de copies, le paiement d'une redevance est abandonné au profit du paiement d'une somme ne pouvant excéder le coût de la reproduction.

- Le droit d'accès indirect

Comme auparavant, le droit d'accès aux fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique reste indirect. Toute personne souhaitant exercer son droit d'accès à ces fichiers doit s'adresser à la CNIL 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 toutes investigations utiles. Le commissaire ainsi désigné exerce, aux lieu et place du requérant, le droit d'accès, de rectification ou d'effacement des données soit inexactes, soit collectées ou conservées en contradiction avec la loi.

Jusqu'à l'intervention de la loi du 18 mars 2003 pour la sécurité intérieure, la Commission ne pouvait que notifier à l'intéressé qu'il avait été procédé aux vérifications demandées ainsi que le prescrivait les termes même de l'article 39 de la loi du 6 janvier 1978 sauf pour ce qui concerne les fichiers des renseignements généraux pour lesquels des modalités particulières d'exercice du droit d'accès - permettant sous certaines conditions, et après accord du ministère de l'intérieur, la communication de son dossier au requérant – étaient fixées par le décret du 14 octobre 1991.

Cette loi a modifié sur ce point la loi de 1978 qui prévoit désormais (nouvel article 41) que « 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 ».

En revanche, l'article 42 nouveau de la loi de 1978 instaure, par analogie avec l'article précédent, un droit d'accès indirect pour les fichiers constitués à des fins de recherche et de constatation des infractions et en particulier à des fins de recherche des infractions fiscales. Désormais, un régime similaire à celui des traitements de défense ou de sécurité sera susceptible d'être appliqué à ces traitements.

4. Le droit de rectification (article 40)

Comme le prévoyait déjà la loi de 1978, toute personne peut demander que soient rectifiées, complétées, mises à jour ou effacées les données la concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Les données pourront également être verrouillées à sa demande.

Lorsque des modifications seront apportées, le responsable du traitement devra justifier, sans frais et à la demande de la personne, des opérations qu'il a effectuées. Auparavant, il devait délivrer une copie de l'enregistrement modifié.

Seule disposition de la nouvelle loi concernant les données sur les personnes décédées, ce nouvel article 40 offre désormais aux héritiers d'une personne décédée la possibilité d'exiger que le responsable d'un traitement comportant des données concernant le défunt prenne en considération le décès et procède aux mises à jour, si des éléments portés à la connaissance de ces héritiers leur laissent présumer que ces données n'ont pas été actualisées.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

III. LES DÉCLARATIONS DE FICHIERS : UNE SIMPLIFICATION DES FORMALITÉS ET UN CONTRÔLE DÉSORMAIS « CIBLEÉ » SUR LES TRAITEMENTS « A RISQUES »

La loi de 1978, dans sa rédaction antérieure à la loi du 6 août 2004, soumettait à formalités auprès de la CNIL, sans distinction, tout projet de traitement automatisé de données nominatives, et se fondait essentiellement, pour déterminer le contrôle préalable de la CNIL, sur un critère organique, à savoir la nature publique ou privée du responsable du traitement. Ainsi, les traitements relevant du secteur public, pour être mis en œuvre, devaient-ils obtenir au préalable un avis favorable de la CNIL alors que les traitements du secteur privé n'étaient astreints qu'à simple déclaration, la CNIL étant tenue de délivrer un récépissé dès réception de celle-ci, son rôle devant se borner « à s'assurer de la régularité de la déclaration effectuée auprès d'elle au regard des prescriptions » exigées en l'espèce par la loi ainsi que l'avait rappelé le Conseil d'Etat en annulant un refus de délivrance de récépissé prononcé par la CNIL (arrêt du 6 janvier 1997 Caisse d'épargne Rhône Alpes C/ CNIL). Toutefois, la loi prenait en compte un second critère matériel fondé sur la sensibilité relative des données traitées, pour selon le cas, soit soumettre à autorisation particulière leurs traitements (cas du numéro de sécurité sociale (ou NIR) et des données révélant les origines raciales, les opinions politiques, philosophiques ou religieuses des personnes ou encore leurs appartenances syndicales ou leurs mœurs) soit au contraire, prévoir un allègement de formalités pour certaines catégories de traitements « courants » et ne portant manifestement pas atteinte à la vie privée et aux libertés, qui pouvaient faire l'objet de déclarations simplifiées de conformité à des normes édictées par la CNIL

Se conformant tant à la lettre qu'à l'esprit de la directive 65/46/CE, la nouvelle loi, en son chapitre IV, modifie de façon substantielle les obligations déclaratives des responsables de traitements:

la déclaration devient le régime de droit commun pour la plupart des traitements, que ceux-ci relèvent de personnes publiques ou de personnes privées, de larges possibilités d'exemption et d'allègement des formalités étant prévues ;

désormais, ne sont soumis à autorisation ou avis de la CNIL, conformément à l'article 20 de la directive, que les seuls traitements présentant des risques particuliers au regard des droits et libertés des personnes;

les fichiers manuels doivent, sous certaines conditions, faire aussi l'objet de formalités auprès de la CNIL, puisque l'article 20 de la loi du 6 août 2004 relatif aux dispositions transitoires donne aux responsables de fichiers manuels un délai de trois ans pour se mettre en conformité avec la nouvelle loi.

Il convient de noter que ces dispositions sont immédiatement applicables. Cependant, les responsables de traitements dont la mise en œuvre est régulièrement intervenue avant la publication de la loi disposent d'un délai de trois ans pour mettre leurs traitements en conformité sauf si celle-ci n'a pas pour effet de modifier les caractéristiques des traitements auquel cas aucune formalité nouvelle ne devra être accomplie (article 20 de la loi du 6 août 2004).



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

1 . Une simplification des formalités déclaratives pour les traitements exempts de risques

Doivent faire l'objet de déclaration tous les fichiers publics ou privés qui n'en sont pas dispensés ou qui relèvent d'autres régimes de formalités.

- De nouvelles possibilités de simplification

Comme le prévoyait déjà la loi de 1978 dans sa rédaction antérieure à la loi du 6 août, la CNIL peut édicter des normes permettant d'encadrer les conditions d'utilisation de certaines catégories de traitements « courants » ne portant pas atteinte à la vie privée ou aux libertés et de simplifier en conséquence les obligations déclaratives des responsables de traitements qui s'y conforment. Usant largement de ce pouvoir réglementaire, elle a adopté depuis sa création 36 normes simplifiées : ainsi, 70 % des traitements déclarés à la CNIL le sont aujourd'hui sous forme simplifiée. Et de nouvelles normes simplifiées sont en cours d'élaboration telle celle relative aux fichiers de gestion du personnel dans le secteur privé.

En permettant aux organisations représentatives de formuler auprès de la commission leurs propositions lors de l'élaboration des normes, la nouvelle loi consacre une démarche de concertation pratiquée depuis longue date par la Commission, en particulier avec les organisations syndicales et patronales.

Par ailleurs, la CNIL a désormais la possibilité d'accepter, pour un organisme donné une déclaration unique regroupant un ensemble de traitements présentant des finalités identiques ou liées entre elles, telles que par exemple, le recrutement, la gestion du personnel la formation, l'évaluation (article 23 II).

- Les exonérations de déclarations

La loi prévoit désormais la possibilité d'une exonération de formalités soit d'office pour plusieurs catégories de traitements (registres destinés exclusivement à l'information du public, traitements de conservation d'archives, fichiers de membres ou de correspondants d'organismes et associations à caractère religieux, politique, syndical...) soit par la CNIL elle-même.

La Commission peut ainsi, aux termes de l'article 24, exonérer de déclaration certains traitements « courants » ne portant pas atteinte à la vie privée ou aux libertés « 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 ».

Ce pouvoir nouveau devrait permettre à la CNIL de réorienter ses moyens d'action vers des activités jugées prioritaires : l'examen approfondi des projets « sensibles » (par exemple la biométrie), l'instruction des plaintes et réclamations, le développement des contrôles sur place. Cet objectif était clairement énoncé dans le rapport sur la transposition en droit français de la directive 95/46, remis en 1998 au Premier ministre par M. Guy Braibant qui préconisait d'ailleurs qu'un grand nombre de traitements soit dispensé de déclaration, afin de recentrer l'action de la CNIL sur le contrôle *a posteriori*.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

La Commission a, par une décision du 14 décembre 2004, dispensé de déclaration les fichiers de paie conformes aux règles fixées précédemment par les normes simplifiées 28 (employeurs privés) ou 36 (employeurs publics).

Enfin, innovation majeure, l'article 22 prévoit une dispense de déclaration de traitements (à l'exclusion des traitements à risques) pour lesquels le responsable de traitement a désigné un « correspondant à la protection des données à caractère personnel », sauf en cas de transfert de données à caractère personnel à destination d'un Etat non-membre de la Communauté européenne. Ces dispositions, qui ne sont pas d'application immédiate, devraient être précisées par décret.

2- Un contrôle *a priori* limité aux traitements présentant des risques particuliers d'atteinte aux droits et libertés

Les traitements soumis à autorisation relèvent des articles 25 à 27 dont l'application apparaît complexe du fait des nombreux renvois qu'ils comportent. De la lecture combinée de ces dispositions, et notamment du premier alinéa de l'article 25 il ressort que le législateur a entendu expressément maintenir, pour certaines catégories de traitements à risques relevant du secteur public et en particulier pour tous les traitements dits de souveraineté (non couverts par la directive) un régime de demande d'avis, excluant explicitement l'application du régime de l'autorisation par la CNIL.

Le critère organique lié à la qualité juridique du responsable du traitement (public- privé) n'a donc pas disparu. En outre, la procédure de demande d'avis se décline selon des modalités différentes selon les caractéristiques du traitement.

Pour déterminer le type de régime d'autorisation applicable, le recours ou non, dans un traitement, au NIR, Numéro d'Inscription au Répertoire National d'Identification des Personnes physiques, numéro d'identification attribué par l'INSEE et largement utilisé dans la sphère sociale (numéro de sécurité sociale) constitue le critère premier d'orientation du choix de la formalité, le second critère à prendre en considération étant comme il a été indiqué la nature publique ou privée du responsable du traitement. Enfin, un troisième critère de sélection doit être pris en compte : l'enregistrement de données sensibles relevant de l'article 8.

- Le régime de la demande d'avis (articles 26 et 27)

Il convient à cet égard de distinguer les demandes d'avis exigeant un projet de décret en Conseil d'Etat (articles 26 II, 27 I), de celles exigeant un projet d'arrêté (article 26 I, 27 II) ou un projet de décision de l'organe délibérant (article 27 II).

Sans entrer dans le détail de ces procédures, il doit être seulement relevé que la procédure applicable est déterminée à la fois en fonction de la qualité juridique de l'autorité publique responsable du traitement, de la finalité de celui-ci et de la nature des données enregistrées. A titre d'exemple, doivent être autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la CNIL :



- ❑ les traitements portant sur des données sensibles mis en œuvre pour le compte de l'état qui intéressent la sûreté de l'état, la défense ou la sécurité publique ou dont l'objet est la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté (article 26 II) ou encore qui portent sur des données biométriques (telles que les empreintes digitales) ;
- ❑ les traitements mis en œuvre pour le compte de l'état, d'une personne morale de droit public, d'une personne de droit privé gérant un service public – qui portent notamment sur le NIR, sauf lorsqu'ils 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 (cas des organismes de protection sociale obligatoire), soit d'établir l'assiette, de contrôler ou de recouvrer les impositions et taxes de toute nature (cas de l'administration fiscale), soit d'établir des statistiques », auquel cas un décret ne sera exigé que si ces traitements comportent en outre des données sensibles relevant de l'article 8 ou des données relatives aux infractions, condamnations et mesures de sûreté ou donnent lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents (article 27 I et II).

Si la nouvelle loi prévoit, comme les dispositions antérieures, qu'au terme d'un délai de deux mois, le silence de la CNIL équivaut à un avis favorable, les procédures exigeant un avis conforme de la CNIL (en cas de traitements de données sensibles) ou l'intervention d'un décret en cas d'avis défavorable ont été supprimées. Il doit toutefois être noté que la loi prévoit une obligation de publication des avis de la CNIL qui s'agissant des traitements précités devra être réalisée de façon concomitante à l'acte réglementaire autorisant le traitement.

- Le régime de la demande d'autorisation à la CNIL (article 25)

Ce régime, jusqu'alors limité aux fichiers de recherche médicale et aux traitements d'évaluation des pratiques de soins, est étendu à dix catégories de traitements considérés comme présentant des risques soit en raison de la sensibilité des données traitées soit en raison de la finalité ou des caractéristiques du traitement.

Doivent désormais être autorisés par la Commission³ :

- ❑ les traitements statistiques, automatisés ou non, de données sensibles réalisés par l'INSEE ou par un service statistique ministériel (article 8 II 7°),
- ❑ les traitements, automatisés ou non, de données sensibles « appelés à faire l'objet à bref délai d'un procédé d'anonymisation » reconnu conforme par la CNIL (article 8 III), tels que par exemple, les enquêtes statistiques réalisées par des sociétés de communication médicale ;

³ La CNIL dispose d'un délai de deux mois pour se prononcer ; en cas d'absence de réponse dans ce délai, la demande d'autorisation est réputée rejetée.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

- ❑ les traitements, automatisés ou non, de données sensibles « justifiés par l'intérêt public » (article 8 IV) ; sont concernés par exemple les fichiers de gestion des prestations des organismes d'assurance maladie obligatoire qui comportent l'enregistrement, sous forme de codes détaillés des actes médicaux ou encore des médicaments ;
- ❑ les traitements automatisés portant sur des données génétiques (sauf ceux « mis en œuvre par des médecins ou des biologistes qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements », qui relèvent de la procédure de déclaration) ; il s'agit, par exemple, des fichiers de résultats de tests génétiques, dans le cadre de recherche de paternité, mis en œuvre par les laboratoires d'analyse agréés ;
- ❑ les traitements, automatisés ou non, « portant sur des données relatives aux infractions, condamnations ou mesures de sûreté » (sauf ceux des auxiliaires de justice qui relèvent de la procédure de déclaration et des traitements d'infractions pénales mis en œuvre par l'Etat)relevant d'autorités publiques, de personnes morales gérant un service public ou encore des sociétés de droits d'auteurs dans le cadre des actions de lutte contre le téléchargement illicite de fichiers (musique, vidéo) sur internet ;
- ❑ 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 » ; il s'agit d'encadrer les fichiers dits « listes noires » : fichiers internes de lutte contre la fraude, fichiers mutualisés d'impayés que ce soit dans le domaine de la téléphonie fixe ou mobile, du crédit, des banques, de l'assurance, des loueurs de véhicules mais aussi les traitements de crédit scoring ;
- ❑ les traitements automatisés ayant pour objet soit 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, soit l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes, sont ici concernés les interconnexions de fichiers de personnes relevant du secteur privé (ainsi que d'interconnexions entre fichiers du secteur public et fichiers du secteur privé) ainsi que l'interconnexion, au sein d'une même personne morale de droit privé, de fichiers présentant des finalités différentes ;
- ❑ les traitements qui requièrent une consultation du Répertoire National d'Identification des Personnes Physiques (RNIPP) tenu par l'INSEE ou qui portent sur des données parmi lesquels figure le Numéro d'Inscription au Répertoire (NIR) et donc de son équivalent, le numéro de sécurité sociale ;
- ❑ les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

- les traitements automatisés comportant des données biométriques (empreintes digitales, iris de l'œil, reconnaissance du contour de la min, reconnaissance faciale...), nécessaires au contrôle de l'identité des personnes. Le contrôle préalable de ces traitements, expressément demandé par la CNIL, devrait lui permettre d'encadrer plus rigoureusement dans le secteur privé les conditions d'utilisation des techniques biométriques sensibles qui telles les empreintes digitales comportent des risques particuliers d'atteinte à la vie privée.

Le législateur a assorti ce régime d'autorisation de possibilités de simplification : ainsi, la CNIL a désormais la possibilité de délivrer une autorisation unique pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant les mêmes destinataires.



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

IV. DU CONTRÔLE SUR PLACE AUX SANCTIONS : L'ACCROISSEMENT DES POUVOIRS D'INTERVENTION DE LA CNIL

1. la réalisation des contrôles sur place

La loi du 6 janvier 1978, dans sa rédaction antérieure à la loi du 6 août, autorisait déjà à la Commission à procéder à des vérifications sur place à l'égard de tout traitement. Évoquées succinctement dans l'ancienne loi (un seul alinéa leur était consacré à l'article 21), les règles fixant les modalités des contrôles font désormais l'objet d'un chapitre spécifique (chapitre VI : article 44), plusieurs dispositions de la loi y faisant par ailleurs référence (article 11 et 21).

La nouvelle loi précise ainsi que les membres et les agents habilités de la CNIL «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 devra être informé préalablement de ces contrôles. 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 qui statue par ordonnance motivée selon la procédure du référé prévue par les articles 493 à 498 du nouveau code de procédure civile dans le ressort duquel sont situés les locaux à visiter (ou du juge délégué par lui), saisi à la requête du président de la CNIL. La visite s'effectue alors sous l'autorité et le contrôle du juge qui l'a autorisée et qui peut se rendre dans les locaux durant l'intervention.

Par ailleurs, les membres et agents de la CNIL peuvent accéder aux programmes informatiques et aux données, en demandant la transcription par tout traitement approprié, recueillir, sur place ou sur convocation, tout renseignement et toute justification utile, demander communication et prendre copie de tous documents utiles à l'accomplissement de leurs missions.

Toutefois, les pouvoirs d'investigation de la CNIL connaissent certaines limites. Ainsi, l'avant-dernier alinéa de l'article 44-III de la loi prévoit-il que « 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 services de santé, et qui est mis en œuvre par un membre d'une profession de santé ».

En outre, si de façon générale, les personnes interrogées dans le cadre des vérifications sont tenues de fournir les renseignements demandés, cette obligation ne s'applique pas aux personnes astreintes au secret professionnel (article 21, dernier alinéa). Le Conseil constitutionnel a relevé que « dans le silence des dispositions de la loi du 6 janvier 1978 antérieures à la loi déferée, les personnes interrogées par la Commission Nationale de l'Informatique et des Libertés étaient déjà soumises au secret professionnel ».



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

Seules les personnes expressément tenues au secret professionnel sont susceptibles de l'opposer à la délégation de la Commission et le Conseil Constitutionnel, dans sa décision précitée, a pris soin de préciser que « l'invocation injustifiée du secret professionnel pourrait constituer une entrave passible des peines prévues par l'article 51 nouveau de la loi du 6 janvier 1978⁴ ».

2. De nouveaux pouvoirs de sanction pour la CNIL

- Un éventail de sanctions graduées

Alors qu'auparavant, la CNIL, constatant un manquement à la loi, ne pouvait que délivrer des avertissements aux organismes en cause ou les dénoncer au parquet, la nouvelle loi la dote de pouvoirs de sanctions administratives et pécuniaires importants.

L'éventail des mesures coercitives et des sanctions tel qu'il est défini au chapitre VII de la loi du 6 janvier 1978 (articles 45 à 49) est large : hormis l'avertissement, la Commission pourra désormais, après une mise en demeure infructueuse et à l'issue d'une procédure contradictoire, prononcer une sanction pécuniaire – à l'exception des traitements mis en œuvre par l'Etat –, une injonction de cesser le traitement (pour les traitements relevant du régime déclaratif), ou encore retirer son autorisation (pour les traitements soumis à une telle procédure).

En outre, en cas d'urgence et de violation des droits et libertés résultant de la mise en œuvre d'un traitement, la Commission pourra décider l'interruption temporaire de celui-ci ou le verrouillage de données (pendant trois mois) à l'exception de certains traitements de l'Etat et en particulier des traitements dits de souveraineté intéressant la sûreté de l'Etat, la défense ou la sécurité publique et ceux ayant pour objet la recherche d'infractions pénales ou l'exécution des condamnations, pour lesquels la CNIL aura cependant la possibilité d'informer le Premier ministre « pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée ».

Enfin, en cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL pourra demander en référé au juge d'ordonner toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

Le montant des sanctions pécuniaires susceptibles d'être infligées par la CNIL pourra atteindre 150 000 € lors du premier manquement constaté, et 300 000 € ou 5% du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une entreprise dans la limite de 300 000 € (article 47 alinéa 2). Le montant de ces sanctions devra en outre être « proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement » .

⁴ Article 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 :

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 ;

(...) »



COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

- Les règles de procédure applicables au prononcé des sanctions

Autre nouveauté introduite par la loi du 6 août la plupart des mesures coercitives, parmi lesquelles les sanctions pécuniaires, seront prononcées, non par la formation plénière de la commission (dont ne relèveront que les décisions de verrouillage des données et d'information du Premier ministre) mais par une formation restreinte composée de 6 membres (le président, les deux vices-présidents et trois membres élus par la commission en son sein pour la durée de leur mandat) et dont ce sera d'ailleurs l'unique fonction.

L'article 46 de la loi modifiée dispose que les sanctions qui relèvent de la compétence de la formation restreinte « sont prononcées sur la base d'un rapport établi par l'un des membres de la CNIL, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte (...) ».

Ce même article précise les dispositions devant être prises pour assurer le respect du principe du contradictoire qui doit sous-tendre la procédure de sanction quelle que soit la formation de la commission qui la prononce. Il est ainsi prévu que le rapport proposant la sanction soit notifié pour observations au responsable du traitement qui peut se faire représenter ou assister.

Enfin, la loi du 6 janvier 1978 modifiée prévoit que « 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 ». Le législateur a ainsi entendu laisser à la CNIL une marge d'appréciation dans la publicité qui doit entourer les sanctions qu'elle prononce.

L'éventail des sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal, qui ne subissent pas de changement substantiel, ne doit pas être oublié, la CNIL conservant bien entendu la possibilité de dénoncer au parquet les infractions à la loi dont elle aura connaissance.