

Mémoire pour l'obtention du DESS droit de l'internet administration-entreprise
Session de septembre 2005
Carole BUI

**LE CORRESPONDANT A LA PROTECTION DES
DONNEES A CARACTERE PERSONNEL, UN NOUVEL
ACTEUR INTRODUIT PAR L'ARTICLE 22 DE LA LOI
DU 6 JANVIER 1978 MODIFIEE**

Président du jury : *Monsieur Georges CHATILLON, directeur du DESS droit de l'internet administration-entreprise*

Membre du jury : *Madame Pascale COMPAGNIE, magistrat et chef du bureau des libertés publiques à la Direction des Libertés Publiques et des Affaires Juridiques (DLPAJ) – Ministère de l'Intérieur et de l'Aménagement du Territoire*

: Marie-Claire ROGER-GRAUX

Je tiens à remercier Madame Pascale COMPAGNIE, Mademoiselle Catherine GROUBER, Monsieur Georges CHATILLON ainsi que Monsieur Herbert MAISL pour leur aide et leur soutien lors de l'élaboration de ce mémoire.

SOMMAIRE

INTRODUCTION.....p.2

PARTIE I : LE CORRESPONDANT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL, UNE NOUVELLE FONCTION UTILE ?
.....p.8

CHAPITRE I : Le correspondant à la protection des données, une nouvelle fonction aux multiples enjeux.....p.9

Section 1 : Un allègement des formalités préalables.....p.9

Section 2 : Une garantie du respect des libertés individuelles et de la vie privée des personnes.....p.19

CHAPITRE 2: Les missions du correspondant, des missions essentielles à la protection des données à caractère personnelp.26

| | |
|---|-------------|
| Section 1 : Les missions expressément conférées par la loi..... | p.26 |
| Section 2 : Une mission implicite : la diffusion de la «culture informatique et libertés ». | p.31 |
| PARTIE II : LE STATUT DU CORRESPONDANT, UN STATUT AU CŒUR DES CRITIQUES..... | p.36 |
| CHAPITRE 1 : Les modalités de désignation, une limite au champ d'intervention du correspondant..... | p.37 |
| Section 1 : La désignation, des conditions relatives à la personne du correspondant à la protection des données à caractère personnel à respecter..... | p.37 |
| Section 2 : La désignation, une procédure minutieuse à respecter..... | p.48 |
| CHAPITRE 2 : De la cessation des fonctions du correspondant à la protection des données à caractère personnel et de sa responsabilité..... | p.51 |
| Section 1 : La cessation des fonctions en dehors de tout manquement..... | p.51 |
| Section 2 : La cessation des fonctions résultant de manquements de la part du correspondant..... | p.52 |
| CONCLUSION..... | p.57 |
| BIBLIOGRAPHIE..... | p.59 |

INTRODUCTION

Dernière à transposer la directive européenne 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation des données¹, la France aura attendu neuf ans pour adapter la loi « informatique et libertés » du 6 janvier 1978² aux évolutions technologiques et à la circulation internationale des données.

En effet, bien qu'ayant fixé les principes généraux régissant la protection des données à caractère personnel, à savoir la protection des informations relatives « à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »³, et malgré les incessants efforts de la Commission nationale informatique et libertés (CNIL) pour préciser les contenus de ces derniers, secteur par secteur, par ses avis et ses rapports d'activité, la loi de 1978 commençait à s'essouffler face à l'apparition de la révolution numérique et à la massification des données.

Ce « déficit d'effectivité » et cette inadaptation à la « micro-informatique répartie et multipliée » de l'ancienne législation, soulignés à juste titre par Guy BRAIBANT dans son rapport « *Données personnelles et société de l'information* » remis au Premier Ministre et relatif à la transposition de la directive 95/46/CE en droit français⁴, rendait inévitable le remaniement profond opéré par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard de traitements de données à caractère

¹ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données, JOCE n°L281 du 23 novembre 1995

² Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978

³ Article 2 de la loi du 6 janvier 1978 modifiée

⁴ Rapport présenté au gouvernement sur la transposition en droit français de la directive européenne du 24 octobre 1995 relatif au traitement des données et à leur libre circulation du 3 mars 1998

personnel⁵ quant à son champ d'application, aux conditions de licéité désormais précisément déterminées, à la consolidation des droits des personnes sur leurs données, au renforcement des pouvoirs de la CNIL avec l'instauration des pouvoirs de sanctions et à la disparition de la *summa divisio* entre secteur public et secteur privé.

Un des grands changements également apportés à la loi « informatique et libertés » de 1978 par la loi du 6 août 2004 consiste en un allègement indéniable des formalités préalables notamment par un recentrage du contrôle a priori de la CNIL sur les traitements de données à caractère personnel⁶ présentant des risques particuliers d'atteinte aux droits et libertés et par de nouvelles possibilités de simplification, notamment par une exonération de déclaration par l'introduction d'une nouvelle fonction : le correspondant à la protection des données à caractère personnel. C'est sur ce dernier point que notre propos se fixera.

Le correspondant à la protection des données introduit par le III de l'article 22 de la loi de 1978 constitue sans conteste une véritable innovation dans le domaine de la protection des données à caractère personnel voire « LA véritable révolution du nouveau régime ainsi instauré » pour certains auteurs⁷. Cet article précise que « à l'exception de ceux qui relèvent des dispositions prévues aux articles 25⁸, 26 et 27⁹ ou ceux qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés ». Cet article ajoute dans son paragraphe III que « les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi, sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé ».

En d'autres termes, la désignation d'un correspondant à la protection des données à caractère personnel permet au responsable du traitement¹⁰, qu'il soit une entreprise ou une collectivité locale, d'être dispensé de déclarer ses fichiers soumis à l'obligation de déclaration générale de l'article 23 ou soumis à l'obligation de déclaration simplifiée de l'article 24 exception faite lorsque les données contenues dans ces applications font l'objet d'un transfert vers un Etat non membre de la Communauté européenne.

⁵ Loi n°2004-182 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JO du 7 août 2004, p.14063

⁶ Selon l'article 2 de la loi de 1978 modifiée, il s'agit de « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi le verrouillage, l'effacement ou la destruction* ».

⁷ Eric BRABY, « Le correspondant CNIL », L'informatique professionnelle n°229, déc.2004 p.10

⁸ Article 25 : traitements relevant du régime d'autorisation préalable de la CNIL

⁹ Articles 26 et 27 : traitements relevant du régime d'avis préalable de la CNIL pris après arrêté ministériel ou après décret en Conseil d'Etat.

¹⁰ Le responsable d'un traitement de données à caractère personnel est, au sens de l'article 2 de la loi du 6 janvier 1978 modifiée, « *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ».

Qu'est qu'un correspondant à la protection des données à caractère personnel ?

Il n'existe pas à l'heure actuelle de véritable définition du correspondant. Selon les propres termes de la loi, le correspondant est la personne chargée d'assurer de manière indépendante le respect des obligations prévues par la loi, bénéficiant des qualités requises pour exercer ses missions et tenant une liste des traitements immédiatement accessible à toute personne qui en fait la demande.

Ce nouvel acteur n'est pas à confondre avec le correspondant du Commissaire du Gouvernement auprès de la CNIL instauré par une circulaire du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés¹¹. Ce dernier est un haut fonctionnaire (directeur d'administration centrale ou fonctionnaire de rang équivalent) implanté dans chaque ministère qui a pour mission de «veiller à la protection de la vie privée dans les traitements automatisés» notamment dans les projets particulièrement sensibles et, d'assumer «l'ensemble des compétences que requiert la mise en oeuvre des textes et des directives du Gouvernement relatives à la protection de la vie privée dans les traitements automatisés».

Il ne s'agit en aucun cas d'un correspondant dit de protection des données à caractère personnel même si certains auteurs font remonter les origines de ce dernier au correspondant du commissaire du gouvernement auprès de la CNIL¹². En effet, le correspondant à la protection des données à caractère personnel est originaire de nos voisins européens.

Il paraît également utile de préciser que le correspondant n'est également pas à confondre avec l'institution spécifique des correspondants des organismes de presse maintenue par la loi du 6 janvier modifiée puisqu'un autre article de la loi leur est consacré.

L'article 67 2° nouveau dispose en effet que pour les traitements ayant pour finalité «l'exercice, à titre professionnel, de l'activité de journaliste», «la dispense de l'obligation de déclaration prévue par l'article 22 est subordonnée à la désignation par le responsable du traitement d'un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en oeuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi».

De plus, à l'opposé du correspondant, l'exonération de formalités préalables dont bénéficient les correspondants des organismes de presse concerne les traitements soumis à un régime d'autorisation autrement dit ceux portant sur les données sensibles de l'article 8¹³ et des infractions, condamnations et mesures de sûreté.

Un concept venu d'ailleurs...

Cette nouvelle institution, assez éloignée de la tradition française de protection des données personnelles essentiellement basée sur une position centraliste de régulation dont la CNIL est la parfaite illustration, résulte de la transposition de la notion de «détaché à la protection des données à caractère personnel» de l'article 18 de la directive 95/46/CE. Cet article dispose que «les Etats membres ne

¹¹ Circulaire du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés : application aux administrations et à l'ensemble du secteur public de la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés ; rôle des ministères et coordination par le commissaire du gouvernement auprès de la CNIL, JO du 17 mars 1993

¹² Claire LEVALLOIS BARTH et Arnaud BELLEIL, « Le correspondant informatique et libertés : une fonction en attente de clarification », Expertises n°283, juillet 2004 : « *Le choix français du correspondant trouve une double origine : une origine européenne [...] et une origine française puisqu'une circulaire du 12 mars 1993 organise la désignation, dans chaque ministère, d'un haut fonctionnaire comme correspondant du Commissaire du Gouvernement auprès de la CNIL* ».

¹³ Les données sensibles sont, au sens de l'article 8 de la loi du 6 janvier 1978 modifiée, des « *données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ».

peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivantes : [...]lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis un détaché à la protection des données à caractère personnel chargé notamment : d'assurer d'une manière indépendante, l'application interne, des dispositions nationales prises en application de la présente directive , de tenir un registre des traitements effectués par le responsable du traitement , contenant les informations visées à l'article 21, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées ».

Le dispositif du « détaché à la protection des données à caractère personnel » avait été lui même introduit dans la directive sur demande de l'Allemagne qui souhaitait conserver cette institution qui était expérimentée depuis un certain nombre d'années. Outre Rhin, la loi fédérale relative à la protection des données du 20 décembre 1990 prévoit l'obligation de désigner un « détaché à la protection des données » ou « Datenschutzbeauftragte » dans les entreprises. Cette obligation a même été étendue en 2001¹⁴ au secteur public fédéral (« Bundesbeauftragte ») ainsi qu'au niveau de chaque Land (« Landbeauftragte ») dans le cadre de la transposition de la directive européenne.

Ce dispositif est également développé dans d'autres pays qui en retirent satisfaction : en Suède, au Luxembourg et aux Pays-Bas où cette désignation est optionnelle, en Corée du Sud, en République Slovaque où cette institution est obligatoire pour les contrôleurs de système supervisant plus de cinq personnes, aux Etats-Unis et au Canada où une grande partie des entreprises dispose déjà d'un correspondant ou « Chief Privacy Officers » (CPO).

Ajoutons que certaines autorités de protection en Norvège, Finlande, Suisse et en Grande-Bretagne recommandent aux compagnies d'employer un tel correspondant. L'Organisation de Coopération et de Développement Economique (OCDE) a même fait de ce correspondant l'objet d'une recommandation.

Cependant, malgré l'expérimentation existante depuis un certain nombre d'années dans d'autres pays, l'introduction dans l'ordre juridique français de ce nouvel acteur en France ne s'est pas réalisée sans difficultés...

Entre accords et désaccords : une adoption du dispositif des correspondants difficile...

Dans son rapport remis au Premier Ministre sur la transposition de la directive¹⁵, Guy BRAIBANT s'était opposé à la généralisation du correspondant à la protection des données à caractère personnel en soulignant que « si elle se rattache en Allemagne à une certaine culture de cogestion, l'institution de ces délégués se heurterait en France à de sérieuses difficultés ».

Le rapporteur redoutait notamment qu'une situation d'inégalité soit instaurée selon la désignation ou non du correspondant mais également que la condition d'indépendance posée par la directive ne puisse pas être respectée en raison de l'absence d'un statut de salarié protégé. Ainsi, le dispositif avait été écarté par le projet de loi initial, exception faite dans le domaine de la presse où ce correspondant pouvait constituer valablement, selon le rapporteur, « un moyen de concilier la liberté d'expression et la protection de la vie privée ».

En 2001, la CNIL, émettait des doutes quant à l'utilité d'une telle fonction en France : son directeur de l'administration et de la communication Thierry Jarlet, interrogé sur l'apparition des premiers Chief Privacy Officer en Europe, y voyait un véritable « effet de mode »¹⁶.

¹⁴ Bundes-Datenschutzgesetz du 18 mai 2001 (BGBl IS 904) modifiant la BDSG du 20 décembre 1990 (BGBl IS 2954), <http://www.goethe.de>

¹⁵ Rapport présenté au gouvernement sur la transposition en droit français de la directive européenne du 24 octobre 1995 relatif au traitement des données et à leur libre circulation du 3 mars 1998

¹⁶ Florent LATRIVE, « A client fiché, directeur d'intimité », Libération, 27 janvier 2001

Le 1^{er} avril 2003, le Sénat adopte en première lecture le projet de loi dont l'orientation a été changée, sous l'impulsion du sénateur Alex TÜRK¹⁷, rapporteur au nom de la Commission des lois, par l'adoption notamment d'un nouvel amendement relatif au dispositif des correspondants à la protection des données à caractère personnel.

En effet, l'amendement n°38¹⁸ étend la dispense de déclaration qui concernait initialement les traitements portant sur des données sensibles mis en œuvre par des associations ou organismes à caractère religieux, syndical, politique et les traitements ayant pour objet la tenue d'un registre destiné à l'information du public (hypothèques, registre du commerce et des sociétés...), à tous les responsables de traitements qu'ils soient des entreprises, des administrations ou des collectivités locales à la condition qu'ait été nommé un correspondant. Le sénateur TÜRK y voit une opportunité pour la CNIL « de limiter les fichiers clandestins qui sont nombreux à fonctionner », de mettre en place « un canal idéal pour faire passer le nécessaire message pédagogique de la CNIL vers l'ensemble des utilisateurs » et d'instaurer « un substitut de déconcentration » beaucoup plus souple que cette dernière sans ajouter de nouvelles structures administratives.

Le 29 avril 2004, l'Assemblée Nationale adopte le texte ainsi modifié en deuxième lecture et réaffirme l'utilité du dispositif « à l'heure de la généralisation de l'outil informatique ».

Sur rapport du député Francis DELATTRE¹⁹, membre titulaire de la CNIL, la commission des lois constitutionnelles, de la législation générale de la République de l'Assemblée nationale s'est montrée favorable au dispositif mais a manifesté sa volonté de « renforcer » le dispositif notamment sur la question du statut et plus précisément sur celle de l'indépendance, condition nécessaire à l'accomplissement des missions du correspondant. L'étude de droit comparé des régimes applicables aux correspondants en Allemagne et aux Pays-Bas présentée par le rapport a conduit à la proposition d'un amendement n°14²⁰, modifiant le III de l'article 22 à deux niveaux : l'instauration d'un statut particulier de correspondant sans pour autant en faire une nouvelle catégorie de salarié protégé, le champ d'application du III de l'article 22 jusqu'alors ambigu qui est désormais restreint aux traitements soumis à déclaration.

Le 15 juillet 2004, le Sénat adopte définitivement le projet de loi.

Le Conseil Constitutionnel est saisi le 29 juillet 2004²¹ conformément à l'article 61-2 de la Constitution : le III de l'article 22 est notamment mis en cause. Les auteurs de la saisine considéraient que « ce correspondant ne bénéficie pas, à la lettre, de garanties d'indépendance indispensables ». Le Conseil Constitutionnel déclare toutefois la réforme de la loi relative à l'informatique et aux libertés du 6 janvier 1978 conforme à la Constitution, concluant notamment que l'institution des correspondants à la protection des données est entourée de précautions suffisantes²².

Les dispositions du III de l'article 22 n'étant pas d'application immédiate, il faudra attendre un décret d'application qui devrait être publié au début de l'automne pour voir véritablement fonctionner ce dispositif et mettre fin aux interrogations principales portant sur les garanties entourant l'indépendance du correspondant et sur la possibilité d'externaliser la fonction pour les petites structures.

¹⁷ Rapport n°218 du 19 mars 2003 élaboré par Alex TÜRK au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, Ref : <http://www.senat.fr/rap/102-218/102-2181.pdf>

¹⁸ Compte-rendu intégral du Sénat du 1^{er} avril 2003 p.39, <http://www.senat.fr>

¹⁹ Rapport DELATTRE n°1538, séance de l'Assemblée Nationale du 13 avril 2004, <http://www.assemblee-nationale.fr/12/rapports/r1537.asp>

²⁰ Compte rendu analytique officiel de l'Assemblée nationale, séance du 29 avril 2004, <http://www.assemblee-nationale.fr/>

²¹ Conseil Constitutionnel, décision n°2004-499 DC du 29 juillet 2004

²² « *compte tenu de l'ensemble des précautions ainsi prises, s'agissant en particulier de la qualification, du rôle et l'indépendance du correspondant, la dispense de déclaration résultant de sa désignation ne prive de garanties légales aucune exigence constitutionnelle* ».

D'ores et déjà, il ressort des travaux préparatoires que nul n'est insensible aux enjeux considérables engendrés par l'institution d'un tel acteur dans le domaine de la protection des données à caractère personnel en terme d'allégement des formalités préalables à la mise en œuvre des traitements et en terme de diffusion de la « culture informatique et libertés ».

Il convient néanmoins de s'interroger sur l'intérêt de l'introduction d'un correspondant au sein des collectivités locales comme au sein des entreprises dans l'état actuel du droit. Ne serait-il pas un gadget juridique introduit par le législateur ? Ce dernier a-t-il pris suffisamment de garanties juridiques lors de la transposition de la directive afin que cette fonction soit véritablement effective ? Le président Guy BRAIBANT n'aurait-il pas visé juste en estimant qu'il « ne semble pas que cette institution intéressante puisse être utilement transplantée en France » ?

Ainsi, il semble essentiel, afin de répondre à ces interrogations, de se pencher, dans un premier temps, sur la véritable utilité de ce correspondant quant aux enjeux qu'il engendre et à l'importance des missions qui lui seront confiées (PARTIE 1) puis, dans un second temps, sur le statut de ce dernier qui semble être sans conteste le point d'orgue de toutes les critiques ayant émergées lors des travaux préparatoires et qui sont toujours autant d'actualité (PARTIE 2).

PARTIE I : LE CORRESPONDANT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL, UNE NOUVELLE FONCTION UTILE ?

Le correspondant à la protection des données à caractère personnel est sans nul doute la principale innovation apportée par la loi du 6 août 2004 à la loi du 6 janvier 1978. En effet, l'institution de cette nouvelle fonction rompt avec une fonction centralisée occupée depuis un certain nombre d'années par la CNIL.

Face à une opinion partagée entre incroyable enthousiasme et engouement pour cette nouvelle fonction et critiques vivaces, il paraît légitime de se demander si le correspondant est véritablement utile ou du moins quelles pourraient être les raisons qui font de cette fonction un élément générateur d'une meilleure protection des libertés individuelles et plus particulièrement de la vie privée qui est devenue aujourd'hui un véritable sanctuaire.

Il ressort des travaux préparatoires et de la doctrine, que le correspondant à la protection des données à caractère personnel est une nouvelle fonction aux véritables enjeux (CHAPITRE 1) et ce d'autant plus que les personnes concernées par un tel dispositif sont nombreuses en raison de la quasi présence permanente du droit de la protection des données à caractère personnel dans la vie de chacun.

La deuxième piste de réflexion expliquant la volonté du législateur de mettre en place un tel acteur réside dans les missions qui seront confiées au correspondant : il sera loisible de constater que ces dernières sont tout à fait essentielles à la protection des données à caractère personnel au sein des entreprises et des collectivités locales (CHAPITRE 2).

CHAPITRE I : Le correspondant à la protection des données à caractère personnel, une nouvelle fonction aux multiples enjeux

Les principaux enjeux dans lesquels s'inscrit l'instauration de la fonction de correspondant à la protection des données à caractère personnel sont, d'une part, un allègement évident des formalités préalables à la mise en œuvre des traitements (section 1) puis, d'autre part, la garantie du respect de la vie privée et des libertés individuelles des personnes au sein des entreprises comme des collectivités locales (section 2).

Ces enjeux, dont les principaux bénéficiaires sont tout à fait conscients, justifient déjà à eux seuls l'utilité de cette nouvelle fonction. Cependant, ce point de vue est à nuancer au motif que ces derniers se trouvent tout de même limités au regard du champ d'application restreint du III de l'article 22.

Section 1 : Un allègement des formalités préalables

L'allègement des formalités obligatoires a été un des premiers arguments avancés par le rapporteur Alex TÜRK lorsque ce dernier a proposé au Sénat, au nom de la commission des lois, d'introduire le dispositif en droit français. Les sénateurs ont pris conscience de l'enjeu que pouvait être l'allègement des formalités obligatoires puisque ces dernières constituent un passage incontournable par la mise en œuvre des traitements et d'autant plus qu'il serait profitable aux entreprises, aux collectivités locales et à la CNIL elle-même.

I) Les formalités, un passage incontournable à la mise en œuvre des traitements

A/ La soumission des traitements aux formalités préalables, un principe déjà en vigueur avant la modification de la loi de 1978

Déjà dans la rédaction antérieure à la loi du 6 août 2004, aucun traitement automatisé d'informations nominatives ne pouvait être mis en œuvre sans que des formalités aient été accomplies, au préalable, auprès de la CNIL : le secteur privé, pour chacun de ses traitements, devait déposer auprès de la CNIL une déclaration comportant l'engagement que le traitement satisfaisait aux exigences de la loi

conformément à l'ancien article 16²³ de la loi du 6 janvier 1978; le secteur public quant à lui devait déposer une demande d'avis avant que n'intervienne l'acte de création conformément à l'ancien article 15²⁴.

Ainsi, pour déterminer le contrôle préalable de la CNIL, l'ancienne législation se fondait sur un critère organique qui consistait en la nature publique ou privée du responsable du traitement. La loi de 1978 prenait également en compte un second critère matériel fondé sur la nature sensible ou non des informations nominatives traitées : par là même, pour les catégories les plus courantes de traitements, qui ne portent manifestement pas atteinte à la vie privée et aux libertés, une procédure simplifiée avait été prévue par le législateur à savoir une déclaration de conformité à des « normes simplifiées » édictées par la CNIL secteur par secteur. A l'opposé, pour les traitements contenant des données sensibles, à savoir le numéro d'identification au Répertoire National d'Identification des Personnes Physiques²⁵ (RNIPP) ou encore des données relatives à l'origine raciale, aux opinions politiques, philosophiques ou religieuses des personnes, à l'appartenance syndicale, aux mœurs, une procédure d'autorisation était prévue.

B/ Les changements apportés au principe des formalités préalables par la loi du 6 janvier 1978 modifiée

La loi de 1978 modifiée, dans son chapitre IV intitulé « Formalités préalables à la mise en œuvre des traitements », tout en conservant le principe de formalités préalables, apporte des modifications substantielles en remplaçant notamment le critère organique de distinction entre secteur public et secteur privé par un critère matériel basé sur la sensibilité des données traitées.

1) La déclaration ordinaire, régime de droit commun instauré par la loi de 1978 modifiée

Désormais, la déclaration ordinaire du I de l'article 22 devient le régime de droit commun pour tous les traitements qui ne relèvent pas d'une autre formalité, que ces derniers soient mis en œuvre par une personne publique ou une personne privée. Cet article dispose « qu'à l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au second alinéa de l'article 36²⁶, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés ».

L'article 23 précise, quant à la lui, les modalités de mise en œuvre de la déclaration normale. Il prévoit en outre que cette déclaration doit comporter « l'engagement que le traitement satisfait aux exigences de la loi ». Cette déclaration consiste donc en un engagement de conformité de principe, conformité qui ne pourra être vérifiée que dans le cadre d'un possible contrôle a posteriori de la CNIL.

Cette déclaration peut être adressée à la CNIL par voie électronique. Cette dernière, en contrepartie, délivre sans délai un récépissé nécessaire à la mise en œuvre du traitement.

Une autre innovation a été aménagée par la loi nouvelle pour simplifier les démarches des responsables de nombreux traitements : la déclaration unique. Le II de l'article 23 permet que les traitements « relevant d'un même organisme et ayant des finalités identiques » puissent faire l'objet d'une telle déclaration.

²³ « Les traitements automatisés d'informations nominatives effectués pour le compte de personnes autres que celles qui sont soumises aux dispositions de l'article 15 doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de la CNIL ».

²⁴ « Hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la CNIL ».

²⁵ Il s'agit du numéro de sécurité sociale.

²⁶ L'article 36 alinéa 2 concerne les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives.

2) Autres régimes de formalités préalables prévus par la loi

A la suite des modifications apportées à la loi de 1978, ne sont soumis à autorisation (article 25) ou à avis (articles 26 et 27) que les traitements présentant des risques particuliers au regard des droits et libertés individuelles des personnes. A l'opposé, les traitements ne portant pas atteinte à la vie privée et aux libertés individuelles peuvent faire l'objet d'une déclaration simplifiée (article 24) dans les mêmes conditions que celles posées par l'ancienne législation.

a- la déclaration simplifiée de l'article 24

Cette procédure allégée concerne les traitements qui correspondent à l'une des normes dites simplifiées élaborées par la CNIL. Depuis 1978, cette dernière a adopté près de 45 normes²⁷ dont trois en 2004 visant à alléger les formalités préalables des collectivités locales. Ces normes visent « les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés ». A titre d'exemple, la CNIL, dans sa délibération n°2005-002 du 13 janvier 2005, a adopté la norme n°46 destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leur personnel²⁸. Il s'agit, aujourd'hui, de la forme de déclaration la plus répandue puisqu'elle représente près de 70% des traitements déclarés à la CNIL.

Le législateur a également aménagé, au II de l'article 24, la possibilité pour la CNIL d'autoriser les responsables de plusieurs traitements à procéder à une déclaration unique au regard 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 ».

b- le régime de la demande d'autorisation par la CNIL de l'article 25

Avant l'intervention de la loi nouvelle, ce régime était limité aux seuls fichiers de recherche médicale et aux traitements d'évaluation des pratiques de soin²⁹. Le législateur, dans la loi du 6 août 2004, a étendu le régime de l'autorisation à dix autres catégories de traitements qui, du fait de la sensibilité des données traitées, de leur finalité ou de leurs caractéristiques, présentent des risques d'atteintes à la vie privée et aux libertés.

Ainsi, aux termes de l'article 25, doivent être autorisés par la Commission :

- 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 d'un procédé d'anonymisation reconnu conforme par la CNIL (article 8 III) ;
- les traitements, automatisés ou non, de données sensibles justifiés par l'intérêt public (article 8 IV) tels que les fichiers du type « indemnisation des victimes des spoliations pendant la seconde guerre mondiale » ou encore les fichiers de gestion des prestations des organismes d'assurance maladie obligatoire;
- les traitements automatisés portant sur des données génétiques à l'exception des traitements 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, il s'agit, par exemple, des fichiers de données relatives à des tests de paternité ;

²⁷ Voir sur le site de la CNIL, <http://www.cnil.fr/?id=1198>

²⁸ JO n°40 du 17 janvier 2005, <http://www.cnil.fr/index.php?id=1231>

²⁹ Article 40-11 de l'ancienne législation

- les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux des auxiliaires de justice pour les besoins de leur missions de défense des personnes concernées, ici sont notamment visés les fichiers des sociétés de droits d'auteurs dans le cadre des actions de lutte contre le téléchargement illicite de fichiers sur internet ;
- les traitements automatisés susceptibles 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 tels que les « listes noires »³⁰ ;
- les traitements automatisés ayant pour objet soit l'interconnexion³¹ 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 concernées les interconnexions de fichiers de personnes relevant du secteur privé, les 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 comportant des données parmi lesquels figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans toutefois contenir le numéro d'inscription à celui-ci des personnes ;
- les traitements automatisés de données portant un jugement sur les difficultés sociales des personnes ;
- les traitements automatisés comportant des données biométriques, telles que les empreintes digitales ou encore la reconnaissance faciale, nécessaires au contrôle de l'identité des personnes.

Une fois la demande d'autorisation reçue, la Commission dispose d'un délai de deux mois, renouvelable une fois sur décision motivée de son président, pour se prononcer. Passé ce délai, la demande d'autorisation est réputée rejetée.

Comme cela est le cas pour les régimes de formalités précédemment étudiés, « les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires » peuvent être autorisés par une décision unique de la CNIL à charge pour le responsable de chaque traitement d'adresser à cette dernière un engagement de conformité du traitement à la description figurant dans l'autorisation.

c- le régime de la demande d'avis des articles 26 et 27

La demande d'avis concerne les traitements dits à risque relevant du secteur public et notamment les traitements dits de souveraineté³² qui, à l'origine, n'étaient pas couverts par la directive.

³⁰ Selon la doctrine de la CNIL, il s'agit de « 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 ». Voir <http://www.cnil.fr>

³¹ Selon la doctrine de la CNIL, il s'agit de « tout traitement automatisé mis en œuvre par un ou plusieurs responsables qui consiste à mettre en relation (à corréliser) des données ayant une finalité avec d'autres données ayant une finalité identique ou différente. Cette mise en relation (ou corrélation) peut consister à transférer un fichier pour alimenter un autre fichier ou pour réaliser la fusion de ces fichiers, à mettre ponctuellement en relation plusieurs fichiers normalement gérés séparément, par exemple en constituant un fichier d'appel à partir de l'un de ces fichiers qui servira à interroger les autres fichiers et sera enrichi par les résultats de cette interrogation. Il peut également s'agir d'assembler des informations provenant de plusieurs fichiers au sein d'une même base de données (exemple des bases dénommées « entrepôts de données » alimentés par des informations provenant de différents fichiers) avec un éventuel recours à des techniques logicielles de mises en relations ponctuelles (outils dits de datamining) ou de créer un lien technique entre plusieurs bases de données nominatives qui permettra, par exemple, de les consulter simultanément (par exemple, des sites portails permettant par des « liens hypertextes » d'assurer une mise en relation avec d'autres bases) », voir <http://cnil.fr>

³² Aux termes du paragraphe 2 de l'article 3 de la directive européenne, il s'agit des « traitements de données à caractère personnel ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les activités de l'Etat relatives à des domaines du droit pénal [...] »

□ Le régime de la demande d'avis de l'article 26

Aux termes du I de l'article 26, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat « qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique » ou « qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté » doivent faire l'objet, par principe, d'un arrêté du ou des ministres compétents, pris après avis motivé et publié de la CNIL.

Par exception, lorsque ces traitements portent sur des données sensibles au sens de l'article 8, la demande d'avis exige un décret pris en Conseil d'Etat. Ainsi, le choix de la procédure applicable variera en fonction de la sensibilité des données traitées.

□ Le régime de la demande d'avis de l'article 27

Selon la qualité juridique de l'autorité publique responsable du traitement et la finalité, la procédure applicable ne sera pas la même. Il y a lieu de distinguer les demandes d'avis exigeant un projet de décret en Conseil d'Etat (article 27 I) de celles exigeant un projet d'arrêté (article 27 II) ou un projet de décision de l'organe délibérant (article 27 II).

Ainsi, doivent faire l'objet d'un décret en Conseil d'Etat pris après avis motivé et publié de la CNIL :

- les traitements mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public, d'une personne de droit privé gérant un service public et qui portent notamment sur le numéro d'inscription au Répertoire National d'Identification des Personnes Physiques ;
- les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat comportant des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

Doivent faire l'objet d'un arrêté du ou des ministres compétents pris après avis motivé et publié de la CNIL :

- les traitements publics ne comportant pas le NIR mais qui nécessitent la consultation du RNIPP ;
- les traitements publics mis en œuvre par « des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer les impositions et taxes de toute nature, soit d'établir des statistiques » lorsqu'ils comportent le NIR ou portent sur des données biométriques nécessaires à l'authentification et au contrôle de l'identité des personnes, mais sans traiter de données sensibles ni de données relatives aux infractions, condamnations et mesures de sûreté ;
- « les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer » ;
- les traitements publics mis en œuvre dans le but de créer des « téléservices de l'administration électronique » si ces derniers portent sur le NIR ou tout autre identifiant personnel.

Pour ces quatre derniers traitements, la demande d'avis pourra exiger, « en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public », un projet de décision de l'organe délibérant chargé de leur organisation.

Pour les deux régimes confondus, l'article 28 précise que la CNIL dispose d'un délai de deux mois à compter de la réception de la demande pour se prononcer sous peine de voir son avis réputé favorable. Ce délai peut être renouvelé une fois sur décision motivée du président de la Commission.

Il est donc facile de constater que les formalités préalables constituent un passage incontournable pour quiconque souhaite mettre en œuvre un traitement, que cette personne soit originaire du secteur public et du secteur privé. Ajoutons même que cette obligation s'est généralisée aux fichiers manuels qui peuvent désormais faire l'objet de formalités préalables auprès de la CNIL, la nouvelle loi s'appliquant aussi bien

aux « traitements automatisés de données à caractère personnel » qu'aux « traitements non automatisés de données à caractère personnel »³³.

A titre d'illustration, la CNIL, dans son 25^{ème} rapport d'activité, a relevé que, sur la période du 1^{er} janvier au 31 décembre 2004, 66 840 nouveaux traitements de données à caractère personnel ont été déclarés.

C/ Les formalités préalables, une procédure fastidieuse

Les formalités préalables, qu'il s'agisse de déclarations, de demandes d'autorisation ou de demandes d'avis, sont soumises au chapitre IV de la loi de 1978 modifiée. Son article 30 précise qu'elles doivent contenir certaines mentions :

- « l'identité et l'adresse du responsable du traitement ou si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande » ;
- la ou les finalités du traitement ainsi qu'une description générale des fonctions pour les traitements soumis à avis ou autorisation de la CNIL ;
- les interconnexions, les rapprochements avec d'autres traitements ;
- « les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement »³⁴ ;
- la durée de conservation des informations traitées ;
- « le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées » ;
- les destinataires ou catégories de destinataires³⁵ ;
- la fonction de la personne ou du service auprès duquel s'exerce le droit d'accès ainsi que les mesures permettant l'exercice de ce droit ;
- « les dispositions prises pour assurer la sécurité des traitements et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant » ;
- les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Pour la déclaration unique, le responsable devra préciser en plus de celles relatives à l'ensemble des traitements, les informations qui sont propres à chacun d'entre eux.

Force est de constater que ces informations sont assez nombreuses : c'est la raison pour laquelle la CNIL facilite considérablement cette déclaration en mettant à la disposition des responsables des traitement un guide « Comment déclarer ? » accompagné des formulaires devant être fournis à cette dernière³⁶.

³³ Article 2 de la loi du 6 janvier 1978 modifiée

³⁴ Selon l'article 2 de la loi de 1978 modifiée, « la personne concernée par le traitement est celle à laquelle se rapportent les données qui font l'objet du traitement ».

³⁵ Selon ce même article, le destinataire d'un traitement de données à caractère personnel est « toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ».

³⁶ Voir sur le site de la CNIL, http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/declarer-CNIL.pdf

D/ Le non respect des formalités préalables

Dans son article 24, la directive 95/46/CE prévoyait que les Etats membres doivent prendre « les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive ».

Ainsi, le non respect des formalités préalables est incriminé par l'article 226-16 du Code pénal, article introduit par la loi du 6 janvier 1978 modifiée : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

Les formalités préalables constituent un système lourd et contraignant auquel il coûte cher de se soustraire. C'est la raison pour laquelle son allègement par le biais de la désignation d'un correspondant à la protection des données à caractère personnel est très bien accueilli par la plupart des entreprises et des collectivités locales. Cependant, cet avantage, conféré par le correspondant, est limité par le champ d'application du III de l'article 22 de la loi de 1978 relative l'informatique, aux fichiers et aux libertés.

II) Un allègement limité par le champ d'application du III de l'article 22

Tous les traitements ne peuvent bénéficier de l'allègement des formalités préalables procuré par l'institution d'un correspondant à la protection des données. Le champ d'application du III de l'article 22 a notamment été débattu lors des travaux préparatoires de la loi.

Le III de l'article 22 dispose que « les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé ».

Ainsi, les traitements concernés par cette disposition et pouvant, par conséquent, bénéficier de l'allègement des formalités préalables subséquent à la nomination d'un correspondant à la protection des données à caractère personnel sont ceux soumis aux articles 23 et 24, à savoir les traitements obéissant au régime de droit commun de la déclaration normale ou à celui de la déclaration simplifiée exception faite de ceux-ci prévoyant un transfert de données vers un pays non membre de la Communauté européenne. De plus, par une lecture a contrario de ce même article, les traitements soumis au régime de l'autorisation (article 25) ou au régime de l'avis (article 26 et 27) sont également exclus d'un tel allègement.

En effet, il semble logique de permettre un allègement des formalités limité aux traitements ne présentant pas de risques d'atteintes aux libertés et à la vie privée. Quant aux traitements prévoyant un transfert de données vers des pays tiers à la Communauté européenne, la directive du 24 octobre 1995 impose par ailleurs au pays tiers un niveau de protection adéquat ou suffisant.

Pourtant, cette « évidence » ne transparaissait pas dans l'écriture du projet de loi : l'alinéa II de l'article 22 prévoyait que « ne sont soumis à aucune des formalités préalables prévues au présent chapitre les

traitements pour lesquels le responsable du traitement a désigné un correspondant ». Or, le chapitre en question organisait l'ensemble des formalités préalables y compris les régimes d'autorisation. Cette ambiguïté, qui laissait présager une certaine insécurité juridique, a été soulevée à plusieurs reprises notamment par le député Frédéric DUTOIT lors de la séance du 29 avril 2004 de l'Assemblée nationale adoptant le projet de loi en deuxième lecture. Lors de cette même séance, un amendement n°14 fut adopté et mis fin à cette incertitude en excluant toute dispense de formalités pour les articles 25,26 et 27.

Dans une décision du 29 juillet 2004³⁷, le Conseil Constitutionnel efface à tout jamais cette ambiguïté en affirmant que « cet allègement de la procédure n'est pas possible lorsque des transferts de données à destination d'un Etat non membre de la Communauté européenne sont envisagés ; qu'en outre, il ne concerne pas les traitements soumis à autorisation ».

Le bénéfice de l'allègement des formalités préalables se trouve, par conséquent, relativement limité. Cependant, cet avantage apporté par l'institution d'un correspondant garde tout son intérêt dans la mesure où un grand nombre de personnes est concerné, la CNIL y compris.

III) Un allègement tout de même profitable à tous

A/ L'allègement, vers une facilitation de l'utilisation des traitements au sein des collectivités et des entreprises

Comme il a pu l'être précisé précédemment, le système des formalités préalables est un système lourd même si des efforts ont été fait ces dernières années pour faciliter les déclarations notamment par l'aménagement au sein de la nouvelle loi « informatique et libertés » de possibilités de transmission de déclaration par « voie électronique »³⁸ et la mise en place d'un guide disponible sur le site de la Commission³⁹.

³⁷ Conseil Constitutionnel, décision n°2004-499 DC du 29 juillet 2004

³⁸ La transmission des déclarations de traitements par voie électronique a été introduite, à la demande des entreprises, aux articles 23 I et 24 I de la loi du 6 janvier 1978.

³⁹ Guide « Comment déclarer ? », voir sur le site de la CNIL, http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/declarer-CNIL.pdf

Cette lourdeur a eu pour effet de limiter le recours à des traitements mais surtout, de cacher leur existence. Ainsi, à l'heure actuelle, des milliers de traitements clandestins fonctionnent en toute illégalité et à l'insu des personnes concernées. Alex TÜRK, actuel président de la CNIL, avait déjà posé un tel constat durant les travaux préparatoires à l'élaboration du projet de loi.

L'allégement, permis par la nomination d'un correspondant, aura sans nul doute pour conséquence de faciliter la mise en oeuvre des traitements, automatisés ou non, au sein des entreprises et des collectivités locales mais également d'accélérer la sortie de la clandestinité pour beaucoup d'entre eux déjà existants de par la grande transparence apportée par le dispositif.

Le secteur privé, dans le cadre notamment du développement du commerce électronique, et le secteur public par l'instauration de téléservices et téléprocédures dans le cadre de l'administration électronique, sont confrontés à une massification des informations. Le recours à des traitements limiterait, par conséquent, les difficultés d'archivage, de délais de traitements des dossiers et la mauvaise gestion des informations.

B/ L'allégement, vers un désengorgement de la CNIL et un contrôle a posteriori

Durant l'année 2004, 70 294 dossiers de formalités déclaratives ont été traités par les agents de la CNIL⁴⁰, ce chiffre étant en constante évolution. Ainsi, selon le rapporteur Francis DELATTRE « actuellement, 100 000 dossiers, qui ne représentent que deux années d'activité, dorment dans les caves de la CNIL, avant d'aller rejoindre les 800 000 conservés dans les entrepôts d'une société spécialisée »⁴¹.

Ne disposant que de quatre-vingt agents dont trois contrôleurs informatiques et d'un budget d'à peine sept millions d'euros, la Commission est la plus « pauvre » d'Europe⁴². Il semble donc difficile à cette dernière d'exercer ses missions dans de bonnes conditions et notamment de traiter les dossiers de formalités préalables dans des délais raisonnables.

C'est la raison pour laquelle l'allégement des formalités prévues aux articles 22, 23 et 24 est la bienvenue pour la CNIL. En effet, la nomination d'un correspondant réduira de manière considérable le travail en amont de cette dernière. De surcroît, ce correspondant pourra constituer une sorte de relais local pouvant pallier aux antennes régionales que cette dernière n'avait pu mettre en place faute de crédit suffisant. Par conséquent, le dispositif des correspondants constitue un enjeu important pour la CNIL notamment au regard des moyens humains et financiers insuffisants qui lui sont accordés. Certains auteurs vont même jusqu'à affirmer qu'en réalité « l'objectif visé semble bien être un allégement de la paperasserie pour la CNIL bien plus que pour l'entreprise⁴³ ».

⁴⁰ Chiffres révélés par le 25^{ème} rapport d'activité de la CNIL pour l'année 2004

⁴¹ Propos recueillis lors de la séance du 29 avril 2004 de l'Assemblée nationale, compte rendu analytique officiel, ref : http://www.assemblee-nationale.fr/12/cra/2003-2004/205.asp#P55_1041

⁴² En Allemagne, l'homologue de la CNIL dispose de 400 agents. Il y en a 240 au Royaume-Uni et 90 en Roumanie.

⁴³ Claire LEVALLOIS BARTH et Arnaud BELLEIL, « Le correspondant informatique et libertés : une fonction en attente de clarification », EXPERTISES n°283, juillet 2004

Le législateur, en permettant cet allègement des formalités préalables, avait pour objectif, outre le désengorgement de la CNIL, de recentrer le travail de cette dernière sur un contrôle a priori des traitements dits à risque (traitements des articles 25,26 et 27) et sur un contrôle a posteriori des traitements de manière générale⁴⁴. Pour ce dernier contrôle, preuve en est que des mesures ont été prises, notamment par la mise en place de pouvoirs de contrôle et par le renforcement des pouvoirs de sanction opérés par la loi de 2004, afin qu'il soit facilité. Les articles 19 et 44 prévoient des contrôles sur place et sur pièce : « les membres de la CNIL ainsi que les agents de ses services [...] 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 des traitements de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé »⁴⁵. Ils peuvent, dans le cadre de ce contrôle, « demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place et sur convocation, tout renseignement et toute justification utile ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la retranscription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle »⁴⁶.

Ces contrôles a posteriori tendront donc à se développer dans les années à venir. Le président de la CNIL prévoyant pour 2005 « une centaine d'opérations de ce type ». Cependant, il est malheureusement à craindre que les nouveaux pouvoirs de contrôle a posteriori ne restent lettre morte sans moyens supplétifs. Conscient d'une telle réalité, le président de la CNIL a demandé un doublement des effectifs sur quatre ans au gouvernement dans le cadre d'un rapport remis au Premier Ministre Jean-Pierre RAFFARIN en avril 2005.

L'allègement des formalités est certes un enjeu important du dispositif des correspondants mais il n'est pas le seul : l'institution aura également pour conséquence certaine de garantir le respect de la vie privée et des libertés individuelles des personnes concernées par les traitements de données à caractère personnel au sein des entreprises et des collectivités.

⁴⁴ Le rapporteur du projet de la commission des lois de l'Assemblée nationale, Francis DELATTRE, a expliqué la volonté de simplification transparaissant dans la nouvelle loi de la manière suivante : « dégagée de tâches purement bureaucratiques, la CNIL sera plus sur le terrain pour expliquer, conseiller mais aussi contrôler », voir interview dans le 25^{ème} rapport de la CNIL, p. 23

⁴⁵ Article 44 I de la loi de 1978 modifiée

⁴⁶ Article 44 III de la loi précitée

Section 2 : Une garantie du respect des libertés individuelles et de la vie privée des personnes

Aux termes du III de l'article 22, le correspondant est chargé d'assurer «le respect des obligations prévues dans la présente loi » et notamment le respect de son symbolique article 1^{er}, resté inchangé lors de la transposition de la directive européenne en droit français, qui dispose que «l'informatique doit être au service de chaque citoyen. [...] 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 et publiques ». L'un des principaux enjeux de la nomination d'un correspondant à la protection des données sera sans conteste de garantir les libertés individuelles et le respect de la vie privée des personnes au sein même des entreprises et des collectivités, impératif déjà appréhendé par certains, bien avant l'intervention du législateur.

I/ Le respect de la vie privée, un nouvel impératif pour les entreprises et les collectivités locales

Qu'il s'agisse du secteur privé ou du secteur public, le respect de la vie privée des personnes est une préoccupation de tous les instants. Des données à caractère personnel figurent, aujourd'hui, dans la plupart des traitements mis en œuvre par les entreprises ou les collectivités locales qu'il s'agisse de simples traitements de gestion du personnel ou de fichiers client en passant par les traitements nécessaires à la mise en place d'un téléservice. La problématique « informatique et libertés » est donc présente dans tous les secteurs : la prospection commerciale, la santé, la fiscalité, les télécommunications, la banque, le travail...

A titre d'exemple, Marc LOLIVIER, délégué général de la Fédération des entreprises de vente à distance (FEVAD), constate que « la vente à distance et le marketing direct reposent entièrement sur les traitements de données à caractère personnel ». Ce constat apparaît d'autant moins anodin sachant que le marketing direct représente plus du tiers des dépenses en communication des entreprises françaises et que plus de trois français sur quatre achètent à distance.

Dans les collectivités locales, la gestion des imposants services que sont l'état civil, les listes électorales, la gestion du personnel, les inscriptions scolaires, la gestion des redevances, l'action sociale, la communication, est réalisée par des moyens informatiques. Le recours aux traitements de données à caractère personnel est pour ainsi dire généralisé et les données en résultant concernent tout autant les administrés que le personnel municipal. Cette tendance est même accentuée par une volonté des collectivités de mettre en place des applications, appelées à comporter des données à caractère personnel, permettant l'accomplissement de formalités par internet afin de faciliter les démarches des administrés.

Ce recours considérable aux traitements de données à caractère personnel tendra même à se développer au regard de l'utilisation par les entreprises et les collectivités de nouveaux procédés technologiques tels que la signature électronique, la géolocalisation⁴⁷ ou encore la biométrie.

⁴⁷ A l'origine dans le contexte de l'utilisation d'appareils mobiles, comme les téléphones cellulaires, il s'agissait d'un ensemble de techniques qui permettent de déterminer leur position géographique, à partir des ondes radio qu'ils émettent. Mais les applications de géolocalisation vont aujourd'hui beaucoup plus loin. On développe notamment des services dits de « proximité » basés sur la localisation géographique des clients. On peut ainsi proposer des services personnalisés à forte valeur ajoutée : informations touristiques ou météorologiques, jeux, navigation routières, etc. Enfin, la géolocalisation est également utile en matière de balise de détresse ou de surveillance policière.

Il est donc devenu impératif pour les responsables des traitements de se conformer à la loi et la présence d'un correspondant dans leurs structures constitue un atout essentiel du fait de ses compétences et de ses missions. Concernant plus particulièrement les collectivités locales, il est possible d'aller jusqu'à dire qu'il serait un gage de sécurité pour les élus qui, parce qu'ils sont responsable des fichiers mis en œuvre, peuvent voir leur responsabilité engagée.

La stricte conformité à la loi n'est cependant pas la seule motivation conduisant à désigner un correspondant à la protection des données. En effet, une étude portant sur la perception et l'image de la CNIL menée par TNS SOFRES en juin 2004⁴⁸, a pu constater que la protection des données à caractère personnel devient, au cours des années, une problématique bien connue du grand public. Ainsi, à titre d'illustration, 45% disent connaître la CNIL, ne serait-ce que de nom et parmi ces personnes, 36% savent qu'elle a pour mission de protéger les libertés individuelles et la vie privée.

Il est donc intéressant de se poser la question de savoir si une telle conscience par la population de la problématique «informatique et libertés», qui sera grandissante au cours des années à venir, n'a pas retenu l'attention des entreprises et des collectivités locales et n'explique pas, pour une certaine partie, cette volonté de garantir la vie privée et les libertés individuelles notamment en désignant un correspondant à la protection des données à caractère personnel. En d'autres termes, on peut se demander s'il ne s'agit pas véritablement du fer de lance d'une politique de communication, comme cela l'est déjà aux Etats-Unis avec l'instauration de « Chief Privacy Officers » dans de grandes multinationales comme AOL.

Ainsi, la nomination d'un correspondant au sein des entreprises pourrait constituer un véritable argument « marketing » afin d'attirer une clientèle de plus en plus en attente du respect de sa vie privée et de ses données. Comme a pu le constater le président de l'AFCPD, Ludovic DENIS, «le défi à relever est la personnalisation sans intrusion». Cette nomination contribuerait également à accroître la confiance des salariés de l'entreprise et donc à améliorer les relations de travail.

Quant aux collectivités, la nomination d'un correspondant pourrait s'avérer un argument contrant la paranoïa toujours présente du fichage de la population, séquelle irréversible depuis l'affaire SAFARI de 1974⁴⁹, et de ce fait établir une certaine transparence, rétablir son image auprès de l'utilisateur et améliorer la confiance du personnel municipal.

Ce point de vue semble d'autant plus viable que la garantie de la vie privée et des libertés individuelles constitue une priorité pour certains pays depuis déjà longtemps.

⁴⁸ 25^{ème} rapport d'activité de la CNIL p.19, ref :<http://lesrapports.ladocumentationfrancaise.fr/BRP/054000256/0000.pdf>

⁴⁹ Le gouvernement a eu le projet d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers publics. Ainsi, d'un clic aurait-on pu tout savoir d'une personne de sa naissance à sa mort, en passant par sa scolarité, son état de santé, ses revenus, ses éventuels déboires avec la justice ou la police. A partir de cette affaire, l'opinion publique, les médias et les milieux politiques ont pris conscience des dangers qui pouvaient découler de certaines utilisations de l'informatique.

II/ Un enjeu depuis longtemps appréhendé

A/ Un enjeu depuis longtemps appréhendé en Europe et dans le monde

1) Un enjeu depuis longtemps en Europe : l'exemple allemand

L'Allemagne s'est très tôt montrée préoccupée par la problématique de protection de la vie privée et notamment par celle de protection des données personnelles, conséquence inévitable du fichage de la population opérée lors de la seconde guerre mondiale.

Dès 1977, la « loi fédérale sur la protection contre l'usage abusif des données à caractère personnel dans le cadre du traitement des données » fut votée. Cette loi, pionnière en la matière, concernait les données à caractère personnel de tous les types de fichiers de secteur public et privé stockées ou transmises en excluant les traitements des personnes morales. Elle fut abrogée par la loi fédérale du 20 décembre 1990 sur la protection des données (BDSG)⁵⁰, modifiée en 2001⁵¹, suite à un arrêt de 1983 de la Cour constitutionnelle à propos de la loi relative au recensement de la population. Dans cet arrêt, la Cour dégagait un nouveau droit constitutionnel appelé « autodétermination informationnelle » permettant à chaque individu de décider lui-même « quand et dans quelles limites les éléments de sa vie privée sont dévoilés ».

Cette innovation, extrêmement protectrice de la vie privée et des libertés, issue du système de allemand n'est pas la seule. En effet, la loi de 1990 a conservé la fonction de « détaché à la protection des données » créée dès 1977. Ce nouvel acteur, imaginé dans le cadre d'un régime double de contrôle de l'application de la loi, est chargé de veiller au respect, de manière générale, de la BDSG. Il doit notamment veiller à la conformité de l'utilisation des traitements, effectuer un contrôle préalable des traitements dits à risque, rendre accessible à toute personne en faisant la demande les données figurant dans les traitements, conseiller l'organisme qui l'a nommé mais également ses salariés sur les problématiques de protection des données. Pour lui permettre d'exercer pleinement ses missions, il dispose d'une certaine indépendance mais également de certains gages de sécurité lui permettant, par exemple de s'appuyer sur l'autorité compétente « en cas de doutes ».

La protection de la vie privée des personnes par le détaché à la protection des données est d'autant mieux garantie que sa nomination est obligatoire dès lors que plus de quatre personnes sont employées régulièrement au traitement automatisé de données à caractère personnel (ou vingt personnes pour les traitements manuels), qu'il s'agisse de traitements présentant « des risques particuliers » tels que ceux comportant des données sensibles ou ayant pour objet l'évaluation de la personne concernée. Dans le secteur public fédéral, elle devient obligatoire dès que sont en cause des traitements automatisés ou à partir de vingt personnes pour les traitements manuels. Enfin, concernant le secteur public des Länder, la majorité des lois locales impose la désignation du détaché, quelque soit le nombre de personnes employées.

Cet acteur, devenu, au fil de l'expérimentation, l'interlocuteur préféré des autorités de contrôle allemandes comme des personnes concernées par les traitements, remporte un franc succès aujourd'hui. Rien d'étonnant alors qu'il ait inspiré la directive européenne et que d'autres pays tels que la Suède⁵² ou les Pays-Bas⁵³ l'aient très rapidement introduit dans leur propre système juridique de protection des données à caractère personnel.

⁵⁰ Bundes-Datenschutzgesetz du 20 décembre 2000 (BGBl IS 2954), ref : <http://www.goethe.de>

⁵¹ Bundes-Datenschutzgesetz du 18 mai 2001 (BGBl IS 904), ref : <http://www.goethe.de>

⁵² Le dispositif du détaché à la protection des données à caractère personnel a été introduit par la nouvelle loi relative à la protection des données personnelles du 24 octobre 1998 portant modification de la loi de 1973, *Personuppgiftslag*, SFS 1998 :204, <http://rixlex.riksdagen.se/>

⁵³ Le dispositif du détaché à la protection des données à caractère personnel a été introduit lors de la refonte de la loi hollandaise relative à la protection des données à caractère personnel du 23 novembre 1999 suite à la transposition de la directive, *Wet bescherming persoonsgegevens* n°25892 du 23 novembre 1999

2) Un enjeu depuis longtemps appréhendé dans le monde : les exemples américains et canadiens

a- Aux Etats-Unis

Dés 1973, date à laquelle éclata le scandale « Watergate » révélant l'utilisation par l'administration de fichiers publics afin de lutter contre les ennemis du président NIXON, les Etats-Unis prirent vite conscience de l'importance de la protection de la vie privée. Le véritable débat public qui s'ensuivit conduisit à l'adoption en 1974 du « Privacy Act »⁵⁴. Cette loi fédérale, encore aujourd'hui, la plus complète en matière de protection de la vie privée est destinée à protéger la vie privée des individus contre l'utilisation abusive d'enregistrements détenus par ces administrations et permettant à chacun d'accéder aux enregistrements le concernant. Elle ne porte cependant que sur les données personnelles enregistrées par les agences du gouvernement fédéral et ne s'applique pas aux fichiers du secteur privé, aux fichiers de la CIA et à ceux des services de police.

Par la suite, plusieurs lois d'application sectorielles ont été votées afin de la compléter : la loi sur les données financières de 1978 (« Right to Financial Privacy Act »)⁵⁵, les lois de 1984 sur le droit au respect à la vie privée en matière d'éducation et de famille (« The Family Educational Rights and Privacy Act »)⁵⁶ et sur les communications par câble (« Electronic Communications Privacy Act »⁵⁷), la loi de 1988 sur les locations de cassettes vidéo (« Video Privacy Protection Act »⁵⁸) ainsi que la loi de 1998, qui protège la vie privée des mineurs de moins de treize ans (« Children's Online Privacy Protection Act »)⁵⁹.

Malgré un système américain de protection des données personnelles et de la vie privée reposant, en majeure partie, sur l'autorégulation de l'opinion publique et des entreprises, le débat s'essouffla vite laissant place à une utilisation massive et extrêmement libérale des données à caractère personnel par les entreprises.

⁵⁴ The Privacy Act 5 U.S.C § 552a, As amended By Public Law Ref: <http://www.usdoj.gov/04foia/privstat.htm>

⁵⁵ The Right to Financial Privacy Act 12 U.S.C§3401-342,Ref: <http://www.fdic.gov/regulations/laws/rules/6500-2550.html>

⁵⁶ The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99, Ref: www.epic.org/privacy/education/ferpa.html

⁵⁷ The Electronic Communications Privacy Act, 18 U.S.C 2510, PUBLIC LAW 99-508--OCT. 21, 1986 100 STAT. 1848, Ref: <http://cio.doe.gov/Documents/ECPA.HTM>

⁵⁸ The Video Privacy Protection Act 18 U.S.C. § 2710, Public Law 100-618, Ref: www.epic.org/privacy/vppa/

⁵⁹ Children's Online Privacy Protection Act, Sec. 1301-1308, ref: <http://www.ftc.gov/ogc/coppa1.htm>

Puis, à la suite d'un atelier public consacré aux incidences du profiling⁶⁰ sur la vie privée⁶¹, organisé à la demande du vice président Al Gore par le Département du Commerce (Federal Trade Commission) en novembre 1999 mais surtout à la suite du très médiatisé scandale « Double Click »⁶², le débat repris. Les entreprises prirent alors conscience des attentes des consommateurs en terme de protection des données personnelles et de respect la vie privée et des enjeux qu'elles impliquent : la fonction de « Chief Privacy Officer » ou « Corporate Chief Officer » (CPO) était née.

Selon le Privacy & American Business (P&AB)⁶³, service d'information publiant des rapports et une lettre d'information sur la protection des données, le CPO est « responsable de la coordination de toutes les activités de l'entreprise ayant des implications liées à la vie privée, et doit surveiller toutes ses productions, services et systèmes informatiques pour s'assurer du sérieux de ses pratiques de protection des données ». Le CPO, à la différence du correspondant à la protection des données, doit veiller aux intérêts de l'organisme qui le nomme et doit réduire les risques liés à l'utilisation de données personnelles voire développer au sein de l'entreprise un code de bonnes conduites qui sera, bien évidemment exploité en terme d'image et de marketing. Son objectif premier est de restaurer la confiance du consommateur sans laquelle le chiffre d'affaire s'effondrerait.

Qui aurait pu imaginer qu'un Etat dénué de législation de portée générale relative à la protection des données personnelles et d'autorité nationale de protection de la vie privée⁶⁴ aurait pu appréhender l'enjeu de la garantie de la protection de la vie privée ? Le dispositif rencontre pourtant un vif succès aux Etats-Unis où on peut compter, déjà en 2002, près de 500 CPO⁶⁵ dont certains sont élevés au rang de célébrités nationales⁶⁶.

b- Au Canada

Le Canada compte deux lois fédérales sur la protection des « renseignements personnels » : la loi sur la protection des renseignements personnels du 1^{er} juillet 1983⁶⁷ applicable aux services publics canadiens et la loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)⁶⁸ dont l'entrée en vigueur s'est effectuée par étapes. En effet, à compter du 1^{er} janvier 2001, cette dernière était applicable aux organisations de compétence fédérale dans le cadre de leurs activités commerciales telles que les transporteurs aériens, les banques ou encore les organismes de radiodiffusion, puis dès le 1^{er} janvier, aux renseignements personnels relatifs à la santé recueillis par les organisations précitées et enfin

⁶⁰ Technique de marketing qui consiste à analyser le profil des consommateurs pour déterminer leurs motivations, leurs centres d'intérêt, leur tranche d'âge, leur profession, afin de mieux répondre à leurs attentes. Cette technique est très utilisée sur les sites web pour analyser le comportement des visiteurs et modifier en conséquence les pages du site.

⁶¹ «Public workshop on online profiling», ref: <http://www.ftc.gov/bcp/workshops/profiling/online.pdf>

⁶² DoubleClick est une des plus grandes régies publicitaires américaines sur internet. En juin 1999, elle avait fait connaître son intention de fusionner avec la société Abacus Direct, propriétaire de l'une des plus grandes bases de données sur les consommateurs américains, afin d'obtenir des informations particulièrement précises sur les internautes par recoupement des fichiers. Alertée des risques en terme de protection de la vie privée, l'opinion publique a boycotté la société faisant chuter le cours de l'action « Double Click ».

⁶³ Voir leur site : <http://www.pandab.org/>

⁶⁴ La Commission Fédérale pour le commerce (Federal Trade Commission) en charge de la concurrence et de la protection des consommateurs compte, cependant, parmi ses services, un groupe d'experts spécialisés dans les questions de protection de la vie privée.

⁶⁵ Chiffre recueilli lors du Chief Privacy Officer Conférence à Toronto en février 2002 ref : http://www.privcom.gc.ca/speech/02_05_a_020212_e.asp

⁶⁶ Ray Everett Church et Jules Polonetsky, membres fondateurs du Chief Privacy Officer Council, créé en août 2002, sont surnommés par la presse américaine : « privacy czar ».

⁶⁷ Loi sur la protection des renseignements personnels (L.R. 1985, ch. P-21) Ref : <http://lois.justice.gc.ca/fr/P-21/87016.html>

⁶⁸ Loi sur la protection des renseignements personnels et les documents électroniques Ref : <http://lois.justice.gc.ca/fr/P-8.6/>

à compter du 1^{er} janvier 2004, à toutes les organisations du secteur privé sauf dans les provinces qui ont adoptées des lois similaires à la loi fédérale.

Les entreprises canadiennes, bien avant l'intervention de la LRPDE et notamment sa généralisation à l'ensemble du secteur privé en 2004 avaient compris qu'il était impératif de protéger la vie privée des personnes et notamment la vie privée des consommateurs par une bonne gestion des renseignements personnels. C'est ainsi que dès 1999, les grandes structures se dotèrent, sous l'influence de leurs voisins américains, de CPO autrement appelés « responsable de la protection des renseignements personnels » voire même, consacrèrent certains de leurs services à la protection de la vie privée. Les codes de bonne conduite se multiplièrent ainsi que les conférences de CPO.

Ce succès indéniable, preuve du soucis de garantir le respect des libertés individuelles et de la vie privée des canadiens, fut confirmé par la LRPDE de 2004. En effet, cette dernière institue cette fonction officiellement dans son texte en prévoyant, parmi ses dix principes fondateurs, qu'une organisation « est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci dessous ». Cette loi va donc plus loin en imposant aux organismes une obligation de désignation et en aménageant une véritable responsabilité.

B/ Un enjeu depuis longtemps appréhendé en France

En France, depuis déjà quelques années, certaines entreprises ont mis en place au sein de leurs structures un poste de « délégué à la protection des données », afin de garantir le respect de la vie privée à leurs clients et à leurs salariés. Largement inspiré de la fonction de « Chief Privacy Officer », créée et largement expérimentée par les Etats-Unis, ce nouvel acteur a fini de convaincre les chefs d'entreprise de son utilité : le respect de la vie privée est bon pour les affaires !

Ainsi, chez EXPERIAN, société spécialisée dans les systèmes décisionnels et le traitement de l'information, un poste de délégué à la protection des données pour l'Europe de l'Ouest a été créé dès 2001. Ce poste est directement placé sous la responsabilité du directeur juridique et consiste en la gestion des traitements nominatifs internes, des traitements nominatifs externes tels que les bases de données géomarketing ainsi que le conseil aux clients.

Cette stratégie a aussi été appliquée au sein de la Banque de France qui, à la suite de l'entrée en vigueur d'une charte d'utilisation des Nouvelles Technologies de l'Information et de la Communication (NTIC) en mars 2003 sous l'impulsion d'un rapport de la CNIL de 2001 relatif à la cybersurveillance⁶⁹, a désigné un délégué à la protection des données. Ce poste, rattaché directement au délégué de la déontologie, a pour mission de « sensibiliser l'ensemble des responsables métier aux limites fixées par la loi et la jurisprudence en matière d'informatique et des libertés, ainsi que de conseiller les responsables des fichiers sur les formalités à accomplir vis-à-vis de la CNIL ».

⁶⁹ Rapport d'étude et de consultation publique « La cybersurveillance des salariés dans l'entreprise », Hubert BOUCHET, mars 2001, ref : <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/cybersurveillance.pdf>

Garantir le respect de la vie privée est certainement l'enjeu le plus symbolique de la mise en place du correspondant à la protection des données. Cependant, il est à noter que cette garantie apportée par le correspondant reste limitée à certains traitements, comme cela est le cas pour l'allègement des formalités préalables. En effet, seuls les traitements ne portant pas manifestement atteinte à la vie privée et aux libertés, à savoir les traitements soumis aux formalités des articles 23 et 24 pourront bénéficier de cet avantage. En outre, il semble opportun de se demander s'il ne serait plus sécurisant de pouvoir confier la gestion des traitements quel qu'ils soient au correspondant sans pour autant leur faire bénéficier d'un quelconque allègement des formalités. Ainsi, la protection de la vie privée et des libertés apportée par ce nouvel acteur prendrait tout son sens.

Ajoutons que même si ces enjeux sont très importants, il n'en reste pas moins qu'ils restent limités par le champ d'application du III de l'article 22 précédemment évoqué mais également par le fait que la nomination d'un correspondant reste facultative.

CHAPITRE 2:

Les missions du correspondant, des missions essentielles à la protection des données à caractère personnel

Outre l'allègement des formalités obligatoire et la garantie de la vie privée et des libertés individuelles par le correspondant à la protection des données à caractère personnel, la question de l'utilité d'une telle fonction trouve également une réponse au regard des missions qui lui sont confiées. En effet, qu'il s'agisse de missions conférées explicitement par la loi de 1978 modifiée (section 1) ou de missions plus implicites (section 2), elles s'avèrent être essentielles à la protection des données à caractère personnel.

Section 1 : Les missions expressément conférées par la loi

La loi de 1978 distingue de manière très sommaire deux catégories de missions : d'une part, veiller au respect de la loi « informatique et libertés » et d'autre part, tenir un registre des traitements mis en œuvre au sein de l'organisme qui l'a nommé. Leur contenu devrait être précisé par le décret d'application en cours d'élaboration.

I) Veiller au respect de la loi « informatique et libertés »

La loi de 1978, dans son III de l'article 22, dispose que le correspondant à la protection des données est « chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi ». Cette mission très générale mais essentielle de veille au respect de la loi consiste, en pratique, en un véritable travail de conseil, de médiation, d'alerte et de mise en garde de la part du correspondant. Jean-Marie COTTERET⁷⁰, interrogé à propos de ces mêmes missions, considère lui-même que « conseil en amont, pédagogie, audit et médiation devront ainsi accompagner un rôle d'alerte du

⁷⁰ Jean-Marie COTTERET est le commissaire en charge des secteurs « Collectivités locales » et « Audiovisuel » au sein de la CNIL. Voir son interview dans le 25^{ème} rapport d'activité de la CNIL p.27

responsable du traitement sur les irrégularités constatées ». Veiller au respect de la loi consiste également en une tâche pouvant passer pour insignifiante mais pourtant essentielle : la tenue d'un registre des traitements mis en œuvre dans l'entreprise ou la collectivité.

A/ Des missions de conseil, de médiation, d'alerte et de mise en garde

1) Mission de conseil

Cette mission consistera pour le correspondant à la protection des données à caractère personnel à conseiller et à faire toutes recommandations utiles au responsable du traitement sur la mise en œuvre des traitements pour lesquels il a été désigné. L'exercice de cette mission suppose donc que le correspondant soit consulté, au préalable, sur tout projet de traitements de données à caractère personnel.

Selon la doctrine de la CNIL, il devra proposer « les solutions permettant de concilier protection des libertés individuelles et intérêt légitime des professionnels »⁷¹.

Il semble également que son rôle de conseil puisse aller au delà des traitements précités. Son intégration au sein de l'entreprise ou des collectivités locales aura certainement pour répercussion d'être sollicité sur différentes « problématiques informatique et libertés » par le responsable mais aussi par des salariés. L'expérimentation du correspondant en Allemagne, en Suède, au Luxembourg ou encore aux Pays-Bas a révélé plus d'une fois cet état de fait.

Il s'agit donc d'un des rôles essentiels du correspondant car situé en amont : ne vaut-il mieux pas, comme l'énonce un célèbre adage, « prévenir que guérir ».

2) Mission de médiation

De par leur droit d'accès et leur droit de rectification institués par la loi de 1978 aux articles 39 et 40, les personnes concernées par des traitements de données à caractère personnel ont « le droit d'interroger le responsable d'un traitement de données à caractère personnel » en vue notamment d'obtenir des informations relatives aux finalités du traitement, aux catégories de données traitées ou encore aux catégories de destinataires. Elles peuvent exiger de ce dernier « que soient, selon les cas, rectifiées complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

Le correspondant revêt alors le rôle de médiateur lorsqu'il reçoit les demandes et réclamations de ces personnes qui seront, en règle générale des clients, des usagers ou des salariés. En effet, le III de l'article 22 précise que ce dernier « doit tenir une liste des traitements effectués immédiatement accessible à toute personne qui en fait la demande ».

Ce rôle de médiateur fera certainement du correspondant, l'interlocuteur privilégié des salariés et des personnes concernées dans le cadre de leurs demandes d'accès et de rectification. Cette position serait d'autant plus confortée si comme dans la loi allemande et la loi néerlandaise, était prévue une obligation

⁷¹ Propos recueillis dans le « FAQ correspondant informatique et libertés », <http://www.cnil.fr/index.php?1821>

au secret professionnel pour le correspondant. Les détachés allemand et néerlandais sont tenus, en effet, de ne pas révéler l'identité de la personne concernée ainsi que la nature des informations portées à sa connaissance lors des demandes d'accès et de rectification.

Cette mission délicate confiée au correspondant a donc pour mérite de renforcer les droits des personnes sur leurs données personnelles, en plus des mesures prises par la loi. L'identification d'un interlocuteur unique rend efficace le traitement des plaintes et des requêtes formulées par les personnes concernées par les traitements.

3) Mission d'alerte et de mise en garde

Une des missions les plus essentielles mais également les plus craintes par les organismes désireux d'introduire ce nouvel acteur au sein de leurs services, est la mission d'alerte et de mise en garde du responsable du traitement sur les irrégularités constatées dans la mise en œuvre des traitements.

Cette mission induit bien évidemment une veille juridique de la conformité à la loi de 1978 de l'utilisation des traitements mis en œuvre. Cette conformité s'appréciera notamment au regard des principes directeurs de la protection des données à caractère personnel énoncés pour la majeure partie dans le chapitre II de la loi consacré aux conditions de licéité des traitements de données à caractère personnel⁷².

C'est ainsi que dans l'hypothèse d'éventuels problèmes détectés, le correspondant devra alerter le responsable du traitement afin que ce dernier fasse cesser ces irrégularités. Cette mission d'alerte est bien accueillie par les entreprises et collectivités. En revanche, la mise en garde l'est moins. En effet, la loi précise que le correspondant «peut saisir la CNIL des difficultés qu'il rencontre dans l'exercice de ses missions», la non prise en compte de l'alerte déclenchée par le correspondant pouvant constituer une de ses difficultés. La loi va même plus loin en disposant «qu'en cas de non respect des dispositions de la loi, le responsable du traitement peut être enjoint par la CNIL de procéder aux formalités prévues aux articles 23 et 24». C'est dans cette perspective que beaucoup de responsables de traitements préféreront se soumettre aux formalités obligatoires plutôt que d'introduire une «épée de DAMOCLES» au dessus de leur tête.

⁷² Parmi les grands principes directeurs du chapitre II, figurent le principe de loyauté et de licéité de la collecte, le principe de finalité spécifique, explicite et légitime du traitement, le principe de proportionnalité des données par rapport aux finalités du traitement, le principe d'exactitude et de mise à jour des données et enfin le principe de conservation proportionnée à la finalité. Ces principes sont énoncés à l'article 6 de ce même chapitre.

Concernant la saisine de la CNIL par le correspondant dans l'hypothèse de difficultés rencontrées lors de ses missions, la loi reste floue sur le fait de savoir si cette dernière doit être notifiée au préalable au responsable du traitement. Il ne semble pas que le fait de ne pas notifier au responsable du traitement la saisine de la CNIL soit l'orientation prise par le législateur. En effet, le système des correspondants n'a pas été conçu dans une perspective répressive mais plutôt pédagogique. Cependant, dans certains cas d'atteinte grave aux libertés individuelles et à la vie privée, ne serait-il pas possible d'envisager une saisine directe de la CNIL afin de conserver les preuves de la flagrance. La question est posée...

Ce dilemme ne semble pas poser de réelles difficultés pour le secteur public. En effet, aux termes de l'article 40 du Code de procédure pénale, « toute autorité constituée, tout officier ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès verbaux et actes qui y sont relatifs ». Les violations de la loi « informatique et libertés » constituant des délits, il serait donc envisageable pour le correspondant d'aller plus loin qu'une simple saisine de la CNIL en saisissant le Procureur de la République et ce, sans le notifier au responsable des traitements.

Il est à craindre que cette mission d'alerte et surtout de mise en garde associée au caractère facultatif du correspondant dissuade un certain nombre de postulants du fait de la délicatesse de cette dernière : en effet, malgré une indépendance du correspondant établie par la loi, les liens hiérarchiques demeurent et il paraît peu naturel pour la plupart des salariés de « mettre en garde son patron » voire de le dénoncer à l'autorité de contrôle.

B/ Des missions exercées dans le cadre d'une étroite collaboration avec la CNIL

Toutes les missions précitées ne seraient pas vraisemblablement effectives si leur exercice était totalement détaché d'une collaboration entre le correspondant et la CNIL. En effet, la désignation d'un correspondant ne prive pas la Commission de tout pouvoir de contrôle et d'information.

C'est la raison pour laquelle, la loi a aménagé la possibilité pour le correspondant de « saisir la CNIL des difficultés qu'il rencontre lors de l'exercice de ses missions ».

Ces difficultés peuvent tout simplement consister en des problèmes relatifs à l'interprétation de la loi. En effet, bien que destiné à devenir expert dans le domaine de la protection des données à caractère personnel, bon nombre de problématiques « informatique et libertés » restent inabordées par l'autorité de contrôle, il serait donc dangereux pour le correspondant de se prononcer sur ces dernières sans obtenir, au préalable, les conseils de la CNIL. La législation allemande l'a bien compris en aménageant une possibilité pour le détaché à la protection des données personnelles de saisir l'autorité de contrôle « en cas de doutes ».

Ces difficultés peuvent également se révéler plus préoccupantes et consistaient en un refus de la part du responsable du traitement de mettre en conformité avec la loi de 1978 modifiée les traitements lors de leur mise en œuvre. Dans cette hypothèse, le soutien de la CNIL s'avère indispensable pour le correspondant. La loi suédoise, très consciente de telles difficultés, est allée jusqu'au bout de ce raisonnement en rendant obligatoire la saisine dans une telle espèce.

Cette nécessaire collaboration entre le correspondant à la protection des données et la CNIL ira t-elle jusqu'à une obligation de rendre des comptes mise à la charge de ce dernier, comme cela est le cas dans d'autres pays européens. Aux Pays-Bas, par exemple, le détaché à la protection des données doit rédiger un rapport annuel établissant un bilan de son activité. Ce rapport doit être remis au responsable des traitements mais doit également être mis à la disposition de l'autorité de contrôle voire communiqué systématiquement dans certains cas.

II) La tenue d'un registre des traitements

La loi reste assez imprécise sur cette mission. Le III de l'article 22, dans son troisième alinéa, dispose que le correspondant à la protection des données « tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande ». Ce sera donc au décret d'application de préciser cette tâche très importante incombant au correspondant. Cependant, au regard de l'utilité de ce registre assignée par le législateur, il paraît possible de déduire quel pourra être son contenu mais également quelles pourront être les règles régissant sa tenue.

A/ Contenu du registre

1) Les traitements figurant dans la liste

Tout d'abord, la loi précise que ce registre est « une liste des traitements effectués ». Cependant, à la lecture de l'ensemble des dispositions du III de l'article 22, il est difficile de savoir s'il s'agit de l'ensemble des traitements « effectués » au sein de l'organisme ou seulement des traitements soumis « aux formalités prévues aux articles 23 et 24 ». En effet, la lecture du premier alinéa ne semble concerner que la désignation du correspondant et l'allégement des formalités préalables alors que le troisième alinéa semble être général du fait de l'expression « traitements effectués ». La directive n'est pas plus précise puisque cette dernière parle de « traitements effectués par le responsable du traitement ».

Cette ambiguïté juridique n'est pas sans conséquences : si seuls les traitements soumis aux articles 23 et 24 doivent figurer dans ce registre, son utilité se trouvera relativement limitée. Nous nous trouverons donc en face d'une liste incomplète et l'objectif initial assigné à un tel registre par le législateur, à savoir limiter les fichiers clandestins et « révéler à l'autorité de contrôle les fichiers auparavant non déclarés »⁷³ perdra tout son sens. De plus, il est intéressant de se pencher sur la question de savoir si les missions précédemment exposées, et notamment la mission de médiation, ne sont pas en partie tronquées par le fait que la liste ne pourrait concerner que les traitements relevant des articles 22 à 24, à savoir les traitements ne présentant pas de risques d'atteinte à la vie privée et donc les moins susceptibles de comporter des données dites sensibles.

2) Les informations figurant sur le registre

L'article 18 de la directive apporte quelques précisions sur le type d'information devant figurer dans la liste des traitements du correspondant : il dispose que le détaché à la protection des données doit « tenir un registre [...], contenant les informations visées à l'article 21 paragraphe 2 ». Cet article énumère les informations contenues dans le registre tenu par l'autorité de contrôle à savoir :

- « le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
- la ou les finalités du traitement ;
- une description de la ou des catégories de personnes concernées et des données ou des catégories de données qui s'y rapportent ;
- les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;
- les transferts de données envisagés vers des pays tiers ;

⁷³ Rapport DELATTRE n°1537 du 13 avril 2004, p.24

- une description des mesures prises pour assurer la sécurité des traitements ».

Ces informations semblent donc être identiques à celles susceptibles de figurer sur le registre du correspondant à une nuance près : les traitements envisageant des transferts de données vers des pays tiers étant exclus par le III de l'article 22, la référence à ces transferts n'a pas lieu d'être.

B/ Règles régissant la tenue du registre

La première règle régissant la tenue d'un tel registre résulte d'une disposition de la loi: cette liste doit être « immédiatement accessible à toute personne en ayant fait la demande ». La liste des traitements constitue, en effet, la base de référence de l'exercice des droits d'accès et de rectification des personnes concernées par les traitements.

La seconde règle résulte d'un raisonnement logique : l'élaboration d'une telle liste par le correspondant suppose que le responsable des traitements lui ait fourni les moyens de pouvoir la réaliser, à savoir fournir les informations relatives aux divers traitements pouvant être mis en œuvre au sein de l'organisme. Un véritable travail de collaboration entre le correspondant et le responsable des traitements devrait donc s'instaurer. Cette règle est d'autant plus importante lorsque des traitements ont été mis en œuvre avant l'arrivée du correspondant. Cette collaboration entre le correspondant et le responsable du traitement a paru essentielle en Allemagne. La loi fédérale relative à la protection des données est même allée plus loin que la simple fourniture d'informations relatives aux traitements existants en disposant, dans son troisième alinéa de l'article 4(f), que « les organismes publics et privés doivent soutenir le détaché à la protection des données, dans l'accomplissement de ses fonctions, et en particulier, dans la mesure où cela est nécessaire à l'accomplissement de ses fonctions, mettre à sa disposition du personnel auxiliaire ainsi que des locaux, du matériel, des appareils et d'autres moyens ».

Concernant les autres règles, il est possible de les déduire au regard de l'utilité assignée au registre. Comme il a pu l'être précisé quelques lignes au dessus, la liste des traitements tenue par le correspondant est destinée à révéler à la CNIL les traitements clandestins. Ainsi, de manière logique, cette liste devrait être mise à disposition de la CNIL afin de servir de base de référence à la liste des traitements tenue par cette dernière conformément à l'article 31 de la loi⁷⁴. Par conséquent, cela suppose que le registre du correspondant soit fiable. Pour cela, il se devra de le mettre à jour, dans l'hypothèse par exemple de modifications apportées aux traitements ou de suppression, afin d'attester de l'exactitude des informations qu'elle contient.

⁷⁴ L'article 31 de la loi de 1978 modifiée dispose que « la commission met à disposition du public la liste des traitements automatisés ayant fait l'objet des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26 ». Cette liste est disponible sur le site même de la CNIL, <http://www.cnil.fr/index.php?id=29>

Section 2 : Une mission implicite : la diffusion de la « culture informatique et libertés »

Outre la tenue d'un registre et la veille au respect des dispositions de la loi de 1978 modifiée, le correspondant s'est vu confier une mission par le législateur ne figurant pourtant pas dans la loi : la diffusion de la « culture informatique et libertés ». Dans une conférence de presse du 20 avril 2005 présentant son nouveau rapport d'activité pour l'année 2004⁷⁵, la CNIL a déclaré, en effet, que le correspondant « aura un rôle essentiel dans la diffusion de la culture informatique et libertés au sein de l'organisme l'ayant désigné ».

I) Approche de la notion de « culture informatique et libertés »

Le terme « culture informatique et libertés » est utilisé à tout va par la CNIL elle-même comme par les auteurs sans forcément préciser en quoi elle peut bien consister. Selon l'anthropologue Edward B. Tylor, *"la culture est un tout complexe qu'inclut les connaissances, les croyances, l'art, la morale, le droit, les coutumes, ainsi que toutes autres dispositions et habitudes acquises par l'homme en tant que membre d'une société"*⁷⁶. Que peut-il se cacher derrière le terme mystérieux de « culture informatique et libertés ». Est-elle une véritable culture ou plutôt un abus de langage ?

Tout d'abord, il apparaît de manière évidente que la « culture informatique et libertés » consiste en l'esprit de la loi de 1978 relative à l'informatique, aux fichiers et aux libertés parfaitement résumé dans son article premier, resté inchangé lors de la transposition de la directive : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité, ni à la vie privée, ni aux libertés individuelles ou publiques ». Cet esprit apparu dès 1974 après l'affaire SAFARI a été un véritable fil conducteur pour d'autres pays ayant pris conscience de l'intérêt de protéger la vie privée face à une société grande consommatrice de données à caractère personnel.

Puis, la « culture informatique et libertés » consiste également en la doctrine de la CNIL, seule autorité de contrôle française dont l'impact n'est pas négligeable. La doctrine consiste en l'opinion de l'ensemble des auteurs. Ici, il n'y a qu'un seul et unique auteur : la CNIL. Dominique PERBEN, Garde des Sceaux parlait, ainsi, de « culture CNIL, le soucis de répondre aux exigences dont la CNIL est garante » lors de la séance du 29 avril 2004 à l'Assemblée nationale.

Cette doctrine se traduit par l'élaboration d'un rapport annuel d'activité conformément au dernier alinéa de l'article 11 de la loi⁷⁷. Ce rapport aborde la problématique « informatique et libertés » secteur par secteur, contient les délibérations importantes rendues au cours de l'année et la position de la CNIL sur le

⁷⁵ Conférence de presse du 20 avril 2005 présentant le 25^{ème} rapport d'activité de la CNIL pour l'année 2004, ref : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/DP-conf2005.pdf

⁷⁶ 1924 [orig. 1871] Primitive Culture. 2 vols. 7th ed. New York: Brentano's.

⁷⁷ Article 11 : « [...] La commission présente chaque année au Président de la République, au Premier Ministre et au Parlement un rapport public rendant compte de sa mission ».

déploiement de certains grands projets informatiques français, ainsi que l'état actuel du droit de la protection des données à caractère personnel à travers le monde.

La doctrine se traduit aussi par les décisions rendues par la CNIL, qu'il s'agisse de ses délibérations de manière générale, de ses avis, de ses délibérations établissant les normes simplifiées ou les exonérations de déclaration, ses avis sur la conformité à la présente loi des projets de règles professionnelles et des produits ou procédures tendant à la protection des données à caractère personnel, ou à l'anonymisation de ces données. Il s'agit d'une sorte de jurisprudence CNIL.

Cette doctrine trouve une grande diffusion à travers le site internet de la Commission mais également par de la médiatisation de ses membres. Bon nombre d'interviews sont effectivement consacrées aux problématiques « informatiques et libertés ».

Derrière cette « culture informatique et libertés », se trouve donc bien la doctrine de la CNIL puisque on assimile la culture au « nécessaire message de la CNIL ». Le terme « culture » a, en effet, une portée avant tout symbolique.

II) Un rôle avant tout pédagogique

Malgré les efforts de la CNIL pour vulgariser la protection des données à caractère personnel auprès des professionnels et surtout du grand public par un site web performant et compréhensible et par une médiation accrue, beaucoup de personnes restent encore ignorantes de leurs droits et de leurs obligations en matière de protection des données. Faute de moyens financiers et humains, l'institution du dispositif des correspondants s'avère le meilleur moyen de diffuser la doctrine de la CNIL. En effet, il est certain que le développement d'un réseau de correspondants et la sensibilisation accrue du personnel aux problématiques « informatiques et libertés » permettra d'assurer une meilleure connaissance de la loi applicable par les responsables des traitements comme par leurs salariés. Cette introduction des correspondants pourrait même aboutir jusqu'à la reconnaissance d'un savoir faire voire d'une profession.

Ce rôle pédagogique n'est pas ignoré dans d'autres pays ayant introduit un « détaché à la protection des données à caractère personnel ». En Allemagne, par exemple, une des missions essentielles du « détaché » est de « familiariser, grâce à des mesures appropriées, les personnes affectées au traitement avec les dispositions de la loi et avec les autres dispositions en vigueur dans le domaine de la protection des données ainsi qu'avec les exigences particulières de la protection des données »⁷⁸. Quant aux Pays-Bas, ce rôle pédagogique se traduit par la rédaction de codes de bonne conduite en matière de données personnelles qu'il est chargé de diffuser au sein de l'organisme qu'il l'a nommé. Enfin, en Suède, la diffusion en interne des informations sur la loi relative à la protection des données constitue une mission expressément conférée par la loi.

En France, ce rôle pédagogique du correspondant à la protection des données à caractère personnel par la diffusion de la doctrine de la CNIL avait été appréhendé dès les travaux préparatoires et constituait même une des raisons pour lesquelles le Sénat avait changé l'orientation de la loi en introduisant ce nouveau dispositif. Alex TÜRK, rapporteur au nom de la commission des lois estimait, en effet, que « nous

⁷⁸ article 4(g) de la loi fédérale allemande relative à la protection des données à caractère personnel

disposons là d'un canal idéal pour faire passer le nécessaire message pédagogique de la CNIL vers l'ensemble des utilisateurs »⁷⁹.

L'importance de ce rôle fut confirmé dans le rapport DELATTRE : « L'objectif poursuivi par ce nouveau dispositif est avant tout pédagogique puisque l'introduction de correspondants devrait favoriser l'application de la loi du 6 janvier 1978 en facilitant sa prise en considération par les entreprises. En effet, une meilleure circulation de l'information entre le correspondant, les personnes chargées au sein de l'entreprise de recourir ou de mettre en place les traitements et la CNIL devrait contribuer, sans conteste, à l'amélioration de la loi par les entreprises »⁸⁰.

III) Le correspondant, symbole d'un phénomène de société ?

Le fait que le correspondant à la protection des données à caractère personnel soit vecteur d'une « culture informatique et libertés » et qu'il s'agisse d'une véritable nécessité est tout à fait significatif de la période dans laquelle nous vivons : l'ère « Big brother is watching you »⁸¹.

Cette ère fait référence au roman «1984 »⁸² dans lequel Georges ORWELL décrit un pays totalitaire dirigé par un parti unique dans lequel Big Brother, dont le portrait est affiché partout, semble surveiller tout le monde. Toute liberté individuelle y est exclue. La police de la pensée torture, extorque de faux témoignages, rééduque et exécute ceux qui ont une attitude qui ne correspond pas à la norme établie. Les appartements sont équipés d'un télécran qu'il est impossible d'éteindre, qui diffuse la propagande officielle mais qui est également un moyen pour le Parti de surveiller le citoyen.

En France, cette crainte concernait, à l'époque de l'affaire SAFARI, le fichage de la population par l'interconnexion des fichiers publics. Elle s'est, aujourd'hui, focalisée sur le possible fichage du consommateur par les entreprises communément appelé « profiling ». Big Brother, qu'il soit représenté par les grandes entreprises que par l'Etat lui-même, est partout. Certains vont même jusqu'à organiser des cérémonies de remise de prix à tous ceux portant atteinte gravement à la vie privée : les « Big Brothers Awards » ou « Trophées de la surveillance ».⁸³

⁷⁹ Compte-rendu intégral du Sénat du 1^{er} avril 2003 p.39, <http://www.senat.fr>

⁸⁰ Rapport DELATTRE n°1537 du 13 avril 2004, p.24

⁸¹ « Big Brother vous surveille »

⁸² Georges ORWELL, « 1984 », 1949, Gallimard « Folio », 1972, Paris, traduction de l'anglais par Amélie AUDIBERTI

⁸³ Voir leur site : www.bigbrotherawards.eu.org/

Cet état d'esprit dans lequel est plongé le grand public ne pourra que s'atténuer avec l'arrivée du correspondant. Ce dernier, de par son action de sensibilisation au sein de l'organisme qui l'a désigné, fera prendre conscience du respect de plus en plus accru de la vie privée et des libertés individuelles. De plus, il constituera un gardien de la vie privée et des libertés individuelles à visage humain.

En effet, il semble que, contrairement à la pensée véhiculée par ce phénomène de société, la vie privée est devenu un véritable « sanctuaire » de plus en plus protégé. En effet, par une décision du 13 mars 2003 relative à la loi sur la sécurité intérieure⁸⁴, le Conseil Constitutionnel a confirmé la valeur constitutionnelle du droit au respect de la vie privée : « il [...] appartient [au législateur] notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés ». Il l'avait déjà évoqué dans sa décision du 18 janvier 1995 relative à la vidéo surveillance⁸⁵ mais il ne s'agissait pas encore d'une consécration constitutionnelle.

Cette consécration paraissait toutefois imminente : le Haut Conseil avait déjà, dans sa décision du 20 janvier 1993 relative au service anti-corruption⁸⁶, fait entrer la loi du 6 janvier 1978 dans le bloc de constitutionnalité. La consécration du droit au respect de la vie privée n'était donc qu'une question de temps.

⁸⁴ C. Constitutionnel, décision n°2003-467 du 13 mars 2003 relative à la loi pour la sécurité intérieure, Journal officiel du 19 mars 2003, p. 4789, Ref : <http://www.legifrance.gouv.fr/>

⁸⁵ C. Constitutionnel, décision n° 94-352 DC du 18 janvier 1995 relative à la loi d'orientation et de programmation relative à la sécurité, Journal officiel du 21 janvier 1995, p. 1154, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=2749&indice=1&table=CONSTIT&ligneDeb=1> : « la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle ».

⁸⁶ C. Constitutionnel, décision n° 92-316 DC concernant la loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, Journal officiel du 22 janvier 1993, p. 1118, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=2680&indice=1&table=CONSTIT&ligneDeb=1>

PARTIE II : LE STATUT DU CORRESPONDANT, UN STATUT AU CŒUR DES CRITIQUES

Le dispositif du correspondant à la protection des données à caractère personnel a sans aucun doute une utilité. En effet, outre l'allègement des formalités préalables, il est un vecteur formidable de respect de la vie privée et des libertés individuelles ainsi que de diffusion de la «culture informatique et libertés » auprès des professionnels mettant en œuvre des traitements à caractère personnel que du grand public. Cependant, ces grandes avancées en terme de protection des données personnelles semblent être affaiblies par un statut juridique quelque peu flou.

En effet, outre une exigence générale d'indépendance et de formation posée par la loi de 1978 modifiée, aucun statut ne semble être établi. Cette situation juridique propice à l'insécurité est un choix délibéré du législateur : « Expérimentons d'abord, plutôt que de statuer immédiatement les gens : nous verrons, à l'expérience, s'il faut renforcer les garanties »⁸⁷. Ce choix fut l'objet de nombreuses critiques toujours vivaces aujourd'hui. Il faudra donc attendre le décret d'application pour savoir si le législateur a suffisamment encadré la fonction de correspondant afin que ses missions soient véritablement effectives.

Les principales critiques, dès les travaux préparatoires sont axées sur deux points : d'une part, les modalités de la désignation qui constituent une véritable entrave au champ d'intervention du correspondant (CHAPITRE 1), et d'autre part, les conditions entourant la cessation des fonctions et notamment celles relatives à la responsabilité du correspondant (CHAPITRE 2).

⁸⁷ Propos du rapporteur de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, Francis DELATTRE, recueillis lors de la 205ème séance de l'assemblée nationale du 29 avril 2004, ref : http://www.assemblee-nationale.fr/12/cra/2003-2004/205.asp#P55_1041

CHAPITRE 1 :

Les modalités de désignation, une limite au champ d'intervention du correspondant à la protection des données à caractère personnel

Le correspondant ayant un rôle essentiel en terme de protection des données à caractère personnel au sein de l'organisme qui l'a désigné, les conditions entourant sa désignation doivent être très strictes et également suffisamment souples pour permettre un développement de la fonction. C'est justement en raison de l'imprécision juridique entourant ces modalités, que les doutes sont nées quant à la véritable effectivité de la fonction de correspondant et ont même été le prétexte d'une saisine du Conseil Constitutionnel après l'adoption du projet de loi⁸⁸.

Aujourd'hui encore, qu'il s'agisse des conditions relatives à la personne du correspondant (section 1) ou des conditions relatives à la procédure de désignation (section 2), ces dernières attirent les critiques de toute part.

Section 1 : La désignation, des conditions relatives à la personne du correspondant à respecter

Les conditions relatives à la personne du correspondant sont très importantes lors de la désignation. Du respect de ces conditions dépendra le succès ou l'échec de l'implantation de ce nouvel acteur au sein des entreprises et des collectivités. Cependant, ces dernières suscitent un certain nombre d'interrogations, notamment concernant leur caractère protecteur, auxquelles seul le décret d'application pourra répondre.

D) Une personne physique ou morale

Le III de l'article 22 dispose que le correspondant est « une personne bénéficiant des qualifications requises pour exercer ses missions ». On peut ainsi constater que la loi n'apporte aucune précision sur le fait de savoir si le correspondant est une personne physique ou une personne morale. La directive 95/46/CE ne donne pas plus de précisions sur la nature juridique du détaché à la protection des données en énonçant qu'il s'agit d'une « personne désignée par le responsable du traitement de données ». Il ne semble pas pourtant que ces deux possibilités soient, l'une ou l'autre, exclues par le législateur.

Tout d'abord, les autres dispositions de l'article 22 III laissent à penser que le correspondant est une personne physique. En effet, ce dernier « ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions ». Ce rapport à l'employeur et cette capacité à pouvoir subir des sanctions sont assez déterminants de la nature juridique de personne physique.

Cependant, le fait que le correspondant soit une personne morale ne serait pas contraire à l'esprit de la loi puisque ce dernier peut être externe à l'organisme qu'il l'a nommé. On peut tout à fait imaginer, en effet, que la fonction de correspondant soit confiée à un cabinet d'audit, par exemple. Cependant, dans une telle hypothèse, il sera souhaitable, en terme de responsabilité, de désigner une personne physique déléguée par la personne morale pour exercer ses missions.

⁸⁸ Conseil Constitutionnel, décision n°2004-499 DC du 29 juillet 2004

II) Une personne interne ou externe à la collectivité ou à l'entreprise

La loi ne précise pas non plus si le correspondant doit être interne à l'organisme qui l'a nommé ou s'il peut être externe à ce dernier. La directive, quant à elle, prévoit expressément cette possibilité d'externalisation dans son considérant n°49⁸⁹. Les études menées dans d'autres pays sur les détachés à la protection des données ont montré à des degrés divers que l'externalisation de la fonction avait été choisie lors de la transposition. En Allemagne, par exemple, cette externalisation est limitée au secteur privé et aux petites collectivités locales.

La CNIL, interrogée sur une telle possibilité considère que « la loi permet de désigner un correspondant qui n'appartient pas au personnel de l'organisme »⁹⁰. Ce sera toutefois au décret d'application de confirmer une telle externalisation. Cette externalisation est très attendue, aujourd'hui : elle pourrait bien faire émerger un nouveau « marché des correspondants à la protection des données ».

A/Le correspondant interne

⁸⁹ « [...] que des exonérations ou simplifications peuvent pareillement être prévues par les États membres dès lors qu'une personne désignée par le responsable du traitement de données s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées; que la personne ainsi détachée à la protection des données, **employée ou non du responsable du traitement de données**, doit être en mesure d'exercer ses fonctions en toute indépendance; [...] »

⁹⁰ voir interview p.27, 25^{ème} rapport d'activité de la CNIL

1) Des moyens conséquents à mettre en œuvre

Même classique, cette hypothèse s'avère la plus lourde à mettre en œuvre. En effet, la désignation d'une personne membre de l'organisme à la fonction de correspondant à la protection des données va nécessairement impliquer des investissements très importants pour la structure : le correspondant devant réunir de grandes compétences dans le domaine de protection des données et ces compétences étant difficiles à trouver en interne, des dépenses en terme de formation voire en terme de recrutement s'avéreront indispensables.

Outre l'aspect financier, la mise en place d'un correspondant implique un aménagement assez long et complexe. Que l'entreprise ou la collectivité crée un service spécial pour le correspondant ou qu'elle confie cette tâche à une personne déjà salariée de l'organisme (appartenant de préférence à la direction juridique, à la direction des systèmes d'information ou encore à la direction des ressources humaines), l'introduction du correspondant prendra un certain temps.

Dans la première hypothèse où seront certainement concernées les structures dont les traitements à caractère personnel ont une place centrale dans leur fonctionnement, l'aménagement d'un tel service nécessitera une modification des méthodes de travail afin de prendre en compte son existence lors d'éventuels projets informatiques.

Dans la seconde hypothèse, qui correspondra beaucoup plus aux structures ne recourant pas de manière récurrente à des traitements de données à caractère personnel, confier cette mission à un salarié s'avérera relativement périlleux. En raison des missions parfois délicates dont le correspondant est investi et surtout du manque de sécurité juridique, il est fort à parier que peu de salariés se porteront volontaires afin d'assumer cette mission. Or, il est essentiel que ce poste soit expressément accepté par la personne désignée. Cette dernière doit toujours avoir la possibilité de refuser la nouvelle fonction mais aussi d'y mettre un terme dans l'hypothèse d'une acceptation.

Ajoutons que du fait de l'internalisation de la fonction, les parties seront liées par un contrat de travail dans lequel l'objet de la mission devra être défini au préalable. Concernant plus spécifiquement les collectivités locales, l'activité du correspondant devra être officialisée par notamment une mention de cette activité dans la fiche de poste et le temps accordé à cette fonction devra être spécifiquement prévu.

2) Une option idéale pour les entreprises et les collectivités de grande taille

Tous ces paramètres et conséquences poussent de manière évidente à penser qu'une telle internalisation de la fonction de correspondant constitue une option particulièrement adaptée aux grandes structures, ces dernières disposant de ressources financières, humaines et organisationnelles bien plus importantes que celles des petites structures.

Ce constat s'avère d'autant plus réel dans le secteur privé. De nombreuses grandes entreprises s'étant déjà dotées de spécialistes pour la protection des données personnelles⁹¹ ou disposant de services spécialisés tels que les directions juridiques ou de déontologie, l'introduction de la nouvelle fonction s'en trouvera facilitée.

Quant à la personne à désigner, on peut penser qu'il s'agira, dans le secteur privé, d'un cadre et dans le secteur public d'un agent administratif (fonctionnaire titulaire) ou un agent contractuel (contractuel de l'Etat ou contractuel de droit privé).

⁹¹ Certaines grandes multinationales et grandes entreprises telles que IBM France et Expérian se sont dotés depuis 2001 en France de « responsable informatique et libertés » ou « chief privacy officers ».

B/ Le correspondant externe

1) Une possibilité entrevue par la CNIL mais soumise à certaines conditions

A différentes reprises, la Commission a eu l'occasion de confirmer la possibilité d'une externalisation de la fonction de correspondant à la protection des données à caractère personnel. Cependant, ce choix de désigner un correspondant externe ne concernera pas toutes les structures. La CNIL estime en effet « qu'une désignation extérieure ne devrait être possible qu'en deçà d'un seuil à définir et devrait répondre au souci d'une mutualisation des fonctions de correspondant permettant à plusieurs responsables de se regrouper afin de désigner le même correspondant »⁹².

Cette externalisation sera par conséquent ouverte aux petites entreprises et petites collectivités locales, les conditions de seuils restant à être définies par le décret d'application. Cette orientation semble être justifiée au regard des moyens financiers et humains insuffisants dont disposent ces petites structures pour l'implantation en interne d'un correspondant. Ces dernières ne seront donc pas exclues du bénéfice de l'allègement des formalités préalables. En Allemagne, cette condition de seuil a également été prise en compte puisque, par exemple, les petites collectivités locales peuvent se regrouper afin de désigner un détaché commun à la protection des données.

Cependant, les grosses structures ne sont tout de même pas exclues du projet de décret d'application. Lors de sa conférence de presse du 20 avril 2005, la CNIL considère que dans le but de tenir compte de leur organisation, « les fonctions de correspondant informatique et libertés pourront être exercées par un salarié d'une autre société du groupe, d'un groupement d'intérêt économique (GIE) ou encore d'un organisme professionnel auquel appartient le responsable du traitement »⁹³.

2) Les moyens de l'externalisation

Dans l'hypothèse d'une externalisation de la fonction, les parties devront être liées par un contrat de prestations de service : ce contrat devra régler les aspects techniques, économiques et juridiques de l'exercice des missions du correspondant.

Les moyens de l'externalisation seront certainement différenciés selon le secteur public ou le secteur privé. Dans le secteur public, le président de la CNIL prévoit la mise en place de communautés de communes. Dans le secteur privé, ce rôle de correspondant sera revêtu indifféremment par un cabinet de consulting, un expert comptable, un avocat, un organisme spécialisé de correspondants à la protection des données où des compétences en terme de protection des données seront présentes. Il peut donc s'agir autant d'une personne physique que d'une personne morale.

⁹² 25^{ème} rapport d'activité de la CNIL p.27

⁹³ Conférence de presse du 20 avril 2005 présentant le 25^{ème} rapport d'activité de la CNIL pour l'année 2004, ref : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/DP-conf2005.pdf

Cette externalisation de la fonction de correspondant créant une nouvelle demande de la part des entreprises et des collectivités souhaitant bénéficier de la dérogation du III de l'article 22 de la loi de 1978, il est certain que nous assisterons dans les mois à venir au déploiement d'un « marché des correspondants à la protection des données ». L'émergence avant même la sortie du décret d'application d'une association française des correspondants à la protection des données (AFCPD) en est le signe même.

III) Une personne qualifiée

Même si le responsable des traitements dispose d'une entière liberté quant au choix du correspondant, la loi lui impose toutefois de désigner une personne qualifiée.

A/ Des « qualifications requises » exigées

1) Une appréciation imprécise de la qualification du correspondant

Selon le III de l'article 22, le correspondant doit bénéficier des « qualifications requises pour exercer ses missions ». Se pose donc le problème de savoir ce que peut bien recouvrir l'expression « qualifications requises ».

Les lois nationales de nos voisins européens ayant fait le choix, tout comme nous, d'introduire un « détaché à la protection des données », ne sont guère plus précises : la loi fédérale allemande parle de « capacités nécessaires » alors que la loi néerlandaise retient l'expression « connaissances adéquates ».

La CNIL elle-même admet qu'il « n'est pas possible de déterminer a priori la nature et le niveau des qualifications requises qui dépendent de la taille et de l'activité du responsable de traitement. Par conséquent, ils devront être définis par le responsable des traitements en fonction de la situation, des moyens et des besoins. D'où, le choix de la CNIL de ne pas soumettre le choix du correspondant à un agrément de sa part comme cela est le cas au Luxembourg.

Ces qualifications peuvent tout de même être déduites des missions imparties au correspondant. La première évidence est que le correspondant devra avoir une connaissance approfondie de la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 modifiée. Cependant cette seule compétence n'est pas suffisante : il devra également posséder, selon la CNIL, une connaissance « des technologies informatiques qu'elles soient standards ou spécifiques à l'activité de l'organisme l'ayant désigné »⁹⁴. De même, ayant un rôle d'information et d'audit de l'organisme, des compétences dans les domaines du conseil et du management seraient utiles. Enfin, le correspondant sera amené, lors de l'exercice de ses missions, à revêtir le rôle de médiateur tant auprès des salariés et des personnes concernées par les traitements que du responsable de ces traitements, il devra donc faire également preuve de qualités de pédagogie.

2) Enjeux de la qualification

L'importance attachée à la qualification du correspondant à la protection des données a pour but de rendre véritablement effectives les missions confiées à ce dernier. Comment ce correspondant pourrait-il veiller au respect de la loi « informatique et libertés » sans la connaître de manière approfondie ? Comment ce dernier serait-il capable de différencier un traitement soumis aux articles 22 et 23 d'un traitement soumis à autorisation ou avis de la CNIL sans compétence dans le domaine de la protection des données ? Ces interrogations sont capitales pour les organismes car elles montrent dans quelle mesure ces derniers peuvent être mis en danger par un mauvais jugement du correspondant sur l'application de la loi.

⁹⁴ « FAQ correspondant informatique et libertés », ref : <http://www.cnil.fr/index.php> ?

La formation du correspondant a également une certaine importance dans le sens où elle permet de crédibiliser la fonction et donc de favoriser son développement dans d'autres entreprises ou collectivités. Le succès de l'implantation du dispositif du correspondant ne pourra avoir lieu si les seuls exemples sont ceux de correspondants incompetents dont l'inutilité semble être un véritable état de fait. Les enjeux liés à la formation du correspondant sont donc considérables.

La Suède et le Luxembourg ont bien compris ces enjeux : la loi suédoise prévoit d'adresser à l'ensemble des détachés à la protection des données le rapport élaboré en son sein chaque année. Elle propose des formations aux détachés ainsi que du matériel pédagogique téléchargeable de son site internet. La loi luxembourgeoise impose une obligation de formation annuelle dont le non suivi est sanctionné par un retrait de l'agrément par l'autorité de contrôle.

3) La formation, source d'inégalités des collectivités et des entreprises

Malgré cet impératif de formation et à défaut d'agrément de la part de la CNIL⁹⁵, il est à craindre que certains organismes, et notamment les plus petits d'entre eux, ne disposeront pas d'un correspondant compétent comme l'exige la loi. En effet, les petites entreprises et les petites collectivités ayant fait le choix d'internaliser la fonction de correspondant n'auront pas la possibilité, au regard du coût des formations, de proposer une formation de bonne qualité faute de moyens financiers. Ainsi, serait créée une situation d'inégalité entre les organismes.

C'est la raison pour laquelle, afin de résorber cette difficulté, des contacts réguliers doivent être pris avec la CNIL dans l'hypothèse d'un éventuel doute sur l'application de la loi. Il serait également souhaitable d'entrevoir si, comme le Luxembourg, la CNIL ne pourrait pas dispenser elle-même les formations gratuitement ou à un coût accessible au plus grand nombre afin d'assurer une égale formation entre les correspondants.

Cependant, toutes ces exigences et les difficultés qui ressortent de leur mise en œuvre ne montrent-elles pas la nécessité de faire du correspondant une profession réglementée ?

B/ Une profession réglementée déguisée ?

1) Un refus de la part du législateur

Une profession réglementée est définie, selon les directives européennes 89/48/CEE du 21 décembre 1988⁹⁶ et 92/51/CEE du 18 juin 1992⁹⁷ relatives à un système général de reconnaissance des diplômes et des formations professionnelles, comme « une activité professionnelle dont l'accès est subordonné dans un Etat membre à la possession d'un diplôme, mais également celle dont l'accès est libre, lorsqu'elle est exercée sous un titre professionnel réservé à ceux qui remplissent certaines conditions de qualification ». En d'autres termes, il s'agit d'une profession dont l'accès et le titre sont régis par la loi. Les membres des

⁹⁵ Lors des travaux préparatoires, un amendement de M. Patrick BLOCHE prévoyant que la CNIL devait agréer la désignation du correspondant avait été rejeté au motif que cela avait pour conséquence d'alourdir inutilement la charge de travail de la CNIL.

⁹⁶ Directive 89/48/CEE du Conseil du 21 décembre 1988 relative à un système général de reconnaissance des diplômes d'enseignement supérieur qui sanctionnent des formations professionnelles d'une durée minimale de trois ans, *Journal officiel* n° L 019 du 24/01/1989 p. 0016 – 0023, ref : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31989L0048&model=guichett

⁹⁷ Directive 92/51/CEE du Conseil, du 18 juin 1992, relative à un deuxième système général de reconnaissance des formations professionnelles, qui complète la directive 89/48/CEE, *Journal officiel* n° L 209 du 24/07/1992 p. 0025 – 0045, Ref : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc &lg=fr&numdoc=31992L0051&model=guichett

professions réglementées doivent obéir à des règles déontologiques strictes et sont soumis au contrôle de leurs instances professionnelles sous la forme d'un ordre, d'une chambre ou d'un syndicat. A titre d'illustration, sont des professions réglementées les professions d'avocat, d'expert-comptable, de géomètres experts, de commissaire aux comptes...

Au vu de cette définition, il serait tentant de penser que le correspondant à la protection des données à caractère personnel est une profession réglementée déguisée. En effet, elle est régie par la loi de 1978 et est ouverte à ceux qui remplissent certaines conditions de qualification.

Guy BRAIBANT, dans son rapport, avait lui-même soulevé cette hypothèse à plusieurs reprises en constatant que la directive ne précisant pas le statut du correspondant, ce dernier pourrait être « un commissaire aux données analogue au commissaire aux comptes, qui pourrait d'ailleurs cumuler les deux fonctions » puis en rapprochant la situation du correspondant à celle des « médecins du travail ou experts comptables ». Cette piste de réflexion n'a toutefois pas été approfondie par les parlementaires puisque le législateur n'a pas souhaité créer une nouvelle catégorie de profession réglementée.

2) Une solution pourtant envisagée par la doctrine

Eriger la profession de correspondant en nouvelle profession réglementée a pourtant paru une solution adaptée pour certains auteurs de doctrine. La question de l'existence d'un éventuel « commissaire aux données personnelles »⁹⁸ a également été posée. En effet, ce statut apporterait bon nombre d'avantages en terme de formation mais aussi de responsabilité.

a- Un statut garantissant la qualification

L'accès à une profession réglementée est régi par la loi. Les conditions d'accès sont en général subordonnées à l'obtention d'un certificat d'aptitude comportant des épreuves orientées vers les disciplines prépondérantes dans l'exercice de cette profession.

A titre d'exemple, l'article 8 du décret du 27 mai 2005⁹⁹ portant modification du décret du 12 août 1969 relatif à l'organisation de la profession et au statut professionnel des commissaires aux comptes¹⁰⁰ soumet l'inscription sur la liste des commissaires aux comptes à certaines conditions : les candidats « doivent avoir subi avec succès les épreuves de l'examen d'aptitude aux fonctions de commissaire aux comptes, après l'accomplissement d'un stage professionnel jugé satisfaisant ».

Ainsi, s'il en était de même avec le correspondant, les difficultés liées à la formation énoncées précédemment ne se poseraient plus. Mais, ne serait-ce pas aller un peu loin en imposant un certificat d'aptitude au correspondant ? C'est certainement ce qu'a dû se dire le législateur en refusant cette possibilité.

⁹⁸ Claire LEVALLOIS BARTH et Arnaud BELLEIL, « Le correspondant informatique et libertés : une fonction en attente de clarification », Expertises n°283, juillet 2004

⁹⁹ Décret n°2005-599 du 27 mai 2005 portant modification du décret n° 69-810 du 12 août 1969 relatif à l'organisation de la profession et au statut professionnel des commissaires aux comptes, NOR:JUSC0520338D, JORF 29 mai 2005, ref. : <http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=27419&indiceNav=1 &tableNav=CONSOLIDE&ligneDebNav=1>

¹⁰⁰ Décret n°69-810 du 12 août 1969 relatif à l'organisation de la profession et au statut professionnel des commissaires aux comptes, JORF 29 août 1969 rectificatif JORF 12 septembre 1969, ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=4720380&indice=1&table=LEGI&ligneDeb=1>

b- Un statut efficace en terme de responsabilité

Le dispositif des professions réglementées, en plus de garantir la formation de ses membres, apporte une certaine sécurité en terme de responsabilité. En effet, des règles sont prévues dans la plupart des professions réglementées afin d'engager la responsabilité du professionnel dans l'hypothèse où ce dernier aurait manqué à ses missions.

Par exemple, le commissaire aux comptes voit sa responsabilité civile et même pénale engagée pour les fautes et les infractions commises dans l'accomplissement de sa mission. Des sanctions disciplinaires peuvent également être prononcées à son encontre en cas de simple faute déontologique.

Conférer une telle responsabilité au correspondant ne réduirait-il pas de manière considérable le nombre de postulants à la fonction et mettre ainsi en péril le dispositif même du III de l'article 22 car, n'oublions pas que la désignation d'un correspondant est facultative.

Cependant, une pratique des professions réglementées s'avère très efficace en terme de responsabilité et demeure intéressante pour le dispositif du correspondant à la protection des données : il est d'usage courant de recourir à une assurance professionnelle. Ainsi, les professionnels du droit, dont font partie les avocats, assurent leurs clients de leurs prestations de service.

IV) Une personne indépendante

Selon la loi de 1978, le correspondant est « chargé d'assurer de manière indépendante, le respect des obligations prévues dans la présente loi ». Cette indépendance entourant l'accomplissement des missions du correspondant, exigence déjà posée par la directive européenne¹⁰¹, est essentielle. Elle permet, en effet, de juger de la véritable effectivité du dispositif du correspondant à la protection des données. Cependant, elle constitue également le point d'orgue des critiques.

A/ L'indépendance, véritable nécessité permettant au correspondant d'exercer ses missions

1) Approche de la notion d'indépendance

Selon une définition classique, l'indépendance est caractérisée par une absence de relations entre deux entités qu'il s'agisse de relations de sujétion, de cause à effet ou de coordination.

Au sens de la loi de 1978, l'indépendance du correspondant se traduit par le fait que ce dernier « ne peut faire l'objet d'aucune sanction de la part de son employeur du fait de l'accomplissement de ses missions ». C'est donc le positionnement hiérarchique du correspondant qui permet d'apporter les garanties suffisantes à une telle indépendance.

La CNIL prévoit qu'il sera ainsi rattaché directement au responsable de traitement pour ne pas « être influencé dans les conseils, recommandations ou alertes qu'il sera conduit à formuler lors de la mise en œuvre des traitements ou dans l'instruction des plaintes et requêtes adressée par les personnes concernées ». Sont également prévus par cette dernière, « une possibilité de communiquer directement avec la direction de l'organisme » et « l'interdiction pour le responsable du traitement d'interférer dans les missions du correspondant ».

Il serait également souhaitable, comme l'ont prévu les législations allemandes et néerlandaises, que le correspondant ne soit pas désavantagé en terme de carrière ou financièrement en raison de l'accomplissement de ses missions.

¹⁰¹ L'article 18 de la directive dispose que le détaché à la protection des données à caractère personnel est chargé « d'assurer, **d'une manière indépendante**, l'application interne des dispositions nationales prises en application de la présente directive ».

2) Incompatibilité de la fonction de correspondant avec certaines fonctions

Cette indépendance implique que le correspondant se voit doter d'une certaine impartialité dans ses décisions. Il ne doit pas notamment être influencé dans son jugement par des considérations nées d'autres fonctions qu'il exercerait parallèlement. En effet, afin que ses missions soit véritablement pertinentes, le correspondant se doit d'être à l'abri de tout conflit d'intérêt.

C'est dans cette perspective que la loi fédérale allemande en a déduit une incompatibilité de la fonction de détaché avec les fonctions de direction de l'organisme. Cependant, l'appréciation des conflits d'intérêt se faisant au cas par cas, l'autorité de contrôle a eu l'occasion de relever d'autres incompatibilités notamment avec des fonctions dans des secteurs d'activité liée aux ressources humaines, aux nouvelles technologies et à l'information ou encore dans des secteurs du marketing, grands utilisateurs de traitements de données à caractère personnel. L'autorité de contrôle allemande va même plus loin parfois en intervenant, sur la demande de salariés, auprès des organismes afin d'obtenir la décharge de certains détachés présentant de manière manifeste une altération de leur jugement en raison d'autres fonctions occupées parallèlement.

Ce choix fait par l'Allemagne d'établir certaines incompatibilités de la fonction de détaché avec d'autres fonctions afin de garantir une certaine indépendance de la fonction semble également avoir été adopté par la CNIL. Ainsi, elle estime que « le directeur de l'organisme ne pourra pas être désigné comme correspondant informatique et libertés »¹⁰².

Là encore, il est intéressant de rapprocher le correspondant à la protection des données à caractère personnel au commissaire aux comptes. Des incompatibilités légales avec certaines activités ou qualités ont été aménagées par l'article 822-11 du Code de commerce¹⁰³ afin de garantir l'indépendance de sa profession. Ainsi, n'aurait-il pas été plus judicieux de faire de la fonction de correspondant une profession réglementée ou au moins confier ce rôle aux commissaires aux comptes. L'exigence d'indépendance posée par la loi de 1978 aurait été respectée contrairement au dispositif actuel dont l'indépendance semble être une sorte de fiction juridique.

B/ L'indépendance, une fiction juridique ?

Malgré certaines mesures envisagées afin de garantir l'indépendance du correspondant à la protection des données à caractère personnel, la principale difficulté réside dans le fait que le correspondant demeure rémunéré par l'organisme qui l'a désigné. Cet état de fait relevé dès les travaux préparatoires de la loi de 2004 n'a pas pour autant décidé le législateur à lui attribuer un statut protecteur. Ce choix du législateur a fait l'objet de nombreuses critiques de la part de la doctrine. Aujourd'hui encore, cette problématique liée à l'indépendance du correspondant constitue le point le plus épineux du statut du correspondant. Il est donc intéressant de se demander si cette indépendance ne constitue pas une fiction juridique au regard de l'absence de statut de salarié protégé. Cette question se pose également plus précisément pour le correspondant dans le secteur public à la vue des possibles incompatibilités entre cette

¹⁰² Conférence de presse du 20 avril 2005 présentant le 25^{ème} rapport d'activité de la CNIL pour l'année 2004, ref : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/DP-conf2005.pdf

¹⁰³Cet article, introduit par la loi n°2003-706 du 1^{er} août 2003 de sécurité financière, dispose « le commissaire aux comptes ne peut prendre, recevoir ou conserver, directement ou indirectement, un intérêt auprès de la personne dont il est chargé de certifier les comptes, ou auprès d'une personne qui la contrôle ou qui est contrôlée par elle[...]le code de déontologie prévu à l'article L. 822-16 définit les liens personnels, financiers et professionnels, concomitants ou antérieurs à la mission du commissaire aux comptes, incompatibles avec l'exercice de celle-ci. Il précise en particulier les situations dans lesquelles l'indépendance du commissaire aux comptes est affectée [...] ».

exigence légale d'indépendance et les règles de la fonction publique marquées par un fort devoir d'obéissance.

1) Un correspondant indépendant mais ne bénéficiant pas de protection

La maigre protection accordée par le législateur permettant au correspondant de « saisir la CNIL des difficultés qu'il rencontre dans l'accomplissement de ses missions » et de « ne faire l'objet d'aucune sanction de la part de son employeur du fait de l'accomplissement de ses missions » a paru peu suffisante pour certains.

En effet, durant les travaux préparatoires, nombre de parlementaires et de sénateurs ont exprimé leurs doutes quant à la réalité de cette indépendance en l'absence de statut protecteur. Afin de pallier cette réelle difficulté, un sous-amendement n°54¹⁰⁴ de l'amendement n°42 avait été présenté, lors de l'adoption en seconde lecture du projet de loi par l'assemblée nationale, par le député Christophe CARESCHE et les membres du groupe socialiste proposant qu'un statut de salarié protégé soit inscrit dans la loi.

Ce statut dont la protection bénéficie déjà aux délégués du personnels, aux membres du comité d'entreprise, aux représentants syndicaux, aux membres du comité d'hygiène, de sécurité et des conditions de travail¹⁰⁵, aux salariés remplissant certaines fonctions sociales (conseillers prud'hommes, conseillers du salariés ou encore les représentants du salarié dans le cadre d'une procédure de redressement et de liquidation judiciaire), aux salariés ayant demandé l'organisation d'élections professionnelles et enfin aux candidats déclarés ou imminents à ces fonctions et les anciens titulaires, soumet à une procédure spécifique, conformément aux articles L412-18, L425-1 et L436-1 du Code du travail, l'employeur qui envisage le licenciement d'un représentant du personnel. Le licenciement ne peut intervenir qu'après soumission du projet au comité d'entreprise (sauf pour les délégués syndicaux) et autorisation de l'inspecteur du travail ou de l'autorité qui en tient lieu.

De la même manière, dans le secteur public, le décret n° 82-447 du 28 mai 1982 sur l'exercice du droit syndical dans la fonction publique¹⁰⁶ confère un statut particulier aux délégués syndicaux : un détachement de droit peut leur être accordé ainsi que des autorisations spéciales d'absence ou des décharges d'activité de service. La loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives

¹⁰⁴ <http://www.assemblee-nationale.fr/12/pdf/cri/2003-2004/cahiers/c20040205.pdf>

¹⁰⁵ Au terme de l'art. L-236-2 du Code du travail : « *Le comité d'hygiène, de sécurité et des conditions de travail a pour mission de contribuer à la protection de la santé physique et mentale et de la sécurité des salariés de l'établissement et de ceux mis à sa disposition par une entreprise extérieure, y compris les travailleurs temporaires, ainsi qu'à l'amélioration des conditions de travail, notamment en vue de faciliter l'accès des femmes à tous les emplois et de répondre aux problèmes liés à la maternité. Il a également pour mission de veiller à l'observation des prescriptions législatives et réglementaires prises en ces matières.* »

¹⁰⁶ Décret n° 82-447 du 28 mai 1982 sur l'exercice du droit syndical dans la fonction publique, JORF du 30 mai 1982, ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=272818&indice=1&table=LEGI&ligneDeb=1>

à la fonction publique territoriale¹⁰⁷ conforte ce statut en apportant des garanties de rémunération et un droit à l'avancement moyen et à la promotion interne.

Aux Pays-Bas, ce statut de salarié protégé a été adopté afin de garantir l'exigence d'indépendance de la directive.

Malgré les garanties apportées en terme de protection, le législateur a refusé d'octroyer un tel statut au correspondant à la protection des données. Le rapporteur, lors de l'adoption en première lecture du projet de loi par le Sénat, a d'ailleurs déclaré qu'il n'était pas question de « créer un nouveau type de salariés 'super-protégés'. L'idée est de faire de la pédagogie et de favoriser l'échange d'informations, pas d'ériger un salarié en défenseur d'un droit par rapport à la CNIL ou par rapport à une quelconque institution »¹⁰⁸.

Cette position fut fortement critiquée par les sénateurs comme par les parlementaires, au point de voir saisir le Conseil Constitutionnel. Cette « tautologie d'indépendance » ne fut toutefois pas remise en cause par ce dernier. Les critiques ne s'essouffèrent pas pour autant allant même pour certains de qualifier le correspondant de « casque bleu »¹⁰⁹.

2) Le correspondant public : des incompatibilités avec les règles de la fonction publique

Les difficultés relatives à la mise en place d'une véritable indépendance du correspondant lors de l'exercice de ses missions s'apprécient plus particulièrement du point de vue du correspondant public. On distingue, en effet, de réelles incompatibilités entre cette exigence posée par la loi de 1978 et les règles régissant le statut de la fonction publique.

Le correspondant des collectivités locales, dans l'hypothèse où ce dernier est un agent public, est soumis à une obligation d'obéissance hiérarchique. Selon l'article 28 de la loi « Le Pors » du 13 juillet 1983¹¹⁰, « tout fonctionnaire, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public ». Ce devoir d'obéissance concerne non seulement les ordres émanant du supérieur hiérarchique mais également les mesures prises pour l'organisation des services auxquels il appartient, le refus d'obéissance constituant une faute professionnelle passible de sanctions disciplinaires.

Il est donc intéressant de se demander si ce devoir d'obéissance ne mettrait pas en péril l'indépendance exigée par la loi. En effet, peut-on considérer qu'une personne soumise à des contraintes hiérarchiques puisse véritablement exercer ses missions de correspondant en toute indépendance ? Ces difficultés de positionnement hiérarchique se feront ressentir lorsque le correspondant sera saisi de plaintes et requêtes des personnes concernées par les traitements et lorsqu'il devra formuler des réclamations à l'égard du responsable du traitement, ces missions s'exerçant en dehors de toutes contraintes hiérarchiques.

L'existence d'un tel devoir d'obéissance soulève d'autres difficultés : dans l'hypothèse d'un refus de la part du correspondant d'obéir à des ordres émanant du supérieur hiérarchique contraires à la loi relative à l'informatique, aux fichiers et aux libertés, ce refus sera-t-il interprété comme une désobéissance passible de sanctions disciplinaires. Selon la dérogation aménagée par l'article 28 de la loi « Le Pors » inspirée de la théorie des baïonnettes intelligentes, cela ne sera pas le cas. En effet, un devoir de désobéissance s'impose dès lors que « l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public ».

¹⁰⁷ Loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, JORF du 27 janvier 1984, ref : <http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=5874&indiceNav=1&tableNav=CONSOLIDE&ligneDebNav=1>

¹⁰⁸ Compte-rendu intégral du Sénat du 1^{er} avril 2003 p.39, <http://www.senat.fr>

¹⁰⁹ Sébastien LALOUE et Hervé GABADOU, « Le correspondant à la protection des données va voir le jour : pour quelles missions ? », ref : <http://www.clic-droit.com/web/editorial/>

¹¹⁰ Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, JORF du 14 juillet 1983, ref : <http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=5870&indiceNav=1&tableNav=CONSOLIDE&ligneDebNav=1>

Outre les modalités de désignation du correspondant à la protection des données à caractère personnel, la loi est également imprécise quant à la procédure de désignation.

Section 2 : La désignation, une procédure minutieuse à respecter

Afin de rendre le dispositif des correspondants à la protection des données à caractère personnel « transparent », la loi a mis en place une procédure de désignation. La dispense de déclaration induite par ce dispositif pourrait en effet faire obstacle au recensement des organismes ayant opté pour le régime du correspondant. C'est la raison pour laquelle, la loi a posé une obligation de notification aux deux instances les plus concernées par la désignation du correspondant : la CNIL et les instances représentatives du personnel.

I) Une désignation devant être notifiée à la CNIL

Le second alinéa du III de l'article 22 dispose que « la désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés ». Cette obligation de notification à l'autorité de contrôle n'a pourtant pas été prévue en Allemagne en raison du caractère obligatoire de la désignation. En quoi peut bien consister cette notification et quelle est son effet ? Ce sera bien évidemment au décret d'application de les préciser. En attendant, la CNIL ainsi que les dispositifs européens du détaché livrent certaines indications.

B/ Contenu de la notification

Cette notification ayant pour but de faire connaître à la CNIL les organismes ayant choisi le dispositif du correspondant à la protection des données, elle contiendra en toute logique l'identité et l'adresse du responsable des traitements ainsi que celles du correspondant (nom, prénom, adresse), le fait de savoir si ce correspondant est un membre interne à l'organisme ou une personne externe. Il serait également utile de préciser, dans l'hypothèse où le correspondant serait une personne morale, l'identité de la personne mandatée par cette dernière. Ces informations seront essentielles afin de faciliter la prise de contact entre le correspondant et l'autorité de contrôle.

On peut se demander, cependant, si à la vue de son absence de pouvoir d'agrément, la CNIL devrait être informée des qualifications du correspondant. Cette possibilité serait cependant un gage de l'effectivité du dispositif. Ne serait-il pas nécessaire également de joindre dans cette notification l'acte d'engagement du correspondant manifestant son acceptation des fonctions et ce dans l'optique d'une certaine sécurité juridique.

Enfin, la CNIL précise qu'elle devra être « avertie de toute modification affectant sa désignation ». Ainsi, tout changement intervenant en cours de mission tels qu'un remplacement, une démission devra être notifié à la CNIL. Cette mesure vise à renforcer la protection du correspondant.

C/ Effet de la notification

Dans sa conférence de presse du 20 avril 2005, la CNIL a déclaré que « le correspondant informatique et libertés ne pourra prendre ses fonctions qu'un mois après notification à la CNIL ». La notification rend par conséquent opérationnelle la désignation du correspondant. Cette notification permettra de fixer le point de départ des exonérations de déclaration des traitements soumis aux formalités préalables des articles 22, 23 et 24.

Cependant, précisons que cette notification ne s'ensuit pas d'un agrément par la CNIL de la personne du correspondant. En effet, la CNIL ne dispose pas d'aucun pouvoir d'agrément de sorte que la désignation relève entièrement du libre arbitre du responsable du traitement.

Il faut également se demander si, comme à l'image des Pays-Bas, les informations contenues dans la notification donneront lieu à la création d'un registre légal des correspondants rendu accessible au public. Ainsi, comme toute publicité, cette notification aura pour effet d'informer les tiers et notamment les personnes concernées par les traitements.

II) Une désignation portée à la connaissance des instances représentatives du personnel

Selon la loi, la désignation du correspondant « est portée à la connaissance des instances représentatives du personnel ». Cette information pourra se faire par lettre ou lors d'un comité. Elle a pour but d'informer le personnel de l'organisme ayant opté pour le dispositif du correspondant. En effet, ce dernier étant destiné à devenir leur interlocuteur privilégié, il semble logique, que la notification de sa désignation leur soit faite.

Ajoutons que cette notification constituera une sorte de première étape de sensibilisation à la législation relative à la protection des données à caractère personnel du personnel et leur permettra de réorganiser leurs méthodes de travail afin de tenir compte de sa présence et de son utilité. Ainsi, serait-il préférable, lors de cette notification, de fixer l'étendue des missions du correspondant.

Cette volonté de soumettre à un dialogue au sein même de l'entreprise les problématiques « informatique et libertés » via les instances représentatives n'est toutefois pas nouvelle. En effet, l'article 432-2-1 du code du travail dispose que le comité d'entreprise est « informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci ».

CHAPITRE 2 :

De la cessation des fonctions du correspondant à la protection des données à caractère personnel et de sa responsabilité

Comme toutes fonctions, celles du correspondant à la protection des données peuvent prendre fin à tout moment. Cette cessation des fonctions peut classiquement intervenir dans deux hypothèses : d'une part, le correspondant peut voir interrompre ses fonctions en dehors de tout manquement de sa part (section 1) puis, d'autre part, cette cessation des fonctions peut résulter de défaillances (section 2) dans l'accomplissement de ses missions.

C'est justement cette deuxième hypothèse qui nous conduira à nous pencher sur la responsabilité du correspondant. Ce dernier point, non explicité dans la loi et source de nombreuses interrogations, sera déterminant quant à l'effectivité des missions du correspondant mais également quant au succès du dispositif au sein des entreprises et des collectivités locales.

Section 1 : La cessation des fonctions en dehors de tout manquement

L'hypothèse la plus classique de cessation des fonctions est celle intervenant en dehors de tout manquement de la part du correspondant dans l'accomplissement de ses missions. Se pose alors la question de la durée des fonctions. Sans autre précision apportée par la loi, il apparaît que la durée de la mission peut être déterminée ou indéterminée.

Dans la première hypothèse, la cessation des fonctions interviendra à l'arrivée du terme de la mission alors que dans la seconde hypothèse, la cessation interviendra par la démission du correspondant.

I) La cessation normale des fonctions : la fin de la mission

Il s'agit donc de l'hypothèse dans laquelle la mission prend fin à l'arrivée du terme. Cela suppose donc que la mission du correspondant est une mission à durée déterminée.

Ce terme doit figurer dans le contrat liant le responsable des traitements et le correspondant. Il serait également intéressant de faire figurer ce terme dans la notification de désignation du correspondant à la CNIL prévue au second alinéa du III de l'article 22 de la loi de 1978.

Au terme de la mission, le responsable des traitements sera libre de désigner un correspondant ou de décider de se soumettre aux formalités obligatoires. S'il décide de désigner un nouveau correspondant, il devra bien entendu mettre en œuvre une nouvelle procédure de notification à la CNIL ainsi qu'à une procédure d'information des instances représentatives du personnel.

II) La cessation volontaire des fonctions : la démission

Il s'agit de l'hypothèse dans laquelle le correspondant met fin à sa mission en démissionnant. Cela suppose qu'il ait mis fin à ses fonctions avant l'arrivée du terme dans le cadre d'un contrat à durée déterminée ou, qu'il y ait mis fin en raison du caractère indéterminé du contrat. Rappelons toutefois que la démission dans le cadre d'un contrat à durée déterminée n'est pas autorisée par la loi sauf dans certains cas limitativement énumérés. Aux termes de l'article L122-3-8 du Code du travail, « sauf accord des parties, le contrat à durée déterminée ne peut être rompu avant l'échéance du terme qu'en cas de faute grave ou de force majeure .Il peut toutefois, par dérogation aux dispositions du précédent alinéa, être rompu à l'initiative du salarié lorsque celui-ci justifie d'une embauche pour une durée indéterminée ».

Cette possibilité de démission est extrêmement importante car elle permet de garantir le consentement du correspondant aux fonctions. Comme ce dernier est libre de refuser le poste de correspondant lors d'une désignation, il peut également être libre d'interrompre ses fonctions à tout moment.

La CNIL prévoyant qu'elle doit être avertie de toute modification affectant la désignation du correspondant, la démission de ce dernier devra donc lui être notifiée. Se pose alors la question de la motivation : le correspondant démissionnaire doit-il indiquer le motif de sa démission ?

Devra-t-il justifier d'un intérêt légitime, sa démission ? Si la réponse est positive, en quoi consiste cet intérêt légitime ? Si on se réfère au droit commun, dans le cadre d'un contrat à durée indéterminée, la démission n'a pas à être motivée.

Se pose également la question du préavis : le correspondant devra-t-il se soumettre à un délai-congé afin de permettre au responsable du traitement de recruter un nouveau correspondant ?

Section 2 : La cessation des fonctions résultant de manquements de la part du correspondant

La seconde hypothèse de cessation des fonctions est celle résultant de la décharge des fonctions du fait de manquements constatés de la part du correspondant lors de l'accomplissement de ses missions. Ainsi, le dernier alinéa du II de l'article 22 dispose que « en cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses missions sur demande ou après consultation, de la Commission nationale de l'informatique et des libertés ». Il ressort de cette disposition une procédure spécifique à la décharge des fonctions du correspondant dans laquelle la CNIL joue un rôle prépondérant. Cette procédure se doit d'être examinée de près car d'elle dépendra la question de la responsabilité du correspondant.

I) La décharge des fonctions, une procédure minutieuse

Selon la loi, la décharge des fonctions du correspondant intervient « sur demande ou après consultation de la CNIL ». Deux types de procédures de décharge sont à distinguer : une décharge à l'initiative du correspondant et une décharge à la demande de la CNIL elle-même.

A/ Une procédure sur l'initiative du responsable du traitement

Lorsque le responsable des traitements envisage de mettre fin aux fonctions du correspondant en raison de manquements constatés dans l'accomplissement de ses fonctions, il doit saisir la CNIL pour consultation. Cette consultation a pour but de protéger le correspondant. La CNIL pourra ainsi procéder à des vérifications des fondements de la demande de décharge : elle pourra vérifier notamment si la décharge des fonctions ne constitue pas une mesure discriminatoire en raison de la mission confiée.

Afin de respecter le principe du contradictoire, le responsable du traitement devra informer le correspondant de cette saisine ainsi que du motif de la décharge. Ce dernier sera à même de formuler ses observations.

Au delà des considérations procédurales, on peut se demander sur quels motifs se fondera le responsable des traitements pour estimer que le correspondant a failli à ses missions.

A première vue, les motifs invoqués seront sans nul doute les manquements aux missions du correspondant précisées dans la loi, à savoir, la tenue de la liste des traitements mis en œuvre et la veille au respect des dispositions de la loi de 1978. Toutefois, n'ayant aucune compétence en matière de protection des données à caractère personnel, comment ce dernier sera-t-il en mesure de prendre une telle décision. Se pose également la question du caractère de l'obligation de veiller au respect de la loi : est-ce une obligation de moyen ou de résultat ? N'oublions pas que le responsable des traitements doit mettre à la disposition du correspondant les moyens d'accomplir ses missions.

Une autre interrogation survient : dans l'hypothèse où la CNIL ne relève pas de manquements réels de la part du correspondant et qu'elle rend un avis défavorable à la décharge, le responsable des traitements sera-t-il dans l'obligation de suivre cet avis ou ne s'agit-il que d'un avis consultatif ? En raison de la matière législative dans laquelle nous nous situons et en raison de l'absence de précisions apportées par le III de l'article 22, il apparaît que cet avis demeure consultatif. Dans une telle perspective, on peut se demander si cette protection accordée par le législateur n'est pas réduite à néant mettant par là même le correspondant dans une situation de grande précarité. De toute façon, une obligation de se conformer à l'avis de la CNIL impliquant une réintégration du correspondant n'aurait-elle pas eu pour conséquence de rendre difficiles les relations de travail entre le correspondant et le responsable des traitements ? Une collaboration entre les deux acteurs étant indispensable au bon accomplissement des missions du correspondant, la fonction de correspondant aurait perdu tout son sens.

Concernant le correspondant introduit dans les collectivités territoriales, une autre ambiguïté apparaît : le responsable du traitement en procédant à la décharge des fonctions du correspondant se voit attribuer les compétences réservées à l'autorité territoriale à savoir le pouvoir de retrait d'affectation et le pouvoir de sanction. Comment est-il possible de concilier cette disposition de la loi avec les règles de la fonction publique territoriale ? Soulignons tout de même que cette difficulté ne se pose pas pour les communes : en effet, selon la doctrine de la CNIL, le maire est considéré comme le responsable du traitement. De ce fait, il y a convergence d'identité entre le responsable du traitement et l'autorité compétence pour mettre fin à une mission.

Cette incompatibilité entre les dispositions de la loi et les règles de la fonction publique sera également soulevée au regard de la divergence entre les procédures de décharge des fonctions prévues par la loi et les procédures de décharge propre à la fonction publique.

Toutes ces interrogations devront de manière certaine être réglées par le décret d'application sous peine d'affaiblir les missions du correspondant et d'assombrir un peu plus son statut.

B/ Une procédure sur l'initiative de la CNIL

Selon le III de l'article 22, la CNIL pourra demander au responsable des traitements de décharger le correspondant à la protection des données non diligent de ses fonctions. Cette possibilité a également été prévue par la loi fédérale allemande du 1^{er} janvier 2002 relative à la protection des données. Le troisième alinéa de son article 4(f) dispose que « la nomination du détaché à la protection des données peut être révoquée en application de l'article 626 du Code civil allemand ; ou dans le cas des organismes privés, également sur demande de l'autorité de contrôle »¹¹¹.

Une procédure contradictoire devra être mise en place : ainsi, avant toute demande de décharge des fonctions au responsable des traitements, le correspondant devra être informé par la CNIL des griefs qui lui sont reprochés et pourra formuler des observations auprès de cette dernière.

Cette faculté de la CNIL de pouvoir demander au responsable des traitements la décharge des fonctions du correspondant montre sa place prépondérante dans le dispositif des correspondant mais également le renforcement de ses pouvoirs de sanction. On pourrait même aller jusqu'à dire que la CNIL s'érige en une sorte de « commission disciplinaire » des correspondants. Cette comparaison ne laisse pas sans rappeler les commissions disciplinaires des professions réglementées.

Cette procédure, comme celle à l'initiative du responsable des traitements, suscite cependant certaines interrogations.

En premier lieu, se pose le problème de l'appréciation des manquements du correspondant. On peut se demander sur quels fondements la CNIL appréciera ces manquements. En toute logique, cette appréciation s'effectuera au regard des missions du correspondant à savoir, la veille du respect de la loi relative à l'informatique, aux fichiers et aux libertés et la tenue du registre.

A titre d'illustration, il serait intéressant de comparer les manquements du correspondant à la protection des données à caractère personnel avec ceux du commissaire aux comptes, ces derniers ayant des missions similaires. Ainsi, est considéré comme un manquement, le fait pour le commissaire aux comptes de ne pas déclencher la procédure d'alerte, dans le cadre de la prévention des difficultés de l'entreprise, ou de la déclencher de manière inopportune. On pourrait donc imaginer pour le correspondant, titulaire également d'une mission d'alerte et de mise en garde, que soit considéré comme un manquement le fait de ne pas la mettre en œuvre lorsque des traitements contreviennent manifestement à la vie privée et aux libertés individuelles mais également lorsque ce dernier l'a mis en œuvre alors que les circonstances ne s'y prêtaient pas.

On pourrait également imaginer comme manquement, la mauvaise qualification juridique faite par le correspondant d'un traitement soumis à autorisation ou avis. Cette dernière hypothèse montre toute l'importance de la formation du correspondant et de contacts réguliers de ce dernier avec la CNIL en cas de doutes sur un traitement.

Cependant, il est certain que le décret se devra de préciser de manière plus approfondie ces missions afin que puisse être déterminé en quoi consiste un « correspondant non diligent ». Eric BRABY, membre de l'Association Française des Correspondants à la Protection des Données (AFCPD), considère également que « la notion de devoirs du correspondant devra nécessairement être précisée au sein d'un référentiel de bonnes pratiques et/ou d'un code de conduite, axe de travail dans lequel s'est aussi engagée l'AFCPD »¹¹².

En second lieu, on peut se demander dans quelles circonstances la CNIL sera-t-elle amenée à constater les manquements correspondant. Cette constatation aura certainement lieu dans le cadre des contrôles sur place et sur pièce, prévus à l'article 44 de la loi de 1978, qu'effectueront les agents de la CNIL au sein des organismes mettant en œuvre les traitements de données. Comment la CNIL choisira-t-elle les organismes

¹¹¹ loi fédérale allemande du 1^{er} janvier 2002 relative à la protection des données, ref :

http://www.bfd.bund.de/information/bdsg_fra.pdf

¹¹² Eric BRABY, « Le correspondant CNIL », L'informatique professionnelle n°229, décembre 2004, p.12

et les correspondants soumis à ces contrôles. Se basera-t-elle sur des dénonciations ou sur une méthode totalement aléatoire ?

Ajoutons que ces contrôles constitueront une charge supplémentaire de travail pour la CNIL. A la vue des effectifs insuffisants de cette dernière et des contrôles a posteriori des traitements de données à caractère personnel que prévoit de réaliser la CNIL, il est à craindre que cette dernière ne puisse pas être en mesure d'effectuer des contrôles sur les correspondants en place. Or, sans ces derniers, il semble peu probable la procédure de décharge des fonctions du correspondant à l'initiative de la CNIL soit véritablement effective. Les seuls exemples de décharge seront certainement ceux à l'initiative des responsables des traitements.

Enfin, la rédaction de la disposition relative à la décharge des fonctions, de par son imprécision, amène une ambiguïté juridique. Cette disposition indique que la décharge pourra se faire « sur la demande de la CNIL ». Cette demande faite au correspondant peut-elle être interprétée comme une injonction de la part de la CNIL ? Si c'est le cas, on assiste une fois de plus au renforcement des pouvoirs de la CNIL, une injonction étant de manière classique un pouvoir attribué au juge. De plus, il serait utile que cette injonction soit assortie de sanctions dans l'hypothèse d'un refus.

Ajoutons, pour conclure, que la procédure de décharge des fonctions constitue le pivot central du dispositif des correspondants. L'établissement d'une responsabilité du correspondant suite à une telle procédure permettrait sans nul doute d'accroître la confiance des organismes en ce nouveau dispositif. Cependant, il semble que cet état de fait n'ait pas retenu l'attention du législateur : cette décharge des fonctions n'entraîne, à la lecture de la loi, aucune véritable responsabilité du correspondant.

II) Une décharge n'entraînant aucune sanction

Ni la directive, ni la loi ne posent de responsabilité du correspondant à la protection des données à caractère personnel.

Or, une telle responsabilité est essentielle au bon fonctionnement du dispositif des correspondants. Sans cette responsabilité, le correspondant ne pourra pas apporter la preuve de son utilité et s'avérera sans aucun doute peu crédible face aux responsables des traitements, aux usagers et aux salariés.

L'enjeu d'une telle responsabilité n'a pourtant pas échappé à certains pays : au Canada, la loi sur la protection des renseignements personnels et les documents électroniques impose aux entreprises de désigner une personne chargée de faire respecter les principes édictés par la loi en terme de protection de la vie privée. Cette personne voit sa responsabilité personnelle engagée lors d'éventuelles défaillances dans l'accomplissement de ses missions. Une telle responsabilité ne paraît pas adaptée en France car elle contribuerait de manière certaine à l'impopularité du dispositif auprès des entreprises et des collectivités. En effet, il est à craindre, qu'à la vue du risque juridique auquel ils s'exposent, les postulants à la fonction de correspondant s'avèrent peu nombreux. Nous nous trouvons là encore face à un paradoxe : la mise en place d'une responsabilité est indispensable au bon fonctionnement du dispositif mais pourrait également être la source de son impopularité. Ce sera donc au décret d'application de solutionner un tel problème.

Se pose également la question de savoir quel type de responsabilité pourrait être mis en cause. Le correspondant verra-t-il engager sa responsabilité sur le plan civil ou sur le plan pénal ? Une responsabilité

pénale serait peut-être trop excessive mais cependant, elle semble envisageable au motif que certains faits contrevenant à la loi « informatique et libertés » sont incriminés aux articles L226-16 et suivant du Code pénal dans une section intitulée « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ». A titre d'exemple, l'article L226-18-1 du Code pénal incrimine « le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes ». Ces incriminations engagent la responsabilité pénale du responsable du traitement.

A l'heure actuelle, l'absence de responsabilité qui caractérise le statut du correspondant permet de penser que les organismes souhaitant bénéficier de la dérogation du III de l'article 22 se dirigeront vers des professions réglementées telles que les professions d'avocat afin de réduire les risques inhérents à un tel secteur. Ces derniers disposent, en effet, d'une assurance professionnelle.

CONCLUSION

De par l'allégement du système des formalités préalables à la mise en œuvre des traitements dont bénéficient les responsables des traitements, la garantie de la vie privée et des libertés individuelles au sein des entreprises et des collectivités locales et la diffusion de la «culture CNIL » auprès du public, le correspondant à la protection des données à caractère personnel ne pouvait que constituer une avancée remarquable dans le domaine de la protection des données.

Cependant, le manque de clarté juridique entourant le statut de cette nouvelle institution, notamment au regard de sa formation, de la mise en œuvre de son indépendance et de l'absence de responsabilité pousse à penser qu'il est une sorte de gadget juridique introduit par le législateur. En effet, même si ce nouvel acteur remporte un franc succès chez nos voisins européens (Allemagne, Suède, Pays-Bas...) ¹¹³, il a été facilement oublié que la réussite de l'implantation du correspondant dans d'autres pays était en majorité due aux garanties juridiques apportées à la fonction telles que la mise en place d'un statut de salarié protégé afin que ce dernier puisse exercer ses missions de manière véritablement «indépendante » ou encore l'instauration d'une responsabilité en cas de manquement du correspondant.

Le choix français, lors de la transposition de l'article 18 de la directive 95/46/CE dans la loi du 6 août 2004, a été d'expérimenter d'abord plutôt que de statufier. Nous verrons donc avec le temps si ce flou juridique se résorbera avec la pratique et si l'engouement annoncé pour le correspondant, constaté actuellement dans une certaine mesure avec l'apparition de l'Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCDP) ¹¹⁴, sera confirmé chez les entreprises et les collectivités locales ou si ce nouvel acteur est prédit à une complète ineffectivité.

Il faut espérer que la publication prochaine du décret d'application, qui aurait dû intervenir en juin selon les prévisions de la CNIL, répondra aux diverses interrogations émises depuis les travaux préparatoires de la loi du 6 août 2004.

¹¹³ Selon l'étude réalisée par la CNIL, 5 324 responsables de traitement ont désigné un détaché à la protection des données à caractère personnel et 3 133 détachés sont recensés par l'autorité de contrôle suédoise. Au Luxembourg, qui n'a introduit le dispositif que fin 2004, 29 détachés figurent sur le registre des détachés mis en ligne au 25 février 2005. ref : <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/dpo-comparaison-UE-VD.pdf>

¹¹⁴ Voir leur site <http://www.afcdp.org>

Nous nous trouvons donc, pour l'instant, dans une position d'attentisme : cette situation peut s'avérer dangereuse du fait que l'instauration d'une telle fonction au sein des entreprises comme au sein des collectivités locales nécessite un aménagement long et complexe notamment en terme de coût et de logistique.

La mise en place d'un tel correspondant nécessite des investissements financiers importants au regard du recrutement et de la formation de ce dernier pour les entreprises et collectivités locales souhaitant internaliser la fonction et au regard du recours à des organismes spécialisés de correspondants pour les structures souhaitant l'externaliser. La situation d'inégalité résultant de la mise en place du dispositif crainte depuis le début par Guy BRAIBANT notamment pourrait donc s'avérer être une réalité : les petites structures pourraient se trouver exclues du bénéfice de cet acteur.

De plus, en terme de fonctionnement, l'instauration du correspondant à la protection des données à caractère personnel entraînera forcément une modification de l'organisation du travail difficile à réaliser dans les deux secteurs, public comme privé. Ce problème sera notamment difficile à surmonter au niveau local où 36 000 communes sont concernées. A ce titre, la CNIL prévoit d'ores et déjà des dispositions permettant un meilleur encadrement de la coordination locale et notamment le déploiement de «délégations interrégionales, vraisemblablement au nombre de quatre suivant la division des préfixes téléphoniques »¹¹⁵.

L'inconsistance du statut du correspondant rejaillit également sur l'image et la notoriété de la CNIL. En effet, il paraît opportun de se demander si cette inconsistance n'affaiblit pas les pouvoirs même de la CNIL, les correspondants constituant des sortes de relais locaux à cette dernière.

Cette réflexion entre dans le cadre du constat d'une Commission déjà fortement affaiblie. En effet, comme il a pu l'être souligné précédemment, la CNIL dénonce depuis un certain nombre d'années le manque de moyens humains et financiers. Cette insuffisance de moyens paraît tout à fait incohérente au regard des missions importantes dont la CNIL a la charge et du renforcement de ses pouvoirs a posteriori intervenu depuis la loi du 6 août 2004.

Alex TÜRK, président de la CNIL, affirme lui-même : « Je suis inquiet pour l'avenir de la CNIL ». C'est justement cet avenir qui nous dira si l'article 22 III de la loi du 6 janvier 1978 modifiée ne sera pas lettre morte et ainsi si le correspondant à la protection des données à caractère personnel n'est pas une chimère derrière laquelle nous courrons de manière insensée...

BIBLIOGRAPHIE

¹¹⁵ Interview d'Alex TÜRK pour Yahoo Actualités, avril 2005, <http://fr.news.yahoo.com>

- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données, JOCE n°L281 du 23 novembre 1995 p.0031-0050
- Loi n°2004-182 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JO du 7 août 2004, p.14063
- Loi fédérale relative à la protection des données du 1^{er} janvier 2002, http://www.bfd.bund.de/information/bdsg_fra.pdf
- Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, JO du 7 janvier 1978
- Loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, JORF du 27 janvier 1984, ref : <http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=5874&indiceNav=1&tableNav=CONSOLIDE&ligneDebNav=1>
- The Privacy Act 5 U.S.C § 552a, As amended By Public Law Ref: <http://www.usdoj.gov/04foia/privstat.htm>
- Décret n°69-810 du 12 août 1969 relatif à l'organisation de la profession et au statut professionnel des commissaires aux comptes, JORF 29 août 1969 rectificatif JORF 12 septembre 1969, ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=4720380&indice=1&table=LEGI&ligneDeb=1>
- Décret n° 82-447 du 28 mai 1982 sur l'exercice du droit syndical dans la fonction publique, JORF du 30 mai 1982, ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=272818&indice=1&table=LEGI&ligneDeb=1>
- Décret n°2005-599 du 27 mai 2005 portant modification du décret n° 69-810 du 12 août 1969 relatif à l'organisation de la profession et au statut professionnel des commissaires aux comptes, NOR:JUSC0520338D, JORF 29 mai 2005, ref. : <http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=27419&indiceNav=1&tableNav=CONSOLIDE&ligneDebNav=1>
- Rapport BRAIBANT « Données personnelles et société de l'information » présenté au gouvernement sur la transposition en droit français de la directive européenne du 24 octobre 1995 relatif au traitement des données et à leur libre circulation du 3 mars 1998, La Documentation française (coll. « Rapports officiels »), 291p.
- Rapport n° 218 du 19 mars 2003 élaboré par Alex TÜRK au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, Ref : <http://www.senat.fr/rap/102-218/102-2181.pdf>
- Compte-rendu intégral du Sénat du 1^{er} avril 2003 p.39, <http://www.senat.fr>
- Rapport DELATTRE n°1538, séance de l'Assemblée Nationale du 13 avril 2004, <http://www.assemblee-nationale.fr/12/rapports/r1537.asp>
- Compte rendu analytique officiel de l'Assemblée nationale, séance du 29 avril 2004, <http://www.assemblee-nationale.fr/12/pdf/cri/2003-2004/cahiers/c20040205.pdf>

- René CHAPUS, « Droit administratif général Tome 2 », 15^{ème} édition, MONTCHRETIEN, 797 pages
- Georges ORWELL, « 1984 », 1949, Gallimard « Folio », 1972, Paris, traduction de l'anglais par Amélie AUDIBERTI
- Nicolas SAMARCQ, « Le correspondant CNIL, un nouveau label pour les entreprises respectueuses de la vie privée des citoyens ? », avril 2005, http://www.droit-ntic.com/news/print_news.php?news=293
- Valérie BOCCARA, « Loi informatique et libertés : des sanctions fortes, des risques accrus », Petites affiches n°33, 16 février 2005 p.3
- Herbert MAISL, « Informatique et libertés : de 1978 à 2004 », Communication-Commerce électronique, janvier 2005 p. 4
- Fabrice FEVRIER, « Les nouvelles obligations de l'employeurs après la réforme de la loi de 1978 relative à l'informatique, aux fichiers et aux libertés », janvier 2005, http://www.droit-ntic.com/news/print_news.php?news=280
- Sophie VULLIET-TAVERNIER, « Après la loi du 6 août 2004 : nouvelle loi « informatique et libertés », nouvelle CNIL ? », Droit social n°12, décembre 2004 p.1055
- Eric BRABY, « Le correspondant CNIL », L'informatique professionnelle n°229, décembre 2004 p.10
- Nathalie METALLINOS, « La fonction de détaché à la protection des données en Allemagne et aux Pays-Bas », Droit social n°12, décembre 2004 p.1066
- Patrick HAUSS, « Un correspondant CNIL extérieur à l'entreprise ? », novembre 2004, http://www.clic-droit.com/web/editorial/imprimer.php?art_id=310
- Alain BENSOUSSAN, « Le correspondant à la protection des données à caractère personnel : un maillon important de la réforme », Gazette du palais, 10 au 12 octobre 2004 p.7
- Alain BENSOUSSAN, « Le correspondant à la protection des données à caractère personnel », <http://www.alain-bensoussan.com/pages/130/>
- Eric A. CAPRIOLI et Anne CANTERO, « La loi n°2004-801 du 6 août 2004 sur les données personnelles : pouvoirs pour la CNIL et nouvelles opportunités pour les entreprises », octobre 2004, http://www.caprioli-avocats.com/pages/publications/edocs/edocs_donneesperso_cnil.ht
- Etienne DROUARD, « La transition entre la loi « informatique & libertés » de 1978 et celle de 2004 », Expertises, octobre 2004 p.335
- Gérard HAAS, « Correspondant à la protection des données : une nouvelle fonction informatique », octobre 2004, http://www.journaldunet.com/juridique/juridique_041019.shtml
- Alex TÜRK, « Loi informatique et liberté : la protection des personnes sort renforcée », août 2004, <http://www.journaldunet.com/tribune/040831turk.shtml>
- Hervé GABADOU et Sébastien LALOUE, « Le correspondant à la protection des données va voir le jour : pour quelle mission ? », août 2004, http://www.clic-droit.com/web/editorial/imprimer.php?art_id=292

- Oriane COINTET, « Quand la CNIL déconcentre : le dispositif du correspondant à la protection des données personnelles en voie d'être adopté », 16 juillet 2004, <http://www.legalbiznext.com/cgi-bin/news/viewnews.cgi?category=8>
- Frank GARNIER, « L'émergence des Chief Privacy Officer », juillet 2004, http://www.csecurity.com/site/html/article_emerge_CPO.php
- Hubert D'ERCEVILLE, « Premiers correspondants pour la CNIL », juillet 2004, <http://www.01net.com/article/247030.html>
- Claire LEVALLOIS BARTH et Arnaud BELLEIL, « Le correspondant informatique et libertés : une fonction en attente de clarification », Expertises n°283, juillet 2004
- Joël BOYER, « Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? », Petites Affiches n°102 du 22 mai 2003 p.4
- Georges CHATILLON, « Confiance envers l'administration électronique – perspectives pour un cadre juridique des données personnelles et de la vie privée », mars 2002, <http://dss-droit-internet.univ-paris1.fr/bibliotheque/>
- Jérôme THOREL, « Fichiers, embrouilles et liberté de la presse », février 2002, <http://www.zdnet.fr> www.zdnet.fr/actualites/internet/0,39020774,2103952,00.htm
- Robert GOLD, « A Primer for Your Chief Privacy Officer (CPO) », juin 2001, <http://www.e-commercealert.com/article297.html>
- Florent LATRIVE, « A client fiché, directeur d'intimité », Libération, 27 janvier 2001
- Jean CUMMING, « The privacy net », <http://www.cba.org/CBA/National/janfeb04/feature1.aspx>
- Conférence de presse de la CNIL du 20 avril 2005, http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/DP-conf2005.pdf
- 1ères Assises des Correspondants Informatiques et Libertés du 21 avril 2005
- « Le correspondant presse : un régime dérogatoire pour tenir compte de la liberté de la presse », avril 2005, <http://www.cnil.fr/index.php?id=1796&news%5Buid%5D=252&cHash=8051858754>
- 25^{ème} rapport d'activité de la CNIL (année 2004), La Documentation Française, 2005, 112 p.
- Le Forum des droits de l'internet, « loi informatique et libertés, un nouveau cadre juridique pour les traitements de données à caractère personnel », octobre 2004 p.24
- « Le CIL : un vecteur de diffusion de la culture informatique et libertés », juin 2005, <http://www.cnil.fr/index.php?id=1835>
- « Le Correspondant informatique et libertés (CIL) », mai 2005, [http://www.cnil.fr/index.php?id=1823&news\[uid\]=265&cHash=bb74b7630e](http://www.cnil.fr/index.php?id=1823&news[uid]=265&cHash=bb74b7630e)
- « Les collectivités locales et la protection des données personnelles », février 2005, <http://www.cnil.fr/index.php?id=1717&print=1>
- « La transposition de la directive 95/46/CE », <http://www.cnil.fr/index.php?id=1351>

- « Etude de droit comparé sur les correspondants à la protection des données », <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/dpo-comparaison-UE-VD.pdf>
- « Premières décisions de la CNIL en matière d'autorisations », décembre 2004, <http://www.cnil.fr/index.php?id=1735>
- « La CNIL rend publique sa vision du correspondant informatique et libertés », novembre 2004, <http://www.cnil.fr/index.php?id=1707>
- « Collectivités locales et administration électronique », novembre 2004, <http://www.cnil.fr/index.php?id=1295>
- « Nouvelle loi informatique et libertés : instauration possible de correspondants à la protection des données dans les collectivités locales », juillet 2004, <http://www.maire-info.com/articles/archive.asp?param=4639>
- « Lois sur la protection des renseignements personnels au Canada », http://www.privcom.gc.ca/fs-fi/02_05_d_15_f.asp
- « Se conformer à la Loi sur la protection des renseignements personnels et les documents électroniques », http://www.privcom.gc.ca/fs-fi/02_05_d_16_f.asp
- « Les correspondants CNIL », juillet 2003, <http://www.juristic.net/article83.html>
- Association Française des Correspondants à la Protection des Données à Caractère Personnel, <http://www.afcdp.org>
- Conseil Constitutionnel, décision n°2004-499 DC du 29 juillet 2004, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=391&indice=1&table=CONSTIT&ligneDeb=1>
- C. Constitutionnel, décision n°2003-467 du 13 mars 2003 relative à la loi pour la sécurité intérieure, Journal officiel du 19 mars 2003, p. 4789, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=357&indice=1&table=CONSTIT&ligneDeb=1>
- C. Constitutionnel, décision n° 94-352 DC du 18 janvier 1995 relative à la loi d'orientation et de programmation relative à la sécurité, Journal officiel du 21 janvier 1995, p. 1154, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=2749&indice=1&table=CONSTIT&ligneDeb=1>
- C. Constitutionnel, décision n° 92-316 DC concernant la loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, Journal officiel du 22 janvier 1993, p. 1118, Ref : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=2680&indice=1&table=CONSTIT&ligneDeb=1>

ANNEXE 1

Décret n°81-1219 du 30 décembre 1981

Décret relatif à l'organisation de l'administration centrale du ministère de l'intérieur et de la décentralisation.

version consolidée au 23 mai 1984 - [version JO initiale](#)

Le Premier ministre, Sur le rapport du ministre d'Etat, ministre de l'intérieur et de la décentralisation, Vu la loi n° 45-01 du 24 novembre 1945 relative aux attributions des ministres et à l'organisation des ministères, modifiée par le décret n° 59-178 du 22 janvier 1959 relatif aux attributions des ministres.
Vu la loi n° 66-492 du 9 juillet 1966 portant organisation de la police nationale ;
Vu le décret n° 81-241 du 12 mars 1981 portant statut de l'inspection générale de l'administration au ministère de l'intérieur ;
Vu l'avis du comité technique paritaire central du ministère de l'intérieur en date du 14 décembre 1981 ;
Vu l'avis du comité technique paritaire central des services actifs de la police nationale en date du 14 décembre 1981 ;
Vu l'avis du comité technique paritaire des services techniques du matériel en date du 18 décembre 1981 ;
Vu l'avis du comité technique paritaire du service des transmissions en date du 23 décembre 1981,

Article 1

Les attributions de l'administration centrale du ministère de l'intérieur et de la décentralisation ressortissent aux directions générales, directions et services suivants :

1. Direction générale de l'administration ;
2. Direction générale des collectivités locales ;
3. Direction générale de la police nationale ;
4. Direction de la réglementation et du contentieux ;
5. Direction de la sécurité civile ;
6. Direction des transmissions et de l'informatique ;
7. Direction des affaires politiques, administratives et financières de l'outre-mer ;
8. Direction des affaires économiques, sociales et culturelles de l'outre-mer ;
9. Services rattachés au cabinet du ministre.

Article 2

Le ministre d'Etat, ministre de l'intérieur et de la décentralisation, dispose de l'inspection générale de l'administration.

Le haut fonctionnaire de défense assiste le ministre d'Etat, ministre de l'intérieur et de la décentralisation, pour l'exercice de ses responsabilités de défense.

Article 3

Le directeur général de l'administration anime et coordonne les services chargés :

1. Des affaires politiques ;
2. De la gestion des personnels, à l'exception des personnels administratifs et actifs de la police nationale ;
3. Des affaires financières, immobilières et sociales.

Deux directeurs d'administration centrale, adjoints au directeur général, assistent celui-ci dans l'exercice de ses missions.

Article 4

Le directeur général des collectivités locales anime et coordonne les services chargés :

1. De l'équipement et du développement des collectivités locales ;
2. De leurs finances ;
3. De leur personnel ;
4. Des structures des collectivités locales, de leurs services et de leurs établissements publics.

Il est également chargé d'un service conseil des maires.

Article 5

Le directeur général de la police nationale anime et coordonne les activités :

1. De la direction du personnel de la police ;
2. De la direction de la formation et de l'équipement de la police ;
3. Des directions et services actifs de police.

Article 6

Le directeur de la réglementation et du contentieux anime et coordonne les services chargés :

- De la réglementation du statut des étrangers et de la circulation transfrontière ;
- De la réglementation intérieure, notamment en matière de sûreté de l'Etat, d'ordre public, de salubrité et de tranquillité publique, de circulation et de sécurité routière ;
- Du contentieux général et des affaires juridiques.

Article 7

Le directeur de la sécurité civile anime et coordonne les services chargés de l'étude et de la mise en oeuvre des mesures de prévention et de secours destinées à assurer la sauvegarde des personnes et des biens, en cas d'accidents, de sinistres et catastrophes ou dans les circonstances ressortissant à la défense civile.

Article 8

Le directeur des transmissions et de l'informatique assure, en accord avec les services utilisateurs, la préparation du schéma directeur de développement des transmissions et des plans d'exécution de ce schéma. Dans les mêmes conditions, il assure, en liaison avec la commission de l'informatique, la préparation du schéma directeur de développement de l'informatique et de la bureautique et des plans d'exécution de ce schéma.

Il anime et coordonne les services chargés des études et de l'exploitation des systèmes de transmission et de traitement de l'information.

Article 9

Des arrêtés du ministre d'Etat, ministre de l'intérieur et de la décentralisation, fixeront l'organisation intérieure et les attributions des directions et services visés aux articles 1er à 8.

Article 10

Le décret n° 75-714 du 23 juillet 1975 relatif à l'organisation de l'administration centrale du ministère de l'intérieur, modifié par les décrets n° 75-1111 du 5 décembre 1975 et n° 79-854

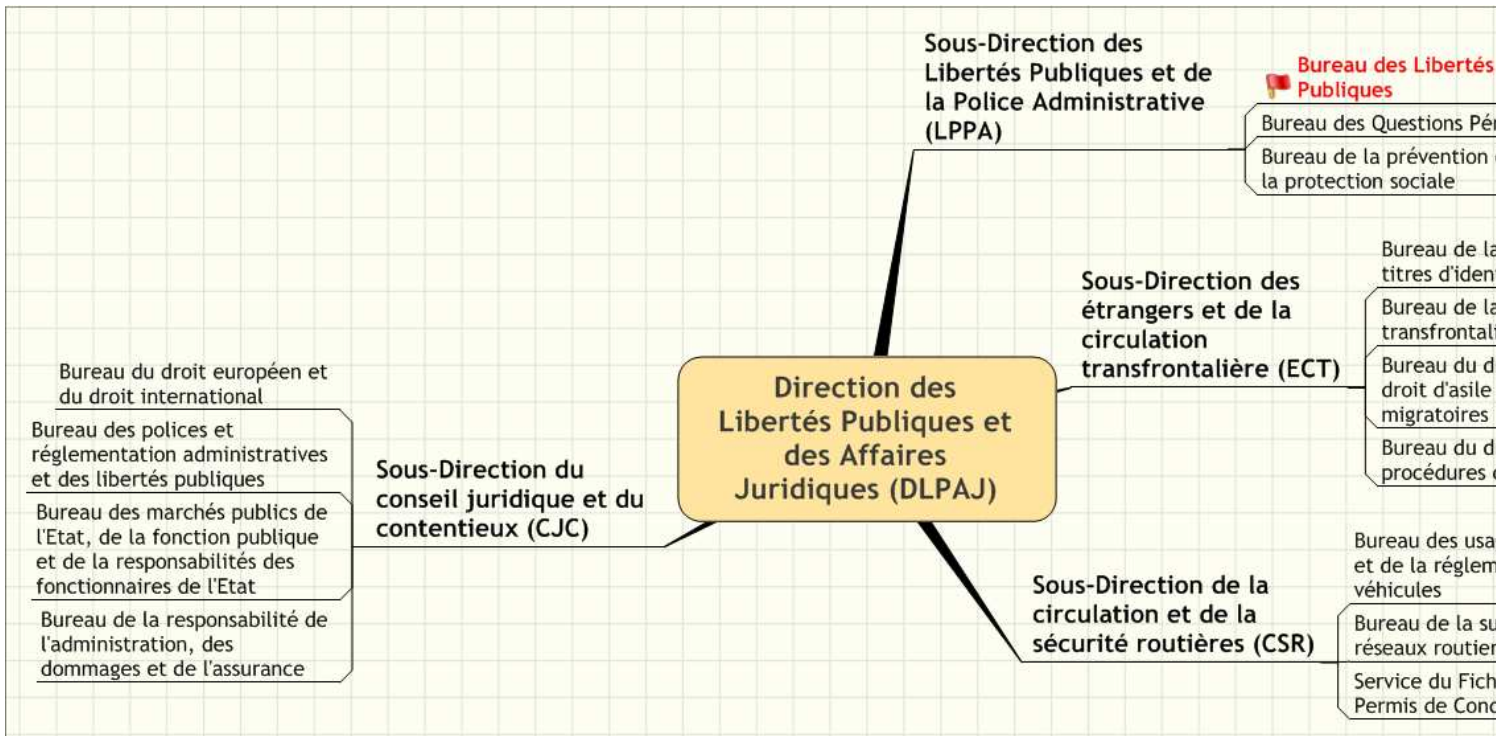
du 3 octobre 1979, est abrogé.

Article 11

Le ministre d'Etat, ministre de l'intérieur et de la décentralisation, est chargé de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

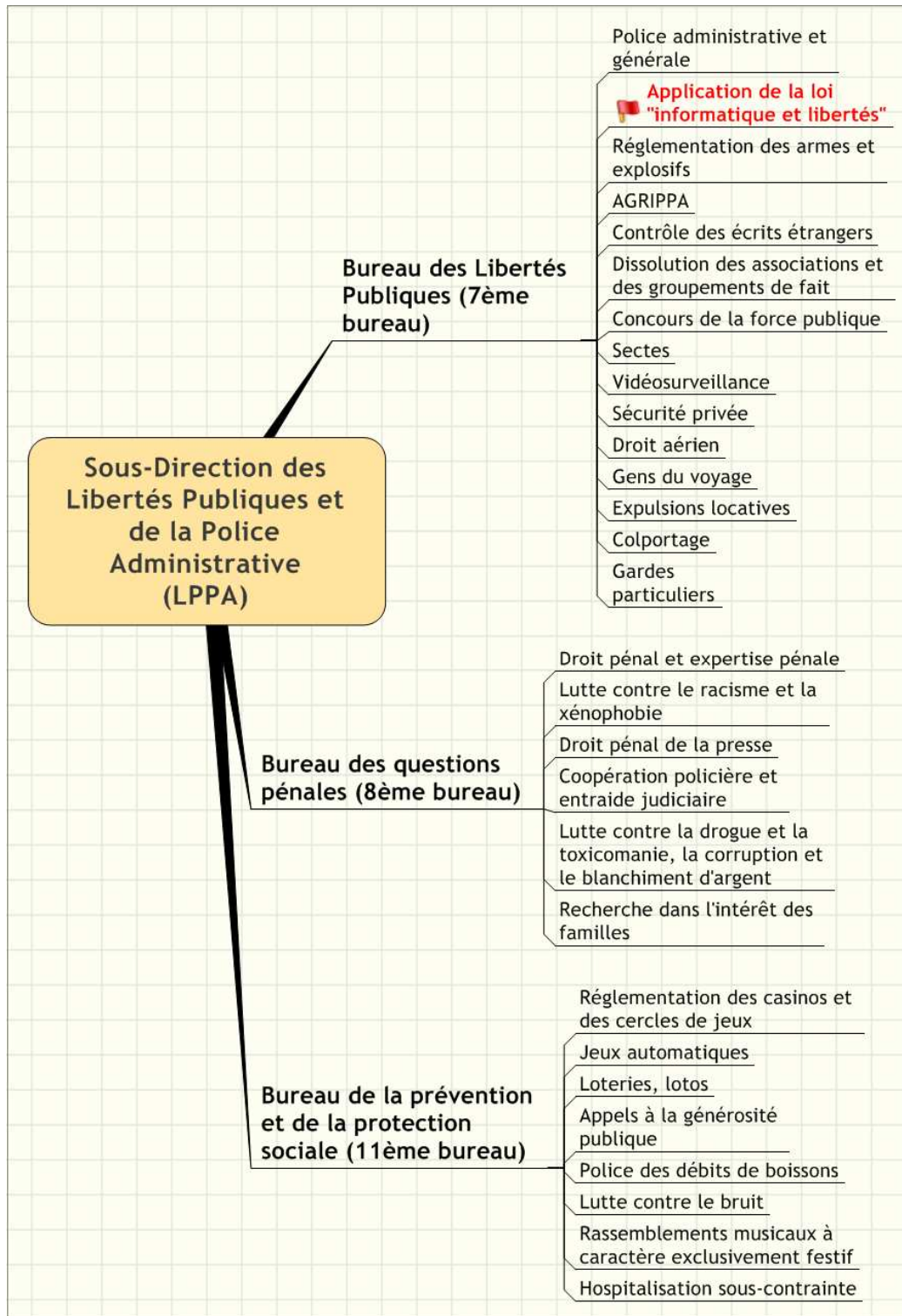
ANNEXE 3

Organigramme de la Direction des Libertés Publiques et des Affaires Juridiques



ANNEXE 4

Organigramme de la Sous-Direction des Libertés Publiques et de la Police Administrative



ANNEXE 5

J.O n° 64 du 17 mars 1993 page texte n°

TEXTES GENERAUX

PREMIER MINISTRE

Circulaire du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés: application aux administrations et à l'ensemble du secteur public de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés; rôle des ministères et coordination par le commissaire du Gouvernement auprès de la Commission nationale de l'informatique et des libertés (C.N.I.L.)

NOR: PRMX9310900C

Paris, le 12 mars 1993.

Face au développement constant des fichiers informatisés de personnes, deux textes constituent aujourd'hui le cadre juridique de la protection des données et, par conséquent, de la vie privée en matière de traitements automatisés: la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 20 janvier 1981, ratifiée par la France en 1985 (Journal officiel du 20 novembre 1985) dite <<Convention 108>>.

La mise en oeuvre de ces textes au cours des dernières années permet aujourd'hui, à la lumière de l'expérience acquise, d'envisager de nouvelles mesures qui sont de nature à améliorer leur application et à renforcer leur efficacité.

La portée de ces textes doit être entendue dans son acception la plus large, qu'il s'agisse de la référence faite par la loi au <<traitement automatisé des données à caractère personnel>> ou par la convention au <<traitement automatisé d'informations nominatives>>. Une attention toute spéciale sera portée aux traitements automatisés concernant des applications qui recourent à l'image et au son, tels que les messageries électroniques ou les systèmes de vidéosurveillance.

La commercialisation des fichiers ou l'accès direct à ceux-ci peuvent aussi poser des problèmes de protection de la vie privée dont il convient de mesurer l'importance.

Une vigilance particulière doit également être apportée aux applications comportant des transmissions de données à l'étranger (flux transfrontières de données), en raison notamment des incidences du développement de la libre circulation des biens, des services et des personnes.

En conséquence, il appartient à chaque département ministériel, dans le respect des orientations du Gouvernement, d'élaborer ses propres directives en ce qui concerne le développement de l'informatique, en veillant à ce que soient plus largement prises en compte toutes les dimensions de la protection de la vie privée.

Le commissaire du Gouvernement auprès de la C.N.I.L. sera tenu informé des directives que vous donnerez à vos services et de leur mise en oeuvre dans votre département. Il m'en rendra compte chaque année.

La présente circulaire abroge et remplace la circulaire du 30 juillet 1982 relative aux liaisons entre la C.N.I.L. et les administrations. Vous veillerez à son application effective en prenant les mesures prévues ci-après.

1. Désignation dans chaque ministère d'un haut fonctionnaire comme correspondant du commissaire du Gouvernement auprès de la C.N.I.L.

1.1. Le correspondant du commissaire du Gouvernement auprès de la C.N.I.L.

sera un directeur d'administration centrale, ou un fonctionnaire de rang équivalent, choisi notamment parmi les membres d'une inspection.

Ce haut fonctionnaire aura pour mission de veiller à la protection de la vie privée dans les traitements automatisés. Il veillera à ce que les projets particulièrement sensibles tiennent le plus grand compte, dès leur conception, des impératifs de protection de la vie privée. Il coordonnera la préparation des décisions des services en ce qui concerne celles de leurs attributions qui peuvent être en relation avec l'objet de sa mission.

Pour les dossiers relatifs aux traitements utilisant des données sensibles, aux traitements faisant appel à des innovations technologiques, aux traitements de fichiers de population, aux interconnexions et communications hors frontières, ce haut fonctionnaire saisira le commissaire du Gouvernement auprès de la C.N.I.L. du dossier définitif de demande d'avis au plus tard trois semaines avant sa transmission à la Commission nationale de l'informatique et des libertés.

Ce dispositif sera complété par la désignation d'un membre de votre cabinet chargé de suivre les dossiers <<Informatique et libertés>>, en liaison avec le haut fonctionnaire désigné et le commissaire du Gouvernement auprès de la C.N.I.L.

Le Premier ministre

à Mesdames et Messieurs les ministres et secrétaires d'Etat
 touche tous les domaines d'activité de l'administration et du secteur public.

| |
|--|
| |
|--|

| | |
|---|---------------------------------------|
| <p style="text-align: center;">DIRECTION DES LIBERTES PUBLIQUES ET DES AFFAIRES JURIDIQUES</p> <p style="text-align: center;">Bureau des libertés publiques</p> <p><u>Référence :</u></p> | <p><u>REDACTEUR :</u></p> <p>Tel.</p> |
|---|---------------------------------------|

| |
|---------------|
| <u>OBJET:</u> |
|---------------|

| | | | | | |
|---------------------------------|------|---|---|--------------------------------------|--------------------------|
| DESTINATAIRES SUCCESSIFS | VISA | POUR | | | TRANSMISSION DATE |
| | | S I G N A T U R E | I N F O R M A T I O N | D E C I S I O N | |

| | | | | | |
|--|--|--|--|--|--|
| M. DEMATTEIS, Adjoint au Chef du Bureau des Libertés Publiques | | | | | |
| Mme COMPAGNIE, Chef du Bureau des Libertés Publiques | | | | | |
| M. BONNEAU, Sous-Directeur des Libertés Publiques et de la Police Administrative | | | | | |



| | | | | | |
|--|--|--|--|--|--|
| M. FRATACCI, Directeur des Libertés Publiques et des Affaires Juridiques | | | | | |
|--|--|--|--|--|--|

Déclaration NORMALE

| | |
|--|---|
| 1 PREMIERE DECLARATION <input type="checkbox"/> DECLARATION DE MODIFICATION <input type="checkbox"/> DECLARATION DE SUPPRESSION <input type="checkbox"/> Préciser dans ce cas le n° d'enregistrement du traitement que vous souhaitez modifier ou supprimer : <input type="text"/> | Cadre réservé à la CNIL N° d'enregistrement <input type="text"/> <input type="checkbox"/> D <input type="checkbox"/> DT <input type="checkbox"/> A |
|--|---|

2 Organisme déclarant

| | | | |
|----------------------------------|---|--|--------------------------------|
| Statut juridique : | Secteur public <input type="checkbox"/> | Secteur privé <input type="checkbox"/> | N° SIREN <input type="text"/> |
| Nom ou Raison Sociale | | | N° APE <input type="text"/> |
| Adresse | | | Téléphone <input type="text"/> |
| Code postal <input type="text"/> | Ville | | |

3

Service ou organisme chargé de la mise en œuvre du traitement

Si le nom et les coordonnées sont identiques à ceux de l'organisme déclarant, cochez sinon complétez ci-dessous

Nom ou RS
Adresse
Code postal Ville Téléphone

4

Service ou organisme auprès duquel s'exerce le droit d'accès *

Si le nom ET les coordonnées sont identiques 1) à ceux de l'organisme déclarant, cochez 1
2) à ceux du service chargé de la mise en œuvre, cochez 2 sinon complétez ci-dessous

Nom ou RS
Adresse
Code postal Ville Téléphone

5

Traitement déclaré

Nom du logiciel Année de mise en oeuvre
Population concernée (catégories de personnes concernées et nombre approximatif).....
Finalités principales
.....

6

Transferts d'informations hors de l'Union européenne

Existe-t-il des transferts d'informations hors de l'Union européenne ? OUI NON
Si vous répondez « oui », précisez quels sont les pays concernés

7

Personne à contacter

Nom Prénom Fonction.....
Tél : fax : Adresse électronique@.....

8

En cas de déclaration de suppression signer ici et ne pas compléter la feuille 2

Nom du signataire Signature
Fonctions l'habilitant à signer
Date Le (JJ/MM/AAAA) / /

* Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe.

Les informations portées sur ce formulaire et figurant en gras sont obligatoires. Elles font l'objet d'un traitement informatisé à la CNIL et sont destinées aux membres et services de la Commission chargés de l'instruction de votre dossier et au public désireux de s'informer de l'existence d'un fichier dans les conditions prévues à l'article 31 de la loi du 6 janvier 1978. Vous pouvez exercer votre droit d'accès aux informations qui vous concernent en vous adressant à : la CNIL, 21 rue Saint-Guillaume 75340 PARIS cedex 07

9

Fonctions de l'application *

| | |
|----|--|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |

10

Sécurités et secrets

Mettez-vous en place des règles permettant de contrôler l'accès à l'application ?
 OUI 1 NON 2
 Prenez-vous des dispositions pour protéger votre réseau des intrusions extérieures ?
 OUI 1 NON 2
 Les données elles-mêmes font-elles l'objet d'une protection particulière (anonymisation, chiffrement, ...) ?
 OUI 1 NON 2

11

| | | | | | |
|--------------------------|----------|--|--------------------------|----------|---|
| <input type="checkbox"/> | A | Données d'Identification (nom, prénoms sexe, initiales, n°s d'ordre, date et lieu de naissance...) | <input type="checkbox"/> | I | Moyens de déplacement des personnes |
| <input type="checkbox"/> | B | NIR, N° de Sécurité Sociale ou consultation du RNIPP | <input type="checkbox"/> | J | Utilisation des médias et moyens de communication |
| <input type="checkbox"/> | C | Situation familiale | <input type="checkbox"/> | K | Données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes |
| <input type="checkbox"/> | D | Situation militaire | <input type="checkbox"/> | L | Données biométriques |
| <input type="checkbox"/> | E | Formation – Diplômes - Distinctions | <input type="checkbox"/> | M | Santé, données génétiques, vie sexuelle |
| <input type="checkbox"/> | F | Adresse, caractéristiques du logement | <input type="checkbox"/> | N | Habitudes de vie et comportement |
| <input type="checkbox"/> | G | Vie professionnelle | <input type="checkbox"/> | O | Informations en rapport avec la police |
| <input type="checkbox"/> | H | Situation économique et financière | <input type="checkbox"/> | P | Informations relatives aux infractions, condamnations ou mesures de sûreté |

12

Catégories des destinataires

Catégories d'informations fournies *

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|----|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10 | Interconnexion, mise en relation, rapprochement ** | | | | | | | | | | | | | | | |

13

Le traitement a pour objet l'interconnexion de fichiers dont les finalités principales sont différentes ?
 OUI 1 NON 2
 Le traitement a pour objet l'interconnexion de fichiers dont les finalités correspondent à des intérêts publics différents ?
 OUI 1 NON 2
 Les données peuvent- elles êtres cédées, louées, échangées à des fins commerciales ?
 OUI 1 NON 2

14

Nom du signataire..... **Signature**
 Fonctions l'habilitant à signer
 Date

* Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe.

Mesures prises pour faciliter l'exercice du droit d'accès

(Complément de la rubrique 4 du formulaire)

La loi du 6 janvier 1978 reconnaît à toute personne figurant dans un traitement un droit d'accès aux renseignements la concernant (articles 39 et suivants).

De plus, l'article 32. I de la loi prévoit que :

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

1. de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2. de la finalité poursuivie par le traitement auquel les données sont destinées ;
3. du caractère obligatoire ou facultatif des réponses ;
4. des conséquences à son égard d'un défaut de réponse ;
5. des destinataires ou catégories de destinataires des données ;
6. de l'existence d'un droit d'opposition¹¹⁶ au traitement de ses données et d'un droit d'accès et de rectification ;
7. le cas échéant, des transferts de données à destination d'un Etat non membre de la Communauté européenne.

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

1. Quelles sont les mesures d'information adoptées en conséquence (cf. modèles ci-après) ?

Joindre le modèle que vous diffusez effectivement

2. Décrivez les mesures administratives et techniques prises pour faciliter l'exercice du droit d'accès :

- Indiquez le nom du service, ou de la personne habilitée à répondre à ces demandes individuelles d'accès _____

- Indiquez les mesures techniques prises (ex. : possibilité d'accéder en ligne à son dossier ...).

3. Quels sont les délais moyens prévus pour la communication des informations ?

(La CNIL recommande une communication dans un bref délai : immédiat à quelques jours en fonction du lieu et du support de conservation de l'information) _____

¹¹⁶ toute personne peut s'opposer, pour des motifs légitimes, à ce que des données la concernant figurent dans un fichier .Ce droit d'opposition peut être exclu pour certains traitements du secteur public (Ex.: fichiers tenus par les services fiscaux, les services de police, les services de la justice, la sécurité sociale). Toute personne a aussi le droit de s'opposer, sans frais, et sans avoir à se justifier, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale

**MODÈLE DE NOTE D'INFORMATION
A PORTER SUR LES FORMULAIRES DE COLLECTE**

_____ (indication de l'identité du responsable du traitement)

« Les informations recueillies font l'objet d'un traitement informatique destiné à ... *(préciser la finalité . Les destinataires des données sont : _____ (précisez).* Conformément à la loi « informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à _____ *(préciser le service).*[vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant]¹¹⁷»

**MODÈLE DE NOTE D'INFORMATION
SUSCEPTIBLE D'ÊTRE AFFICHÉE**

«Le(s) service(s) _____ *(citer le nom du ou des services concernés)* dispose(nt) de moyens informatiques destinés à gérer plus facilement _____ *(indiquer la finalité du traitement).*

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : ... *(préciser les destinataires).*

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service _____ *(citer le nom du service ou des services concernés).* [toute personne peut également, pour des motifs légitimes, s'opposer au traitement des données la concernant]¹¹⁸»

¹¹⁷ à ne pas faire figurer si le traitement présente un caractère obligatoire.

¹¹⁸ à ne pas faire figurer si le traitement présente un caractère obligatoire.

Données traitées, origine des données, destinataires et durée de conservation des données

(Complément de la rubrique 11 & 12 du formulaire)

Il convient de détailler les éléments cochés en rubrique 11 & 12 du formulaire en complétant le tableau ci-dessous

| Détail des données à caractère personnel traitées | Origine des données | Destinataires des données | Durée de conservation sur support informatique (*) |
|---|---------------------|---------------------------|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

(*) Cette durée ne peut être illimitée ; elle doit être définie en fonction de la finalité du traitement (cf. recommandations de la CNIL dans les guides sectoriels)

Joindre éventuellement à ce tableau les formulaires de collecte des informations.

Attention :

- les traitements portant sur des données parmi lesquelles figure le NIR, Numéro d'Inscription au Répertoire national d'identification des personnes physiques ou qui requièrent la consultation de ce répertoire sont soumis à des procédures spéciales d'autorisation (articles 25 et 27).
- les traitements de données relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par (article 9) :
 - les juridictions, les autorités publiques et les personnes morales 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 (ex : cabinets d'avocats) ;
 - les personnes morales mentionnées aux articles L321-1 et L 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteinte aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits. (ex : sociétés de droit d'auteur d'œuvres musicales).

Sont en principe interdits les traitements de données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.. Toutefois, certaines catégories de traitements ne sont pas soumises à cette interdiction, dans la mesure où la finalité du traitement l'exige (article 8).